



AI-driven 6G networks and compliance with Open Internet rules

Challenges and opportunities with AI and
Digital Twins

Olga Batura, Prachi Sachdeva, Pieter Nooren

Document properties

Document title	AI-driven 6G networks and compliance with Open Internet rules - Challenges and opportunities with AI and Digital Twins
Authors	Olga Batura, Prachi Sachdeva, Pieter Nooren (TNO)
Reviewers	Marios Avgeris (UvA), Paul van der Wiel (TNO)
Dissemination level	Public
Status of the document	Final
Version	1.0
Work Package	WP5.4 Technology-Policy Co-Development (formerly WP4.5 in FNS Phase 1)
Deliverable	Part of FNS Milestone 5.4.1
Contractual delivery date	December 2026
Delivery date	30 September 2026
File name	FNS6G_20260930_AI_DTs_Open_Internet_v1.0.docx

Major contributions to impact pathways

Sustainable earning power	X
Digital autonomy and resilience	
Sustainability	

Management Summary

6G networks are being designed with Artificial intelligence (AI) embedded into their architecture, making AI an inseparable ('native') element of network functioning. It is envisioned that AI will, among other things, manage and optimise the use of network resources in an increasingly autonomous way. AI will thus actively determine in (near-)real time how to treat the various traffic streams in the network. This raises the question on how the AI-driven network management can comply with the existing European Open Internet rules (OIR, formerly known as the European net neutrality rules). This sectoral regulation sets rules on the equal treatment of all internet access traffic by internet access providers.

This white paper aims to put forward a balanced analysis. On the one hand, one can see the introduction of increasingly autonomous AI-driven networking as adding to the opacity of network management decisions, requiring new and further work to ensure compliance with the OIR. On the other hand, one can explore the opportunities for promoting and assessing compliance introduced by AI-driven networking and the Network Digital Twins (NDTs) that will accompany the AI. The two research questions in this paper therefore are:

- Can an AI-driven network be trained to comply with the OIR? How can (agentic) AI monitor compliance with the OIR?
- Can an NDT assist in an analysis of OIR compliance? How does that fit in the wider ongoing development of NDTs for 6G networks?

These questions are investigated by looking with considerable detail at the proposed architectures for AI-driven 6G networking, the potential roles for Mobile Network Operators (MNOs) and equipment vendors in the deployment of AI-driven networks and NDTs, and the key points of the OIR and the BEREC guidelines, including those on measurement methodologies.

Connecting these technical and regulatory perspectives shows that AI-driven 6G networks can be trained to comply with the OIR and that NDTs can support compliance. However, this does depend on a number of conditions being met for the development of AI and NDTs. There will be a learning curve, and the compliance benefits will materialise depending on the maturity and predictability of AI models. This is a task for the researchers, vendors and operators who develop and deploy the AI and NDTs. They weigh and decide on the quality and volume of training datasets, the room they provide to AI to steer networks, and the effort they put in interoperable interfaces that allow digital twins from different suppliers to be integrated. NDTs will remain imperfect models: their value depends on finding a workable 'sweet spot' between sufficient technical detail and acceptable computational, energy and telemetry efforts.

On the regulatory side, there are also actions that can be taken to encourage the use of AI and NDTs to improve regulatory compliance. BEREC can provide specific potential examples of network management situations with preliminary remarks on their compliance, as was done for 5G slicing cases earlier. The use of AI and NDTs in compliance will also benefit from the wider European drive to digital ready legislation, which includes making legislation machine absorbable and suitable for processing by AI.

A key takeaway from our findings and recommendations in Chapter 5 is that in the assessment of compliance, the above factors come together for both operators and regulators. They each depend on knowledge, inputs and actions from 'the other side': the operators and vendors work on the research and deployment of AI and NDTs, while regulators provide the guidelines and can develop machine absorbable regulation. It is therefore recommended that regulators consider setting up *regulatory sandboxes*. These can help to explore, in a more practical way and with industry involvement, the interaction between existing rules and use of evolving AI and NDT technologies.

Table of contents

List of Acronyms	5
1. Introduction.....	6
1.1. AI-driven networks and Open Internet	6
1.2. Research questions	7
1.3. Approach and structure of the white paper	7
1.4. The 6G Future Network Services programme	7
2. AI-driven networking.....	9
2.1. AI in the 6G architecture	9
2.2. AI-agents for 6G	10
2.3. Network Digital Twins	14
2.4. Relation between AI and Network Digital Twins.....	15
3. Open Internet requirements under the EU legal framework.....	17
3.1. Fundamentals of the Open Internet rules.....	17
3.2. Monitoring and measurement of Open Internet	18
4. AI and digital twins and Open Internet compliance in 6G networks.....	20
4.1. AI and Open Internet compliance	20
4.1.1. AI and its role in resource management.....	20
4.1.2. The link between AI-driven decisions and Open Internet rules	21
4.1.3. Training of AI.....	21
4.2. A future role for Network Digital Twins in Open Internet compliance.....	22
5. Findings and recommendations	26
5.1. Findings.....	26
5.2. Recommendations for companies and researchers	27
5.3. Recommendations for policymakers and regulators.....	28
Annex A. Network and application parameters to be assessed in the context of Open Internet	30
References.....	31

List of Acronyms

3GPP	3 rd Generation Partnership Project
A2A	Agent2Agent (Protocol)
ACM	(Netherlands) Authority for Consumers and Markets
AF	Application Function
AI	Artificial Intelligence
BEREC	Body of European Regulators for Electronic Communications
DT	Digital Twin
ETSI	European Telecommunication Standards Institute
EU	European Union
EZK	Ministerie van Economische Zaken en Klimaat (Ministry of Economic Affairs and Climate Policy)
FNS	Future Network Services
IAS	Internet Access Service
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISAC	Integrated Sensing and Communications
ISG	Industry Specification Group
ITU	International Telecommunications Union
KPI	Key Performance Indicator
LLM	Large Language Model
MCP	Model Context Protocol
ML	Machine Learning
MNO	Mobile Network Operator
NDT	Network Digital Twin
NF	Network Function
NRA	National Regulatory Authorities
OIR	Open Internet Regulation
OSI	Open Systems Interconnection (Model)
QoS	Quality of Service
RAN	Radio Access Network
RDI	Rijksinspectie Digitale Infrastructuur (Dutch Authority for Digital Infrastructure)
UAV	Uncrewed Aerial Vehicle
UE	User Equipment
XAI	Explainable AI
ZSM	Zero-touch network and Service Management

1. Introduction

1.1. AI-driven networks and Open Internet

6G networks are being designed with Artificial intelligence (AI) embedded into their core architecture, making it an inseparable element of network functioning. It is envisioned that AI will, among other things, in an increasingly autonomous way manage and optimise the use of network resources, actively determining in (near-)real time how to treat the various traffic streams in the network.

While real-time AI-driven decision-making is likely to enable innovative services and applications, ensure greater energy efficiency, and improve network performance overall, it also presents regulatory challenges. Will AI treat all internet access traffic equally as required by the European Union's Open Internet Regulation (OIR)¹? Can AI optimise network performance without discriminating against certain content, applications or services, as required by the OIR? The AI model opacity may prevent us from effectively understanding the decisions AI takes in the network.

This white paper explores the interactive relationship between the technical developments in AI-driven mobile networks, including their (agentic) AI and digital twins (DTs), on the one hand, and the Open Internet rules on the other hand. The paper aims to bring together the technical perspective, stemming from the development of AI-driven network and DTs, with the regulatory requirements of the current OIR, and examines how OIR compliance of the future AI-driven networks can be ensured. The paper, thus, can deliver useful technical insights for policy makers and regulators and explain the relevance of regulatory frameworks for companies and researchers developing future 6G technologies.

Compliance with the OIR is currently a topical issue, with BEREC conducting public consultations on the Further Guidance on 5G Network Slicing ([1, 2],) and the debates around the OIR in the recently proposed Digital Network Act heating up [3]. The BEREC consultations focussed at 5G slicing, for which compliance with the OIR proved and still proves to lead to discussion. From a conventional standpoint, 6G's AI-driven networking may well be seen as introducing a new round of complications around OIR compliance. Current traffic management in mobile networks (including 5G slicing) is still handled deterministically by human operators who, through management systems, explicitly assign resources to applications and their underlying traffic flows. With AI-driven networking, the resource assignment is governed by the AI-driven, intent-based networking and subject to real-time modification, potentially without human intervention. This would complicate the analysis and demonstration of compliance of traffic management with the OIR on internet access services and specialised services.

At the same time, the AI-driven networking also brings potential new powerful approaches around the OIR. This is the main line of analysis in this paper: the new technology can be seen as *helping* in the analysis of compliance with the OIR rather than as a further complication:

- The (agentic) AI may be trained to comply with the OIR rules for specialised services and internet access services.
- The Network Digital Twins (NDTs) that will be introduced alongside AI may be used to perform realistic virtual experiments to determine the effect of the traffic management on the applications.

¹ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310, 26.11.2015: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R2120>.

As a final introductory note, we observe that the OIR is only one of many regulations and requirements that AI-driven networks will need to comply with. In this white paper we focus at the OIR as it is a well-defined area of regulation with relatively few provisions that are well researched and interpreted, yet still lead to discussion in application to new technologies. This sharp focus allows us to examine in detail how alignment with current regulation can be achieved and new instruments for improving compliance may be created. It is for further study to widen the scope and try the approach in other policy and regulatory areas.

1.2. Research questions

This white paper addresses two research questions:

- Can an AI-driven network be trained to comply with the OIR? How can (agentic) AI monitor compliance with the OIR?
- Can an NDT assist in an analysis of the OIR compliance? How does that fit in the wider ongoing development of DTs for 6G networks?

1.3. Approach and structure of the white paper

The work presented in this white paper is based on desk research on the current and expected developments in the AI-driven networks and, specifically, AI agents and DTs, and the existing OIR rules. In addition, interviews were conducted with stakeholders from government, academia and industry to gather a range of relevant perspectives. These were (in alphabetical order): Authority for Consumers and Market (ACM), Dutch Authority for Digital Infrastructure (RDI), Keysight, KPN, Ministry of Economic Affairs and Climate Policy (EZK), Nokia, Odido, University of Amsterdam, and VodafoneZiggo. The insights from these interviews have been used to enrich the analysis and also validate it where possible, acknowledging that the analysis is future-looking with the associated intrinsic uncertainties. Finally, this white paper has been reviewed by the FNS partners involved in the technology-policy co-development work.

The white paper is structured as follows. Chapter 2 discusses what AI-driven networking is expected to look like in 6G and how AI and NDTs will be used in 6G networks. Chapter 3 provides a short overview of the central provisions related to Open Internet policy in the EU and discusses the regulatory approaches to assess and measure compliance with the OIR. Chapter 4 focuses on the interplay of AI-driven networks, NDTs and Open Internet requirements. Chapter 5 closes the paper with the summary of main findings related to AI-driven networks and Open Internet and relevant recommendations to industry and policy makers.

Because AI-driven networks and NDTs can be expected to show substantial development in the near future, it is expected that it is useful to revisit the analysis in this paper when the view on their capabilities has become more precise. As explained later in this paper, within the Future Networks Services (FNS) programme, there are specific experiments planned on the training of AI to comply with the OIR. The results of these experiments and the wider developments in AI and NDT will be analysed in a follow-up white paper.

1.4. The 6G Future Network Services programme

This white paper has been developed in the FNS programme [4], the Dutch multi-year public-private program on 6G development. FNS works on specific and connected topics in 6G: chips and components, AI-driven networks, and 6G applications in key sectors. This is combined with work aimed at strengthening the 6G ecosystem through a large-scale national 6G testbed and standardisation. Although FNS is a Dutch 6G programme, it is firmly embedded in the larger European and international effort on 6G development.

For the successful uptake of 6G technology, it is important that its development is well aligned with existing and future policies. This is the motivation for including research on policy-technology co-development in the FNS work on the 6G ecosystem, with AI-driven networking as one of the key topics. The FNS partners contributing to the policy-technology work are (again in alphabetical order): the Dutch Authority for Digital Infrastructure (RDI), Ericsson, KPN, Liberty Global, Ministry of Economic Affairs and Climate Policy (EZK), Nokia, Odido and TNO. The aim of this work is, among other things, to provide analysis and inputs for policy makers at the Dutch and EU levels. FNS does not have a role in policy decisions themselves.

2. AI-driven networking

2.1. AI in the 6G architecture

AI is a key technical component for 6G, both for the network itself and in the support of applications. This is seen at the highest level in the International Telecommunications Union's (ITU) framework recommendation for IMT 2030 that sets the requirements for 6G [5, 6]. The ITU has set out six new additional capabilities for IMT 2030, one of them being AI. Following from the ITU, 3GPP has started the global standardisation of 6G that explicitly includes AI [7]. 3GPP defines two important concepts for AI: AI for 6G System and 6G System for AI; and work on defining and standardising both is underway in multiple working groups. The European flagship project of 6G, HEXA X II, also considers AI-driven networks as one of the foundational pillars for 6G, and also investigates NDTs [8].

In its work on AI, FNS designs and develops algorithms, software modules and agentic-AI components that make the network self-driving and autonomous, supported by bias-free and explainable AI and decision logic. Also in the FNS 6G architecture [9], one of the design principles is AI-driven decision-making. This means that intelligence will be embedded into all layers (infrastructure, management, orchestration, application, etc.) and cross-cutting planes (security and trust, observability, etc.). Rather than relying on centralised logic and decision frameworks, the architecture will leverage distributed multi-agent systems (also referred to as agentic AI), where autonomous software agents operate at different layers to interpret intents, make local decisions, and coordinate with peers. These agents continuously observe telemetry, learn from context, and act toward fulfilling service goals in real time.

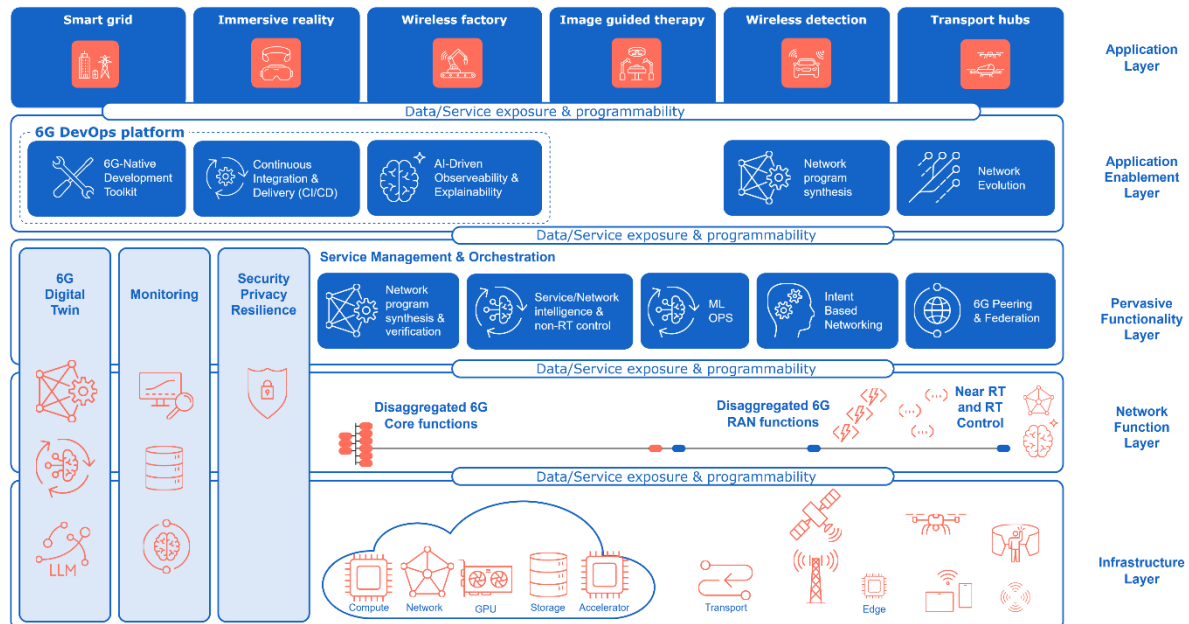


Figure 1: The FNS 6G Architecture.

The high-level FNS architecture presented in Figure 1 follows a top-down approach to ensure that the design is driven by application and service requirements, with a clear focus on how end-user needs translate into system capabilities. The architecture is structured into five horizontal layers, arranged from top to bottom: Application, Application Enablement, Pervasive Functionalities, Network Functions, and Infrastructure. The

first two layers, Application and Application Enablement, define how various verticals and application markets supported by 6G interact with the system, primarily through a unified exposure of network services provided by the underlying layers. The figure specially mentions the sector applications addressed in the FNS 6G application innovation work, the same approach applies to other applications. The Pervasive Functionalities layer encompasses cross-domain orchestration capabilities, enabling the management of network services from the lower layers to meet the diverse requirements of these verticals. Lastly, as the FNS infrastructure has a cloud-native design, the architecture makes a clear distinction between Network Function layer (logical entities that can operate across different hardware and locations) and the Infrastructure Layer.

In addition to these horizontal layers, the FNS architecture introduces three key vertical components—Security, Monitoring, and the 6G Digital Twin—which interact with the Pervasive Functionalities, Network Functions, and Infrastructure layers. These vertical components are designed to cut across and integrate with the lower layers, ensuring comprehensive coverage of critical aspects such as security, observability, and digital representation, respectively.

In 6G, applications may be located across the digital continuum. Applications may run on User Equipment (UE), such as smartphones and IoT sensors, at the network edge around the 6G Radio Access Network (RAN), or in cloud data centres in the network core for data processing and storage, as well as in external cloud infrastructures. An application's location determines its performance characteristics (e.g., edges typically provide lower response times to user endpoints than the cloud), its interfaces for connecting to networks, devices, and software (e.g., is the application deployed as a serverless function, within a virtual machine), and its available tooling for developers and operators (e.g., metric collection, application inspection and introspection).

2.2. AI-agents for 6G

In the global 3GPP standardisation of 6G, an AI agent is defined as an automated intelligent entity capable of e.g. interacting with its environment, acquiring contextual information, reasoning, self-learning, decision-making, executing tasks (autonomously or in collaboration with other AI Agents) to achieve a specific goal [10]. In a 6G network, AI agents help with intent translation. Instead of specifying detailed low-level instructions for the network, operators can define high-level objectives such as performance optimization goals, capacity expansion plans for traffic growth, and response and recovery strategies for automatically detected outages or failures. The role of an AI agent is to translate these high-level objectives into specific actions that it needs to perform (often in interaction with other agents) to reach those objectives.

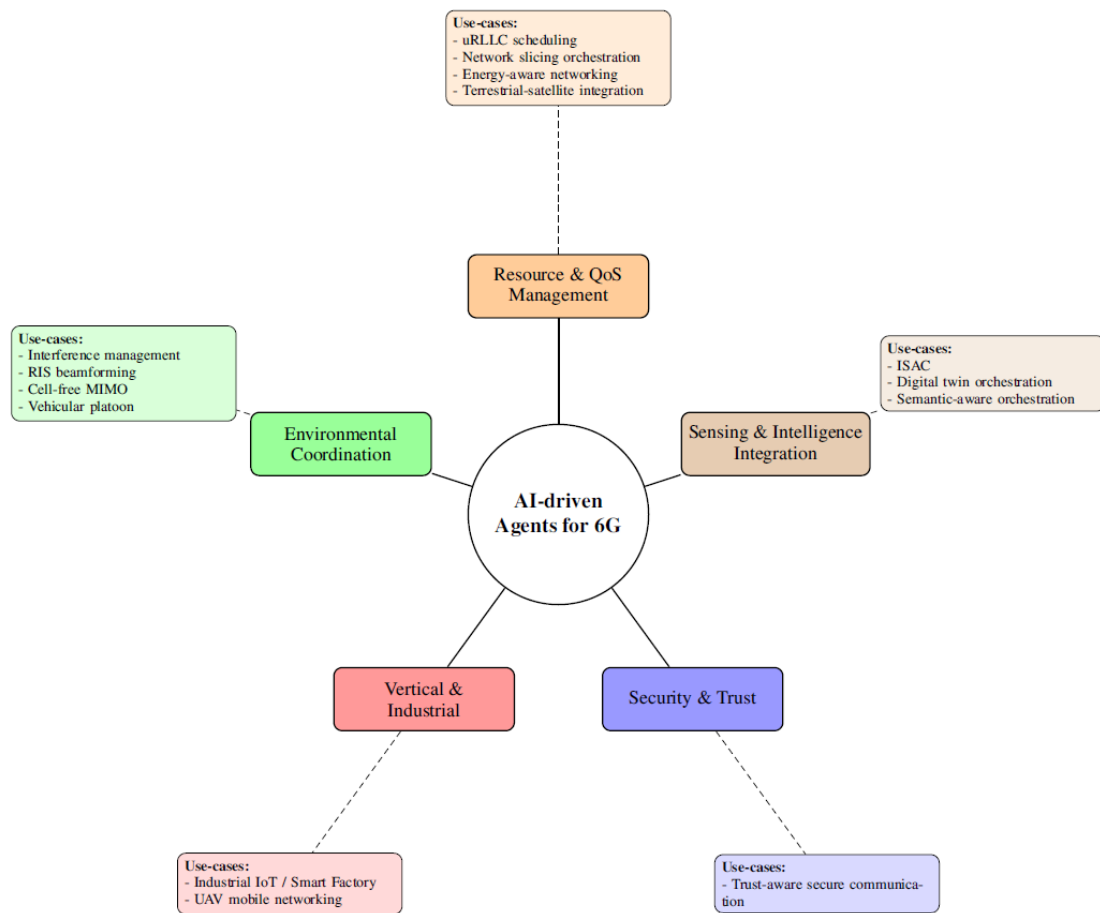


Figure 2: Common use cases in 6G for AI-driven agents [35].

Figure 2 shows several use cases for AI agents in 6G networks. In the context of the Open Internet Rules, multiple use cases are relevant, for example, the use cases in Resource and Quality of Service (QoS) Management involving agents that can make decisions on how to allocate resources optimally and enhance QoS across users and applications. This also links to another important block in the figure, the use cases in Vertical and Industrial, that may require tailored QoS in the 6G network with its specific applications. Note that the two use cases mentioned here, industrial IoT and Smart Factory, and Uncrewed Aerial Vehicles (UAVs) are also prominent 6G applications in FNS. Finally, Integrated Sensing and Communication (ISAC) use cases can be touched by the OIR. Depending on the arrangements, the sensing may consume substantial parts of the radio and uplink transport resources in the network for time-critical transfer of sensing measurements. The justification and impact of tailored QoS for the sensing traffic streams may then be subject to the OIR rules for specialised services (see Section 3.1).

In 6G systems, AI agents will be all-pervasive. This means that AI agents will be in the core network, with each Network Function (NF) likely having its own AI agent or being an AI agent itself, as well as in the RAN and the UE. Applications will also have their own agents, and communication between different applications or between an application and the network can also be facilitated by an AI agent. However, it is important to note that while current efforts in 3GPP are geared towards ensuring that parts of the network (such as the core network) can leverage AI capabilities, they will also ensure that 6G can function fully also as a non-AI network. Thus, requests generated within the network that do not originate from the processing of an intent will also be fulfilled.

While the interfaces between different parts of the network are often standardised, 3GPP will not be standardising the interaction between agents (agent-to-agent communication) or between agents and data sources. Efforts within Internet Engineering Task Force (IETF) are underway to create the framework, use cases and requirements for AI Agent Protocols [11]. Additionally, several de-facto or open standards exist within the industry, and current inter-agent communication sees commonly used protocols like the Agent-to-Agent (A2A) protocol introduced by Google [12] in 2025. The Model Context Protocol (MCP) designed by Anthropic [13] is an open standard for connecting AI agents to external data sources, codebases, and tools, and is also an integral part of the Agentic AI Foundation [14]. As technology develops, it is likely that these protocols evolve as well, and future AI agents and applications may be using more advanced industry-accepted protocols.

There are many proposals on how an agentic AI 6G system can be created in academic research papers [15] and in individual company contributions to standards bodies like 3GPP. A hierarchical multi-agent system is the most common concept, with a central agent managing other agents functioning under its command. One or more AI agents in the network could be the key nodes to handle and fulfil requests containing intent. Typical roles of AI agents may include:

- Planner/coordinator (e.g. central agent, system AI agent, network AI agent, intent analysis agent, planning agent, service decomposition agent). The AI agent function in this role serves as a central node to interpret and decompose the intent, generate a plan, coordinate the capabilities provided by other AI-Agents, non-agentic NFs and trusted Application Functions (AFs) based on the plan, monitor the plan execution and optimise it based on the network feedback and contextual information.
- Specialised executor (e.g. assurance agent, connection agent, data agent, compute agent, service agent, execution agent). The AI agent function in this role is responsible for fulfilling the specialised tasks assigned by another AI agent that acts as the centralised planner/coordinator [10].

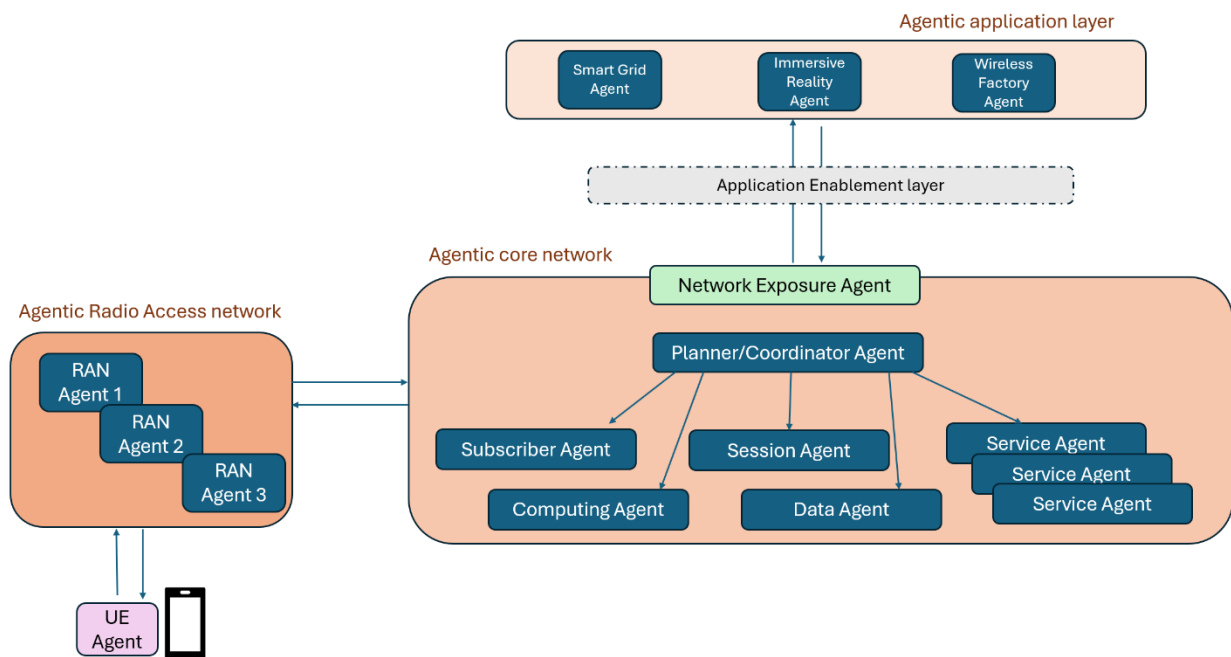


Figure 3: A representation of an agentic 6G system (source: FNS).

Figure 3 shows a possible representation of an agentic 6G network based on the hierarchical multi-agent concept and on the FNS 6G architecture from Figure 1. There are AI agents in all parts of the network: core, radio, at the application layer, and at the UE side. An agentic application layer sits on top, with AI agents for each application that interface with the mobile network. The examples shown here are some of the 6G applications specifically studied in FNS. These application agents rely on the mobile network for the services and connectivity that the applications need. An abstraction layer called the application enablement layer provides services for applications, such as a DevOps platform and interfaces such as CAMARA APIs, cloud deployment APIs, and intent-based interfaces. This layer is also envisioned to be agentic in 6G networks.

These applications interact with the core network through the network exposure agent, which exposes the request from an application and informs the network what is needed for a particular service. The core network here shows different kinds of AI agents for different tasks, such as a session agent, subscriber agent, computing agent, managed by a central agent which acts as a planner or coordinator. Some architectures options presented for 6G also include an AI Management Function (AIMF) that is responsible for managing the AI agents in the core and radio of the network as well as the UE.

Agentic AI systems are still under research, and real network implementations are not expected for a few years. However, there are several ways in which an MNO could deploy agentic AI in their network in the future. The MNO can, of course, create AI agents in-house using known models and train the models using its own real network data. In this way the operator can introduce an agentic structure completely tailored to its needs. However, the operator may also choose to reduce its own development effort by buying vendor products offering integrated AI. At the moment, network vendors offer products (such as network functions) with integrated AI, but this AI is not agentic. Given the research into agentic systems, it is expected that most vendors will also offer agentic AI products in the future. The AI models within these products are trained using synthetic data sets or publicly available online data sets, as access to real network data from an operator is hard to come by for vendors. In an effort to create such data sets for open use, in early 2026 the Smart Networks and Services Joint Undertaking also released a call for projects that would focus on collection, generation and validation of datasets suitable for training AI models for 6G Networks [16]. In the future, reliable open data sets may be available for use, however, currently this also means that when these products are introduced in an MNO's network, a period of re-training is needed. The output of an AI system is heavily dependent on the data it has been trained on, and thus in order to generate the right decisions for the specific MNO network, AI must be re-trained using network data from that particular network.

The AI can be trained on traffic profiles and patterns in the network, which are different for different applications (e.g., video streaming traffic has a different bandwidth-over-time profile than messaging or IoT traffic). When it comes to packet inspection, the analysis of the traffic can technically be performed on the level of IP headers and of IP payloads. IP packet header analysis is commonly used to manage traffic, yet cannot be used to discriminate between different senders or recipients. IP payload inspection techniques are more intrusive as they typically access information in the payload that is addressed to the recipient of the communication. These techniques can still be used for traffic management purposes, for example, when the inspection is based on the protocols. However, when payload inspection is used, privacy and personal data protection rules must be respected in addition to the Open Internet rules.²

² In particular, Article 5(1) of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002 and Article 3 OIR.

To determine whether network management (with AI integrated in certain parts) is making the right decisions and taking the right actions, operators currently monitor the performance of the network against certain KPIs. However, another active field of research is Explainable AI (XAI). XAI is the ability of the AI to explain or to present its working and outcomes in understandable terms to a human [17]. XAI can be used in two stages. The *understanding phase* involves the training and quality assurance of an AI model, whereas the *explaining phase* is important when an ML model is deployed and used in real-world applications, and makes the XAI a useful tool when OIR compliance is in question [18]. If the AI in 6G networks explains itself in a human-readable form, MNOs would have the ability to track decision making better and tailor the deployment to suit their needs, complemented by structured evidence that the AI is capable of producing, such as logs, causal explanations and policy proofs. For now, XAI remains a field of research and its introduction into an operator network is not foreseen in the near future.

2.3. Network Digital Twins

Digital Twins are another key technical ingredient in 5G-Advanced and 6G networks. In the FNS architecture (Figure 1), they are positioned as a key vertical component. A DT is a software representation of an object or a set of objects for the purpose of modelling some of the characteristics and behaviours of such real-world objects or systems. A DT provides support to network management and operations by creating a virtual representation of the corresponding physical network processes. A DT can be created for any physical object in a communication network. The DT may also be created for a group of objects, e.g. for the sets of network objects that form the RAN segment or the NFs in the Core network [10]. This is sketched in Figure 4.

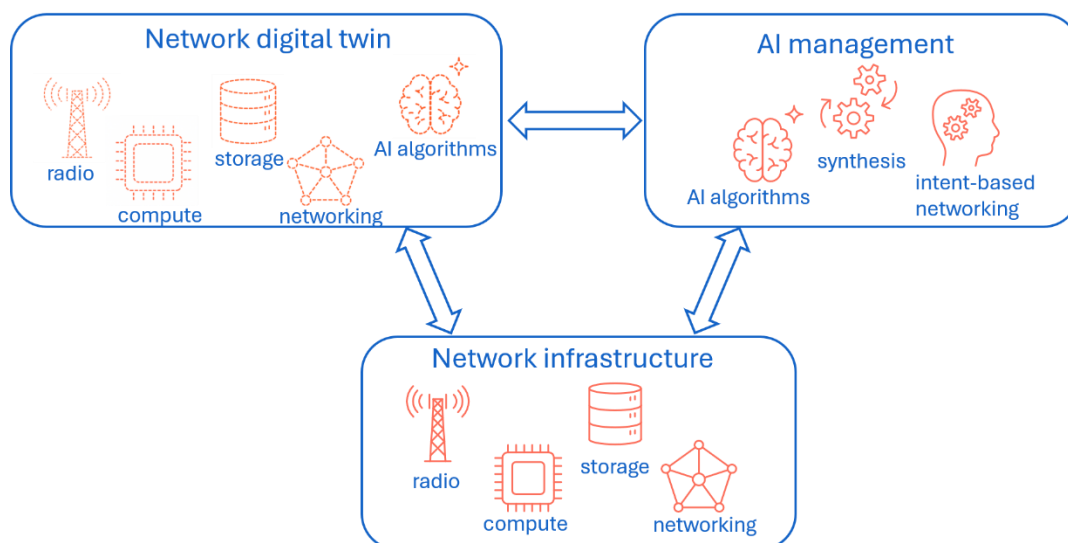


Figure 4: A representation of an AI-based 6G network showing the network infrastructure being modeled in the NDT.

While DTs are a fairly new research area, simulators have existed for a long time. A DT functions as an advanced simulator; however, not all simulators are DTs. Simulators are programmed using mathematical models to replicate the overall behaviour of a system without detailed interaction, and are designed based on physical attributes, design specifications, and environmental conditions. Once programmed, simulators do not interact with real-life processes. On the other hand, a DT can enhance mathematical models through machine learning, AI or other methods, and they depend on operational data collected in real-time from sensors and other sources, and support real-time interfaces into the physical world.

An NDT is used as a replica of a mobile network, to learn how the mobile network would behave in certain scenarios, without causing any changes to the actual mobile network. The NDT can assist in efficient management of mobile networks, help to build resilient networks, help to speed up deployment of new services, and enhance network quality. For example, with NDT, network operators can verify network behaviour before they apply configuration changes to the real network to prevent unintended behaviour, which contributes to resilient networks and enhancement of network quality. Additionally, network automation functions can use an NDT to analyse network behaviour, which can contribute to reducing operator's manual operation and improve management efficiency.

Current efforts in FNS are focused on creating sub-twins of the networks, rather than a single large NDT. In research and practice, the scope of a DT is often limited to the level of abstraction needed to address the specific problem the user is solving at the moment. This means that for some tasks a high level modelling of the network may be sufficient, while for others a detailed NDT of a certain part of the network, such as the radio access network, may be needed. Creating sub-twins ensures that the task is manageable and the performance of the NDTs is validated. In the future, the sub-twins will be integrated to create a full DT of the network. This is expected to be an extensive task and could take a few years to be perfected.

While some MNOs are creating their first generations of DTs in-house using real network data from their networks, it is also possible to buy DTs of certain parts of the network off-the-shelf from a vendor. Many vendors offer DTs of their own products that the operator can use as a building block for their DT of the complete network. The DTs offered by the vendors have typically been configured and tuned using synthetically generated data, as they do usually not have access to real network data. The MNO then integrates these DTs into its network but likely needs to tweak parameters and settings till it can attain a twin that reliably mimics its own network. Most interviews conducted during the writing of this white paper have shown this as the preferred option, as creating an NDT completely in-house is expected to involve more effort. Another option is a custom vendor solution, whereby a vendor could offer to create, as a system integrator, an end-to-end AI driven network for the MNO, with integrated AI agents and DTs for not only its own products but also for products provided by other vendors. Yet another option is that an independent system integrator performs this end-to-end integration. This essentially reduces work at the MNO's end in achieving seamless integration of the different parts of the network. There are examples of such system-integrator approaches in other application areas for DTs, such as data centre operations [19].

2.4. Relation between AI and Network Digital Twins

In the 6G network, AI agents and DTs are expected to work collaboratively. The operator of a mobile network can specify a certain intent, such as optimising the radio resources of a particular area of the network, and the AI agents translate this intent into specific actions. However, the actions derived by the AI agents could also unintentionally hamper network performance for some users. This is where DTs play a role. An NDT is essentially a testbed where the effects of certain actions within the network can be observed. Different variables can be adjusted or kept constant to observe and isolate the effects of certain actions. Based on the results of this testing, and after adaptations of the changes where needed, the changes can then be pushed with confidence into the live network.

However, before the AI-driven network and a DT go live in the network, they must be thoroughly tested to ensure that the results generated by an AI-driven network and its validation in an NDT can be trusted. Here, the operator must ensure that the actions recommended by the AI-driven network and its effects within a DT are indeed equivalent to what would be observed in the real network. In order to fully analyse the results generated by a DT, it is foreseen that logging of decisions/actions will be introduced. These would be human-readable logs giving the operator the opportunity to review the actions carried out.

When AI-agents and DTs work together like a well-oiled machinery, it reduces the need for human control and allows the network to operate more autonomously. The system works as a closed-loop and improves through feedback, reaching a point over time where human intervention is minimal. In the so-called zero-touch network concept [20], human intervention is no longer necessary at all. This concept has been theorised for 6G networks. Efforts towards zero-touch networks include ETSI's Industry Specification Group on Zero-touch network and Service Management (ISG ZSM) [21] which works on several areas such as NDTs, study of the ZSM framework and architecture, and architectural enhancements for agent-based network and service management. However, the reality is that models can shift and are generally not robust enough, thus making a zero-touch network a faraway dot on the horizon. It is likely that for many years to come, MNO networks will require a certain degree of hands-on control, while an increasing number of tasks can be offloaded to AI and NDTs.

3. Open Internet requirements under the EU legal framework

3.1. Fundamentals of the Open Internet rules

The concept of Open Internet, earlier often referred to as net neutrality, refers to the way Internet access service (IAS) providers should treat data carried over their networks from providers (e.g. content, application, services) to end-users and vice versa. In EU law, the concept found its expression in the OIR of 2015. This section provides a summary of the main points to set the scene for the further analysis in this white paper. Several other texts (e.g., an earlier TNO study [22]) treat the topic in (much) more detail and include the role of the BEREC guidelines [23] on the implementation of the OIR and make a mapping to 5G mobile.

The basic principle of the OIR requires that IAS providers treat all traffic equally and non-discriminatorily, both from the technical perspective and in their commercial practices (e.g., prohibition of zero-tariff options).³ The equal treatment of all internet access traffic means that it is managed independently of applications and of end-users. Note that this does not imply that all end-users will experience the same performance and QoS.

While the obligation to ensure Open Internet access lies with IAS providers, it is supposed to guarantee the corresponding right of IAS end users to access and distribute the information, content, applications and services of their choice (Article 3(1) OIR). To this end, Article 3(3) OIR prohibits IAS providers from blocking, throttling and discriminating between content, applications and services. Simply put, with IAS they should provide a best effort, application-agnostic internet access. Importantly, IAS providers may offer internet subscriptions with different levels of quality of service, as long as they are application-agnostic.

Equal treatment of all traffic does not mean that IAS providers should adopt a hands-off approach. They can employ traffic management measures to optimise the QoS, as long as they are reasonable and do not violate the Open Internet obligation. Only in a few exceptional cases (i.e. either to comply with legislation, to preserve network security or to prevent exceptional or temporary congestion) IAS providers may block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services. Whenever traffic management measures are taken, they must comply with the principles of necessity and proportionality regarding the processing of personal data.

Article 3(5) OIR allows the provision of specialised services, i.e. services optimised for specific content, applications or services, if the optimisation is necessary to meet requirements of the content, applications or services for a specific level of quality. The implementation of specialised services must be based on objectively different technical requirements (i.e. to meet a certain level of quality) and not on commercial considerations. Specialised services must not be detrimental to the availability and general quality of general internet access services and do not replace Internet access services.

The OIR does not require MNOs to obtain a prior authorisation in relation to any commercial practices, traffic management practices or specialised services. In this sense, MNOs are presumed compliant, unless established otherwise based on an investigation. National regulatory authorities (NRAs) are responsible for

³ As indicated by the case law of the Court of Justice of the EU in C-854/19 Vodafone (roaming), C-5/20 Vodafone (tethering), C-34/20 Telekom Deutschland (throttling) and others, and interpreted by [23].

monitoring the compliance with Open Internet requirements, for example, by setting the minimum QoS, relevant technical conditions or requesting on traffic management information from MNOs.

3.2. Monitoring and measurement of Open Internet

To ensure that Article 3 OIR requirements are fulfilled by telecom providers, the NRAs must monitor restrictions of end-user rights, contractual conditions and commercial practices, traffic management practices, and Internet access services' performance. They must also monitor the impact of specialised services, if any, on the general quality of internet access. BEREC has adopted guidance and methodologies that provide insight in the approach and the expected level of detail for the monitoring and measurement. This is relevant for the analysis in this paper: the AI-driven networks will be subject to the same monitoring and measurements, which may have consequences for their design. Furthermore, if an NDT is to provide an environment for realistic digital experiments, then it will probably need to provide the same level of detail expected from the real-world measurements that it aims to imitate.

BEREC considers that IAS technical performance can be measured on two levels [24]:

- On the user level, IAS performance can be measured to check its correspondence with the contractual obligations of the IAS.
- On the market level, user-level assessments can be aggregated across different categories (e.g. geographical locations, access technologies, IAS providers). Market-level assessment of performance can be used to check for the presence of specialised services and their influence on Open internet (e.g., degradation of services).

Technical aspects of Open internet, such as network performance and QoS, can be measured based on quantitative data related to specified parameters. Naturally, the interpretation of such measurements can be complicated as it needs to take into account multiple factors, from end-user equipment to signal strength to physical location of the antenna and hurdles between the base station and the receiver. For market-level assessments, data need to be collected over many network points, aggregated and compared across time and different IAS providers. BEREC developed an extensive regulatory assessment methodology [24] for NRAs to use in their monitoring and supervisory functions. This methodology is based on various measurement tools and harmonised measurement approaches for quality of service parameters [25]. These parameters [23, 24, 26] include the IAS speed in download and upload, latency, and blocked ports. These network level parameters are complemented by application level parameters, for example for web browser performance and video streaming. The complete list is in Annex A.

BEREC explains [27] that, for example, NRAs can request the information about IAS provider's traffic categories, QoS requirements for each category and data packets handled by each category. Furthermore, traffic management shall not monitor any specific content, conduct intrusive IP payload inspection or discriminate between encrypted and unencrypted traffic.

For the non-technical aspects of Open Internet (e.g. contractual clauses, pricing policies and other commercial practices), measurement is not possible. Rather, NRAs must conduct assessments based mainly on qualitative data collected through market investigations, requests for information from IAS providers, complaints from users, analysis of traffic measures records and user standard contracts and similar information. An exact methodology for assessment of such information does not exist, and the OIR together with the case law of the Court of Justice of the EU serves as the only authoritative interpretation guidance for the NRAs.

Overall, it can be observed that the OIR – even considering several guiding documents by BEREC – are not always clear to relevant stakeholders. For example, the application of the OIR to network slicing is an issue

that MNOs have been asking to clarify for some time, and where BEREC is currently drafting a separate guidance [28, 29]. It is conceivable that the use of new technologies, such as AI and NDTs, in mobile networks will also cause need for clarification.

In the next chapter, the monitoring and measurement methodologies will be revisited to analyse how AI-driven networking and NDTs relate to them.

4. AI and digital twins and Open Internet compliance in 6G networks

4.1. AI and Open Internet compliance

4.1.1. AI and its role in resource management

Against the background on AI-driven networks, DTs and the OIR from the previous chapters, it is now possible to analyse at which positions in the network decisions taken by the AI can have an impact on compliance with the OIR and in what way. The starting point for this is Figure 3 from Chapter 2. The figure presented below highlights the three parts in the network where decisions taken by the AI could potentially impact compliance.

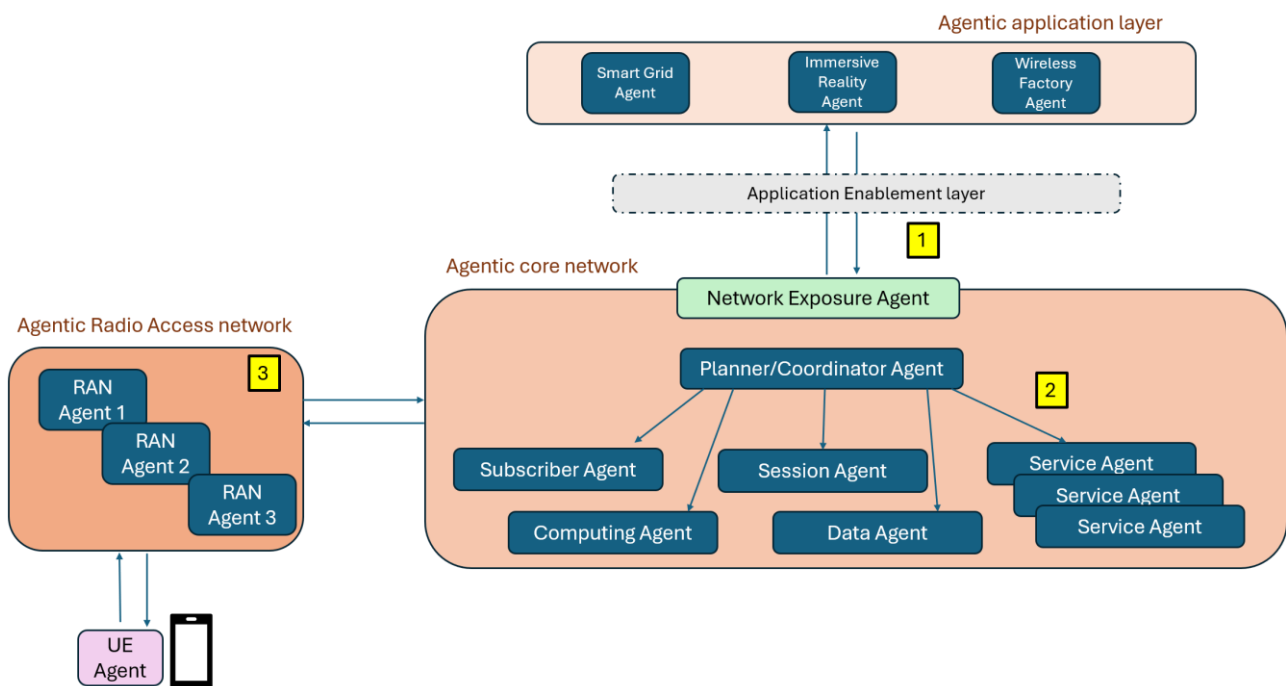


Figure 5: An agentic 6G system with three parts where AI decisions touch on OIR compliance.

- 1) Applications interact with the core network through the network exposure agent and tell the network what is needed for a particular service. This forms a critical layer in the network where decisions taken by agents will play an important role in compliance, because this is where certain applications can receive priority over other applications. Certain applications that are sensitive to latency and jitter may be given a different resource allocation in the lower layers of the networks. All such decisions will be taken by the agents and touch on compliance with the OIR.
- 2) The decisions made at the higher layers in the stack are implemented and brought to execution on traffic flows in the lower layers. This means that the decisions made by the agents operating at the network functions in the core will ultimately dictate the distribution of resources at OSI layer 2 and 3 in network segments in the infrastructure layer, including any priorities and reservations for specific users or applications. This directly touches the compliance with the OIR. Note that over time, the telemetry and feedback generated by the agents at the lower layers will be used by the

agents in the higher layers to learn and refine their decision, which again touches on OIR compliance.

- 3) The RAN in 6G will also have agents that make decisions on how the radio resources are divided amongst different users and applications. Some of the agents in the radio network are steered by agents in the core, and in turn steer agents in the lower levels of the stack. If resources scarcities occur in mobile networks, they are often in the RAN. Optimisation of their allocation has always been a key point of attention for MNOs. There are well-known situations where radio resources become particularly constrained, such as during events with many users are gathered at one location. In congestion situations like this, the agents must make decisions that are in compliance with the OIR.

It is seen that the points in the AI-driven 6G network where agents' decisions touch on Open Internet rules are roughly the same points that are relevant today in 4G and 5G networks. The essential difference is that instead of the human operators at the MNO specifying the detailed instructions and parameters, the agents will be taking the decisions based on their translation of the MNO's intents and breaking those down into specific actions for lower-level agents.

4.1.2. The link between AI-driven decisions and Open Internet rules

As noted above, AI will be deployed in 6G networks at important points of decision-making relevant for Open Internet requirements. Three examples of this are:

- AI (agents) can take automatic autonomous decisions to block certain ports, domains and IP destinations based on legal requirements (e.g. due to violation of intellectual property rights) and on network security grounds. Such decisions may have impact on Open Internet if executed incorrectly (e.g. exceeding the level of blocking necessary). The Open Internet rules must be, therefore, included in the AI instructions next to network security and other issues.
- AI agents can develop and attribute specific QoS parameters to different applications and groups of applications provided via IAS, which would ultimately define traffic management for different applications. AI agents can also assign priority levels for scheduling resources among QoS flows. All these activities must adhere to the OIR rules, not discriminating between services, content and clients.
- AI agents can devise specialised services and take decisions on attributing specific resources to them by assigning priority, allocating bandwidth and in other ways. To avoid negative impacts on Open Internet, such AI agents also need to ensure that optimisation is indeed necessary for specialised services based on their objective technical needs and that the quality of general IAS does not deteriorate.

Moreover, AI can also become relevant for non-technical Open Internet requirements. For instance, AI-agents can be involved in defining or applying the appropriate tariff to IAS services. According to the current OIR rules, such tariffs must exclude zero-rating or tariffs differentiated based on the application carried over the IAS.

There are also certain Open Internet issues that are beyond the scope of AI used in 6G networks. For example, the evaluation of whether specialised services are alternative to IAS is independent of AI.

4.1.3. Training of AI

An AI-driven network must be trained to make suitable decisions. Suitable covers many areas: from satisfying business agreements and SLAs, to optimising short and long-term capacity planning and as will

be clear from the previous sections, complying with regulations such as the OIR. When an AI model for a network is trained, it must learn to comply with all the above, just as a human operator would, and with the expectation that it shows significant added value over human-operated networks, for example through reduction in errors and, better and quicker decision making

The current industry focus is on AI that is trained using Large Language Models (LLMs). However, just like all AI, LLMs suffer from stochasticity: there is a certain amount of unpredictability in their outcomes. In cases where the stochasticity leads to results that are readily recognised as incorrect by humans, this is often referred to as hallucinations. In an effort to increase the grounding of the AI, and to make the outcomes more deterministic, specific training methods such as Retrieval Augmented Generation or neurosymbolic approaches could be used. FNS plans to run an experiment wherein the OIR and the BEREC guidelines will be used as an authoritative input for the LLM, with the aim to ensure that the AI is trained to comply. The decisions from this trained AI will then be tested in a DT, and the outputs will be measured, thus giving us an opportunity to validate the assumptions.

As already indicated in chapter 2 and Figure 6, AI agents in the network will have different functions. There can also be agents created for the specific purpose of coordinating, monitoring, or checking of compliance. These agents can regularly check adherence to different regulations and provide feedback to the other agents to ensure that actions at all levels are compliant with regulatory requirements. Agents could also be programmed to provide human-readable feedback so that the operator can keep track of essential aspects within a network. As a cross-check, this feedback can be compared to logs and traces from the network to confirm that the decisions have propagated correctly to the infrastructure level. This cross-check can be extended to include actual measurements on the performance of IAS at end points, as described in the BEREC measurement methodology (see section 3.2). The challenge here is to build a robust and trusted approach to collect and interpret the potentially large body of data. There can of course be a role here again for AI and then the question of compliance partly shifts to the quality of this particular AI used to evaluate the compliance of other AI with the OIR.

With agents checking compliance and taking measurements at certain points in the network, it is critical to carefully select the data they have access to. Just as in the case of training of AI (section 2.2), privacy and personal data protection rules must be respected when inspecting IP packets.

In the end, the quality of the training depends on the data fed to the model. For training on compliance with the OIR, in addition to the OIR and the BEREC guidelines, operators can use historical data from their network, containing specific cases where compliance was ensured. However, a challenge with historical network data on compliance with OIR is that the data from European MNOs will probably contain only few OIR-relevant cases, as there have been few specialised services and in-IAS differentiation cases in the EU.

4.2. A future role for Network Digital Twins in Open Internet compliance

The desk research and the interviews for this paper confirm that NDTs are an active area for research and also an area where operators and vendors already develop and integrate solutions and products. They have visions and roadmaps to extend and refine their DTs for network segments or products and integrate them into larger NDT). This also opens up future opportunities to exploit NDTs for in the area of OIR compliance. This involves two main use cases:

- Use of NDTs to perform virtual experiments to determine the effect of traffic management measures on the service parameters relevant for the OIR rules. Here, the experiment will typically comprise a comparison of two network configurations, for example a reference configuration that

complies with the OIR and new, proposed configuration with specific traffic management measures for which the compliance is to be checked.

- Use of NDTs to inspect the effect of traffic management in specific historical events by playing back from logs and traces of the network.

Technically, the main question is whether the level of detail available in the NDT analysis is sufficient to assess compliance with the OIR requirements. A clear point of reference is the level described in the BEREC measurement methodology. The desk research and interviews bring out two sides here.

On the *opportunity side*, there are already many network simulators in use, with detailed parameters that are approximately at same level as the BEREC parameters. For many years, there has been an ongoing development of detailed simulators for radio planning driven by the need to optimise the use of spectrum and radio infrastructure. These simulators also go into the distribution of resources over different users and applications, which makes them relevant for the use case of OIR compliance which is also about distribution of resources. These simulators have started to evolve into DTs, for example in the work in FNS programme line 2. Therefore, a certain baseline of NDT functions relevant for the Open Internet use case will become available for the radio access segment. Also, for the core network segment, planning tools and simulators are evolving into NDTs. Although this is for a large part still in the R&D phase, the first steps are already visible in the market for mobile network equipment and software:

- Vendors of mobile network equipment have started to provide DTs of their products, in the form of software products. They are in a good position to provide DTs based on their detailed knowledge of the inner workings of their hardware and software.
- As already observed in section 2.3, some vendors and independent system integrators see potential to integrate the NDTs of individual components into larger network-wide DTs. This provides mobile operators with an option to outsource (parts of) the building and integration of their NDTs as an alternative to in-house development.
- The development of NDTs is accompanied by development of telemetry, needed to determine the proper tuning and setting of the NDTs from the live network.

On the *challenges side*, the technical circumstances in which Open Internet issues actually play out tend to be at the edge of the network performance envelope (similar to a ‘stress test’). If network resources are plentiful then priorities between traffic streams in IAS or between IAS and specialised services have only little effect. It is at peak network loads that the effects become visible: at IP-level, packets may be queued for longer or get dropped which affects the quality of the applications, with the distribution of the effects depending on relative priorities. The precise modelling of these effects calls for very fine-grained NDTs mimicking the hardware-software stack in such a detailed way that these inner workings at peak loads can be determined properly. As the NDTs will likely be implemented in software running on general-purpose cloud infrastructure, the compute time for such a detailed NDT can easily exceed the time interval that is simulated. This is because the signal and packet handling in the real-world network runs on optimised Application Specific ICs (ASICs) or other tailored hardware, which provide several orders of magnitude more performance than generic compute hardware. Of course, the compute time for the NDT can be shortened by running it on optimised hardware and GPUs [30]. However, this moves the NDT closer to the actual network hardware itself, challenging the concept of the NDT as a *digital software* model⁴. A detailed

⁴ One of the WP4.5 partners observed the analogy between the level of detail in an NDT and a [famous story on cartography](#) by Jorge Luis Borges (who was in turn probably inspired by Lewis Carroll). In the story, an empire becomes more and more skilled at cartography and creates increasingly detailed maps, eventually producing a map that has exactly the same physical size as the empire itself.

NDT would also tend to consume a substantial amount of energy in its computations. Apart from this compute challenge, there is also the challenge in the massive amount of telemetry input that needs to be collected from the real-world network to get the precise settings for such a detailed NDT.

Seizing the opportunities while addressing the challenges revolves around finding the proper level of detail of the NDTs (a 'sweet spot'). It is important to recognise that no matter how much detail is put into the NDT, it is still a limited representation of the real-world network. Put otherwise, and still with appreciation for the advanced technology in NDTs: 'All models are wrong, some models are useful'.⁵ Here, the NDT is useful if it is close enough to the real-life network for evaluation of Open Internet requirements. Although, as said, the advanced NDTs are still in the R&D phase, a useful NDT and a sweet spot should appear combining two elements:

- For NDT availability, build pragmatically on the NDT use cases that operators already need for other purposes and that operators and vendors will therefore create anyway. The radio and capacity planning use cases are the most relevant here as they are close to the OIR area. The effort spent on these NDT uses cases will show what is realistically achievable for the level of detail. Since these use cases are key to operators, independent of the OIR, their uptake of these NDTs will give an indication of the confidence the operators themselves have in the NDT modelling. This also provides a baseline of realism to the use of NDTs for OIR compliance.
- For the OIR compliance assessment side, determine a level of detail (and thus level of abstraction) that is sufficient (and thus acceptable) for analysing compliance with the OIR requirements. The BEREC list of Open Internet parameters has considerable detail. It may turn out to be computationally prohibitive to apply to larger networks. One option is to apply it to smaller segments of network that are deemed representative. Another option is to apply it at an abstracted level where the focus is, for example, on throughput and latency. For example, in situations where the throughput approaches the threshold, larger latencies and packet loss become more likely. An understanding of this interaction could be used to model packet loss through throughput and latency. This would reduce the number of parameters and the computational effort. This could lead to more NDTs that are suitable for assessing OIR compliance.

These technical considerations also link to important non-technical factors. The internal compliance departments in MNOs must have trust in NDTs, especially if they are developed or integrated by third parties. According to the interviewed experts, in many cases vendors develop NDTs using synthetic data, as actual network data is not available on the market, not least due to the General Data Protection Regulation and even stricter ePrivacy rules applicable to telcos. Subsequent adjustments of NDTs by telcos using their own data, and deployment of DTs first in an isolated part of the network and slowly integration in the active network help enhancing the precision of DTs and improving trust in them.

Then there is the question to what degree regulators trust the use of NDTs for compliance purposes given that the NDTs are (partly) developed and deployed by the companies they should oversee. Testing in NDTs is unlikely to be ever accepted as evidence of compliance, not least because the real-world circumstances are always different from a simulation and NDTs is an imperfect model (as explained above). At the same time, the regulator cannot have its own NDT for checking MNO's compliance. Not only is the development of NDTs technically complex and expensive, the regulator will also run into the problem of training data

⁵ Attributed to George Box and Norman Draper (1987), https://en.wikipedia.org/wiki/All_models_are_wrong.

availability. Probably it would also need to have multiple NDTs or NDT variants to model the networks of multiple MNOs. Regulatory sandboxes can be a solution to explore the limits of the modelling ability of DTs and, through that, increase the trust of that regulator can place in them. Regulatory sandboxes are concrete frameworks which enable the testing of innovative technologies – even in a real-world environment – for a limited time and in a limited part of a sector or area under regulatory supervision, which ensures that appropriate safeguards are in place [31]. In regulatory sandboxes, operators can demonstrate the performance of relevant parts of DTs to regulator, test various levels of abstraction in the model, or regulator could even request insight into DTs. Regulatory sandboxes will increase the transparency of NDTs for regulators, while also providing more legal certainty for companies that want to use them as a due diligence measure for fulfilling Open Internet requirements.

5. Findings and recommendations

5.1. Findings

Assuming Open Internet remains an important regulatory requirement in the future,⁶ MNOs will have to comply with the obligations, independent of the development and changes in mobile network technology. The 6G AI-driven networks will have to be designed with Open Internet rules in mind, so that they comply with the rules from day one – as well as with the many other requirements from the overall regulatory framework for electronic communications.

The significant change that the deployment of AI-driven networking brings, is that it contains smart technical components that, to a certain degree and under right conditions, can learn the regulatory requirements. As analysed in the preceding chapters, they can support MNOs' compliance with applicable legal requirements. The AI itself also needs to be specifically trained in following the legal requirements. In particular, AI used in the MNO networks can be trained to learn the OIR rules and the relevant parameters and metrics that must be maintained and monitored. NDTs can be used to test and validate new services and their impact on the network traffic, which will allow to adjust the network capacity and new services to comply with the OIR before they are introduced in the live network.

The two research questions from Chapter 1 that have steered the analysis in this paper are:

- Can an AI-driven network be trained to comply with the OIR? How can (agentic) AI monitor compliance with the OIR?
- Can an NDT assist in an analysis of the OIR compliance? How does that fit in the wider ongoing development of DTs for 6G networks?

We conclude that we can answer the first parts of each question with a conditional yes. However, these positive effects cannot be expected from the very beginning. There will be a learning curve, and the compliance benefits will materialise only if certain conditions are fulfilled. The conditions become clear when we look further into the questions:

- A successful deployment of AI and NDTs depends on the maturity and the degree in which research into AI-driven networking takes into account the need to comply with the OIR. Just as many other relevant rules from relevant legal and regulatory frameworks, the OIR rules are not the main driver for research into AIs and NDTs, but they can clearly benefit. The research should therefore include a variety of use cases, not only focusing on technical aspects, but also training for compliance with the regulatory framework and the OIR rules in particular. This will increase the value of AI models, systems and NDTs. A key point in the compliance of AI-driven networks is that the current, often early-day models need to become more predictable (e.g., by reducing the stochasticity in their outputs). The ability to come to more predictable models can be expected to be beneficial for other network use cases as well.
- Another important factor is the actual adoption and roll-out of AI and NDTs by MNOs. Ultimately, each MNO will decide for itself how much freedom to give to AI in its network. This decision will be based on its own business and operational considerations, on de facto and formal standards for

⁶ The proposed Digital Networks Act (DNA) has been under discussion by the European Parliament and the Council at the time of writing of this white paper. Although the proposed DNA contains legal provisions on Open Internet identical to those of the OIR, it is not possible to predict whether and how they may change as a result of the legislative procedure. The progress of the proposed DNA can be monitored at the European Parliament's Legislative Observatory: [https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2026/0013\(COD\)](https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2026/0013(COD)).

AI-driven network functions, experiences and best practices from use case pilots and operational feedback, and the need to comply with the legal and regulatory framework. For NDTs, telcos are likely to have to integrate their in-house DTs of network components (hardware and software) with DTs from different vendors. Interoperability and standardisation of interfaces are crucial to enable such integration and to avoid vendor lock-in.

- A further important factor is the clarity of regulation or, rather, the ability of regulation to be machine absorbable. Laws and regulations usually have a high level of abstraction to encompass a variety of real-life situations and ensure flexibility. This is expected to remain the case in the future. In addition, in some cases the legal situation may not be entirely clear. Some industry players would argue that the discussion on 5G slicing and the OIR is such as case. Both a high level of abstraction and (perceived) ambiguity make it harder to train AI models, as this is best done based on specific and concrete examples. The 'digital by default' principle promoted by the European Commission may help in this regard [32, 33]. This principle of policy and law making means that legislation must be conceived and drafted to be digital-ready, taking into account the existing and emerging technologies. Among other things, this includes drafting clear rules, using simple, precise and concise wording, especially for the implementation parts that can be automated, and introducing experimentation clauses to allow for flexibility in testing new technologies.
- There are also factors that are inherent to the AI and NDT technologies. AI will be trained for compliance based on historical data and on example use cases. With more specific and clear input, the training will be more effective, and the outcomes of the AI will be more precise. However, if new cases are outside the area covered by the use cases in the training, the AI results become less robust as it will need to work from the often high-level of abstraction in the legal frameworks. For NDTs, is important to keep in mind that they are models with inherent limitations in their representation of the reality. They are certainly expected to be useful, but this is always in the context and level of detail of the use cases for which they were created.
- In the assessment of compliance, the above factors come together for both operators and regulators. They both depend on knowledge, inputs and actions from 'the other side': the operators and vendors work on the research and deployment of AI and NDTs, while regulators provide the guidelines and can develop machine absorbable regulation. Here, a constructive interaction is needed to come a proper level of detail of the NDTs (a 'sweet spot') that works for vendors, operators and regulators.

As the development of AI and NDTs progresses over time, both within and outside of FNS, and the experience with the interpretation of the OIR evolves further, the effects of these factors on use of AI and NDTs for OIR compliance will become clearer. As described in section 4.1.3, there is a specific investigation planned in FNS to determine in more detail how an AI agent can be trained by providing the OIR and the BEREC guidelines, in a way that reduces stochasticity in the outputs. It is planned to revisit the analysis and the recommendations in this paper based on the outcomes of this and other research efforts, probably in the form of a follow-up of this white paper.

To promote the effect of AI and NDT as a positive force for greater compliance for MNOs, this white paper closes for now with several recommendations for companies and policymakers.

5.2. Recommendations for companies and researchers

- MNOs and 6G vendors should early on, preferably in the development phase, analyse all legislation that may be applicable to new technologies and explore how to be compliant. On the example of AI and NDTs, compliance goes beyond the area covered by the AI Act (described in an earlier report

[34]). There are many other rules (such as the current European Electronic Communications Code and its Digital Networks Act successor, and the ePrivacy Directive) that must be respected when new technology, services and business models are brought to the EU market. The OIR analysed in this white paper provides only one specific example of such rules.

- MNOs, 6G vendors and researchers should develop and train their AI and develop their DTs with the OIR in mind. Assessment of compliance with the OIR rules is not a main driver for the development of AI and NDTs for 6G networking, as their main aim is on well-known use cases in network planning, optimisation, fault detection and analysis and more. The analysis in this paper shows that there is overlap between the AI, NDTs and data required for these use cases and the OIR compliance use case. AI engineers should work together with compliance and legal experts to establish the training objectives, optimisation parameters and other relevant topics. This helps to achieve compliance early and should reduce the need for costly finetuning or retraining later. As mentioned before, specific research training AI models to comply with the OIR is planned in FNS.
- MNOs, 6G vendors and researchers should use their growing experience in NDTs, telemetry, their deployment and computational demands to determine to what degree they can meet the level detail required by regulators for assessment of OIR compliance. This is a key step in exploring the 'sweet spot' for the level of detail that works for vendors, operators and regulators. It is an important input for a regulatory sandbox (see under the recommendations for policy makers below) that can facilitate a constructive interaction on this level of detail.

5.3. Recommendations for policymakers and regulators

- Policymakers and regulators can encourage the use of AI and NDTs to improve regulatory compliance by providing more clarity in the application of the OIR rules. AI can better learn and abide by instructions that are detailed and precise, illustrated by unambiguous examples and cases. Policymakers have been working on providing such clarity before, independent of AI or NDTs, by providing and updating the BEREC guidelines as a follow-on to the OIR itself. The recently proposed further guidance on 5G network slicing [29] is an example of an input that is suitable to train AI, as it examines specific potential examples of slicing-based service situations, with preliminary remarks on their compliance that are also explained with reference to the BEREC guidelines. Note that such examples are not only helpful for training AI models but also help in general in providing legal certainty. Similar to the examples provided for 5G slicing, there can be examples of benefits of AI-driven resource allocations and distributions when these use cases become apparent and (at least at first sight) appear to raise questions on OIR compliance. Policymakers should develop and publish such examples.
- Policymakers and regulators can assist in determining the role of NDTs in OIR compliance assessment by determining the level of detail in the DT that they find sufficient for their analysis. The set of parameters considered in the 2022 BEREC measurement methodology presents a considerable level of detail, reflecting the views and needs of the regulators at that time. It is recommended to explore, based on the experiences with the methodology since then, whether a smaller set of parameters can also capture the required level of detail. This would help regulators and MNOs looking to use NDTs for their compliance purposes.
- For both points above, policymakers should consider setting up *regulatory sandboxes*. These can help to explore, in a more practical way and with industry involvement, the interaction between existing rules and new technologies (like in the case of the OIR and AI) or between proposed new rules and technology. In a properly defined technical and organisational setting and scope, NDTs and AI can help explore the compliance aspects of products, services or business models, in close

contact with the relevant regulators. This would encourage innovation in situations where both the technology and the interpretation of existing and perhaps new rules is still under development and, at the same time, protect fundamental rights and adhere to basic legal principles.

Annex A. Network and application parameters to be assessed in the context of Open Internet

For a full assessment of Open Internet requirements, a variety of network and application related parameters must be measured and evaluated. BEREC clarifying documents [23] [24] [26, p. Annex 1] contain many parameters that must be considered. In particular, the parameters mentioned in the documents include:

- IAS speed in download and upload (e.g., in bits per second – in browser and app, using TCP over HTTPS),
- Latency (e.g., round trip delay on all platforms, UDP with ICMP or TCP in browser, Android and iOS clients),
- Blocked ports (e.g., incoming and outgoing TCP and UDP port blocking detection on browsers, Android and iOS apps),
- Delay variation,
- Packet loss (e.g., in browser, Android and iOS apps – number of packets to be sent, rate of sending and timeout),
- Availability of connectivity (blocked IP addresses detected in browser, Android and iOS apps),
- DNS manipulation,
- Proxy detection,
- Web browsing performance,
- Video streaming (video start time, number of cuts, average cut time, ratio real-time/video time, delivered bitrate),
- Audio streaming (audio start time, number of stalls, average stall time),
- VoIP quality (Call Setup Success Rate, Call Completion Success Rate, Call Drop Rate),
- Peer-to-peer (number of transferred chunks, number of TCP reset, number of connections),
- Traceroute (number of hops and time needed to reach the measurement peer).

References

- [1] BEREC, “Call for Input for further guidance on 5G network slicing,” 2026. [Online]. Available: <https://www.berec.europa.eu/en/public-consultations-calls-for-inputs/call-for-input-for-further-guidance-on-5g-network-slicing>. [Accessed 1 July 2026].
- [2] BEREC, “Public consultation on the draft BEREC Further Guidance on 5G Network Slicing,” 2026. [Online]. Available: https://www.berec.europa.eu/en/public-consultations-calls-for-inputs/public-consultation-on-the-draft-berec-further-guidance-on-5g-network-slicing?language_content_entity=en.
- [3] J. Soares, “EU’s Digital Networks Act Leaves Big Tech Untouched, Sparks Net Neutrality Concerns,” TechPolicy, 22 January 2026. [Online]. Available: <https://www.techpolicy.press/eus-digital-networks-act-leaves-big-tech-untouched-sparks-net-neutrality-concerns/>. [Accessed 1 July 2026].
- [4] [Online]. Available: <https://futurenetworkservices.nl/en/>.
- [5] ITU, “Draft new Recommendation ITU-R M.[IMT.FRAMEWORK FOR 2030 AND BEYOND] - Framework and overall objectives of the future development of IMT for 2030 and beyond,” 2023. [Online]. Available: <https://www.itu.int/md/R19-SG05-C-0131/en>.
- [6] ITU, “IMT towards 2030 and beyond (IMT-2030),” 2026. [Online]. Available: <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/pages/default.aspx>. [Accessed 1 July 2026].
- [7] 3GPP, “TR 22.870 Study on 6G Use Cases and Service Requirements; Stage 1 (Release 20),” 2026. [Online]. Available: <https://www.3gpp.org/specifications-technologies/releases/release-20>.
- [8] Hexa-X-II, “6G Value, Requirements and Ecosystem - D1.4 Deliverable,” 2025. [Online]. Available: https://hexa-x-ii.eu/wp-content/uploads/2025/05/Hexa-X-II-D1.4_slideset_final.pdf. [Accessed 1 July 2026].
- [9] B. van der Kluit and e. al., “Initial Architecture blueprint, WP2.1, D2.1.1b,” FNS, 2025.
- [10] 3GPP, “Study on 6G Use Cases and Service Requirements, TR 22.870,” 2026. [Online]. Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4374>.
- [11] IETF, “AI-Native Network Protocol (AINP) for Semantic Agent Communication,” 28 May 2026. [Online]. Available: <https://www.ietf.org/archive/id/draft-ainp-protocol-00.html>.
- [12] R. Surapaneni, M. Jha, M. Vakoc and T. Segal, “Announcing the Agent2Agent Protocol (A2A),” GoogleBlog, 9 April 2025. [Online]. Available: <https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/>. [Accessed 1 July 2026].
- [13] Anthropic, “Introducing the Model Context Protocol,” 25 November 2024. [Online]. Available: <https://www.anthropic.com/news/model-context-protocol>. [Accessed 1 July 2026].

- [14] Agentic AI Foundation, "Model Context Protocol," [Online]. Available: <https://aaif.io/projects/model-context-protocol>.
- [15] M. A. Ferrag, A. Lakas and M. Debbah, "6G Needs Agents: Toward Agentic AI-Native Networks for Autonomous Intelligence," 2026. [Online]. Available: <https://doi.org/10.48550/arXiv.2605.01546>. [Accessed 1 July 2026].
- [16] HORIZON-JU-SNS-2026, "Collection, Generation and Validation of Datasets suitable for training AI Models for 6G Networks and for AlaaS," 29 January 2026. [Online]. Available: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/HORIZON-JU-SNS-2026-STREAM-B-01?isExactMatch=true&status=31094501,31094502,31094503&frameworkProgramme=43108390&callIdentifier=HORIZON-JU-SNS-2026&order=DESC>.
- [17] F. Doshi-Velez and B. Kim, "Towards A Rigorous Science of Interpretable Machine Learning," 2017. [Online]. Available: <https://arxiv.org/pdf/1702.08608>. [Accessed 1 July 2026].
- [18] R. Dwivedi, D. Dave, H. Naik, S. Singhal, R. Omer, P. Patel, B. Qian, Z. Wen, T. Shah, G. Morgan and R. Ranjan, "Explainable AI (XAI): Core Ideas, Techniques, and Solutions," *ACM Computing Surveys*, vol. 55, no. 9, pp. 194-227, 2023.
- [19] Nokia, "Nokia Validated Designs (NVD)," [Online]. Available: <https://www.nokia.com/ip-networks/validated-designs/>. [Accessed 1 July 2026].
- [20] M. E. Rajab, L. Yang and A. Shami, "Zero-touch networks: Towards next-generation network automation," *Computer Networks*, vol. 243, 2024.
- [21] ETSI, "Industry Specification Group on Zero touch network and Service Management - ISG ZSM," [Online]. Available: <https://www.etsi.org/technical-groups/zsm/>. [Accessed 1 July 2026].
- [22] P. Nooren, D. N. Keesmaat, A. v. d. Ende and A. Norp, "5G and Net Neutrality: a functional analysis to feed the policy discussion," TNO, 2018.
- [23] BEREC, "Guidelines on the Implementation of the Open Internet Regulation, BoR(22) 81," 2022. [Online]. Available: https://www.berec.europa.eu/sites/default/files/files/document_register_store/2022/6/BoR_%2822%29_81_Update_to_the_BEREC_Guidelines_on_the_Implementation_of_the_Open_Internet_Regulation.pdf.
- [24] BEREC, "Net Neutrality Regulatory Assessment Methodology, BoR(22) 72," 2022. [Online]. Available: <https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/methodologies/berec-net-neutrality-regulatory-assessment-methodology-0>.
- [25] BEREC, "Guidelines detailing Quality of Service Parameters, BoR(24) 42," 2024. [Online]. Available: https://www.berec.europa.eu/system/files/2024-03/BoR%20%2824%29_2042_BEREC%20Guidelines%20on%20QoS.pdf.
- [26] BEREC, "Net Neutrality Measurement Tool, Annex 1, BoR(18) 32," 2018. [Online]. Available: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender->

details/docs/etender/3097/3097_41876_EN-
BEREC%202018%2001%20OT_Tender%20Specification.docx_ENG_V1.pdf.

- [27] BEREC, "Traffic Management," [Online]. Available: https://www.berec.europa.eu/en/all-topics/traffic-management?language_content_entity=en. [Accessed 1 July 2026].
- [28] BEREC, "Public consultation on the draft BEREC Further Guidance on 5G Network Slicing," 2026. [Online]. Available: https://www.berec.europa.eu/en/public-consultations-calls-for-inputs/public-consultation-on-the-draft-berec-further-guidance-on-5g-network-slicing?language_content_entity=en.
- [29] BEREC, "Draft Further Guidance on 5G Network Slicing Annex to the BEREC Guidelines on the implementation of the Open Internet Regulation BoR (26) 84," 2026.
- [30] F. G. Vogt, V. H. S. Lopes, F. Rodriguez, M. C. Luizelli, C. Papagianni and C. Rothenberg, "The GhostTwin: Towards Live Digital Twins via SmartNIC Network Emulation," in *ACM SIGCOMM Posters and Demos '25: Proceedings of the ACM SIGCOMM 2025 Posters and Demos*, 2025.
- [31] Council of the European Union, "Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age," 16 November 2020. [Online]. Available: <https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/en/pdf>.
- [32] European Commission, "Digital-ready Policymaking," [Online]. Available: <https://interoperable-europe.ec.europa.eu/collection/digital-ready-policymaking/digital-ready-policies>.
- [33] European Commission, "Better Regulation Toolbox: TOOL #28. Digital-ready policymaking," [Online]. Available: https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en.
- [34] O. Batura and P. Nooren, "The relevance of the AI Act to 6G: The Safety Component," Future Network Services, 11 December 2024.
- [35] M. Altinas, I. Duru, I. Yazici, S. N. Karahan and S. Cimen, "Artificial Intelligence Agents Shaping the Next Generation 6G Network Systems," January 2026. [Online]. Available: <https://doi.org/10.1109/ACCESS.2026.3667803>. [Accessed 1 July 2026].

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van Future Network Services.