



# The relevance of the AI Act to 6G: The Safety Component

*White paper*

## Document properties

<b>Document title</b>	<b>The relevance of the AI Act to 6G: The Safety Component</b>
<b>Authors</b>	<b>Olga Batura, Pieter Nooren</b>
<b>Reviewer</b>	<b>David Regeczi</b>
<b>Dissemination level</b>	<b>Public</b>
<b>Status of the document</b>	<b>Final</b>
<b>Version</b>	<b>1.0</b>
<b>Work Package</b>	<b>WP4.5 Technology-Policy Co-Development</b>
<b>Deliverable</b>	<b>Part of FNS Milestone M4.5.1</b>
<b>Contractual delivery date</b>	<b>December 2024</b>
<b>Delivery date</b>	<b>11 December 2024</b>
<b>File name</b>	<b>FNS6G_20241211_AI_Act_6G_Safety_Component_v1.0</b>

# Table of contents

- 1. Arguments in brief ..... 4
  
- 2. Detailed analysis of the AI Act provisions on AI systems as safety components ..... 5
  - 2.1. Scope of application of the AI Act to 6G networks ..... 5
    - 2.1.1. Generative AI in 6G networks ..... 6
    - 2.1.2. High-risk uses of AI systems in 6G networks..... 6
  - 2.2. In search of a safety component in 6G ..... 8
    - 2.2.1. In radio equipment..... 8
    - 2.2.2. In critical digital infrastructure such as 6G networks ..... 9
    - 2.2.3. Exemption of high-risk AI system used as a safety component in critical digital infrastructure ..... 11



# 1. Arguments in brief

The Future Network Services (FNS) project has started analysing the relevance of the EU legislation on artificial intelligence (AI) for the future 6G networks. This first analytical paper demonstrates that the **rules of the AI Act on high-risk uses of AI systems are likely to have limited impact on the development of 6G networks**. It also notes that the legal certainty for R&D actors active in the field of AI can be improved by providing further legal guidance at specific points. This paper examines these points in detail with the aim to assist legislators in formulating guidance where they deem appropriate. R&D developers should remain mindful of potential AI Act requirements and pay attention to potential further clarifications coming from the legislators.

The AI Act rules on high-risk uses of AI systems capture only a few of the intended uses of AI for 6G. One relevant use is as a safety component. However, **the notion of a safety component seems to differ depending on the context of use**, namely in critical digital infrastructure (for example, an entire 6G network) or in radio equipment used to build a 6G network:

- A safety component in critical digital infrastructure must directly protect the physical integrity of critical infrastructure or the health and safety of persons and property but is not necessary in order for the system to function. This indicates that a safety component cannot simultaneously fulfil other non-safety functions (e.g. network management). According to the AI Act, AI systems used solely for cybersecurity purposes are not safety components. Under the current understanding of the design and engineering of mobile networks, a safety component as defined by the AI Act is unlikely to exist in 6G networks.
- For radio equipment used in mobile networks, including future 6G networks, the use of AI systems as safety components is more probable. However, by contrast to the use in critical digital infrastructure, the notion of a safety component for radio equipment may be interpreted as fulfilling only a cybersecurity function.

Another relevant point is the **possible exemption of an AI system as a safety component in critical digital infrastructure from the AI Act**. The AI Act provides for such an opportunity, but none of the exempting conditions seem to apply in the context of 6G which introduces a degree of uncertainty for R&D actors.

To ensure stable progress in AI R&D for 6G, it would be helpful to have **more guidance and clarifications from the legislators** on the points mentioned above. This could take the form of guidelines from the European Commission and the AI Office illustrating the application of the relevant AI Act's provisions.

For the successful take-up of 6G technology, it is important that its development is well aligned with existing and future policies and legislations. This is the motivation for including research on policy-technology co-development in the FNS work on the 6G ecosystem, with AI as one of the key topics. For the creation of new economic earning power in the Netherlands around 6G, it is key to provide 6G and AI developers with early insights into the relevant AI legislation.

The sections below present the analysis of the relevant AI Act provisions on high-risk use of AI systems as safety components in the context of 6G in more detail.

## 2. Detailed analysis of the AI Act provisions on AI systems as safety components

Before turning to the in-depth analysis of the AI Act provisions on “safety component”, Section 2.1. discusses the scope of application of the AI Act in relation to 6G. This section also introduces main notions and definitions relevant for the further analysis.

### 2.1. Scope of application of the AI Act to 6G networks

The AI Act<sup>1</sup> applies to all AI systems that are placed on the market or put into service in the EU, independent of the location of the AI provider. Although the definition of an AI system is complex,<sup>2</sup> the following main characteristics are essential. AI systems:

- Run on machines,
- Infer output from the input data,
- Are based on machine-learning, logic- or knowledge-based approaches,
- Have some degree of independence from human involvement,
- Possess the ability to self-learn, and
- Are not a purely rule-based system (i.e. are not if-then systems).

The AI Act also applies to general-purpose AI models (GPAI models) placed on the market in the EU. These are defined as AI models that “display significant generality” and are “capable of performing a wide range of distinct tasks”.<sup>3</sup> GPAI models can be integrated in different AI systems (i.e. either in AI systems for specific purposes or in general-purpose AI systems).

The definitions of both AI systems and GPAI models in the AI Act are broad enough to assume that the complex AI required for 6G networks would satisfy these definitions.

Within this assumption, the application of the AI Act may be triggered by:

- 1) The type of AI developed and used in 6G networks. The example of this is GPAI and more specifically generative AI as a concrete example of it; or
- 2) The type of AI use in 6G networks, i.e. in what situation and function AI is used.

---

<sup>1</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12.7.2024.

<sup>2</sup> Article 3 (1) AI Act contains the following definition of an AI system: “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”.

<sup>3</sup> Article 3 (63) AI Act defines a GPAI model as “an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market”.

Below both situations are discussed.

### 2.1.1. Generative AI in 6G networks

One of the types of AI that can be [used by 6G networks is generative AI](#). Generative AI as such is not regulated by the AI Act. However, large generative AI models are mentioned<sup>4</sup> as an example of GPAI models, which are regulated by the AI Act.

GPAI models (and not GPAI systems<sup>5</sup>) are regulated only if they are made available on the EU market. “Making available on the market” means supplying for distribution or use. This means that a generative AI model will be subject to the requirements of the AI Act when it is first offered on the EU market for further development and integration into AI systems. If the GPAI model provider does not place it on the market but uses it by itself to develop an AI system or integrates it into an AI system, such a GPAI model is subject to the AI Act.<sup>6</sup> However, if a 6G provider develops and uses a generative AI model by itself for R&D, it is not subject to the GPAI-related requirements of the AI Act. If a 6G provider buys a GPAI model or an AI system using such a GPAI model, the 6G provider also is not subject to GPAI-related requirements of the AI Act. The original provider (i.e. the seller) of the GPAI model is the responsible one in this context.

GPAI models have a potential to be widely used in 6G networks. However, at the moment specific realistic use cases are not clearly defined. At FNS, research is ongoing into use cases of GPAI models in 6G context. FNS policy work package will also address this issue in its future deliverable(s) and explore the AI Act provisions relevant to generative AI (i.e. GPAI models) to support and steer R&D.

### 2.1.2. High-risk uses of AI systems in 6G networks

The AI Act mainly focuses on those uses of AI systems (both GPAI systems and narrow-purpose AI systems) that are considered high risk.<sup>7</sup> All categories of high-risk uses of AI systems can be placed in two groups:

- 1) Those that function as a safety component of an already regulated product (i.e. product that is subject to a third-party conformity assessment before putting it on the EU market) or AI systems that are themselves such a regulated product,<sup>8</sup> and
- 2) Those that pose significant risk of harm for health, safety, or fundamental rights of natural persons.<sup>9</sup>

---

<sup>4</sup> See Recitals 99 and 105 AI Act.

<sup>5</sup> We note that GPAI systems are within the scope of application of the AI Act if two conditions are fulfilled cumulatively: if they are placed in use or on the market in the EU and if they are qualified as high risk under Article 6 AI Act.

<sup>6</sup> Recital 97 AI Act. We note that using a GPAI model to develop an AI system can also be considered as usage for purposes of research, developing and prototyping, which is excluded from the requirements of the AI Act by Article 2 (6) AI Act.

<sup>7</sup> Article 5 AI Act also prohibits certain practices involving the use of AI systems. However, none of these practices (uses) is relevant for the functioning of 6G networks.

<sup>8</sup> By this point we mean all AI systems falling under Article 6 (1) in conjunction with Annex I AI Act.

<sup>9</sup> This covers all AI systems falling under Article 6 (2) in conjunction with Annex III AI Act.

The first group consists of only one use (i.e. safety component) in a variety of products that are listed in Annex I AI Act. The common characteristic of these products is that they represent risky products in terms of health and safety harm and are, therefore, subject to harmonised regulation in the EU. Before they are put on the EU market, all these products must undergo a conformity assessment with special (harmonised) standards<sup>10</sup> and receive a CE marking.<sup>11</sup> Among the listed products (e.g. toys, lifts, medical devices, various land, water and airborne vehicles) only one is of relevance for 6G networks, namely radio equipment.

Radio equipment is any “electrical or electronic product that emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination”.<sup>12</sup> It goes without saying that wireless 6G networks will use various radio equipment. Therefore, if AI is used as a safety component in radio equipment and that radio equipment must undergo a third-party conformity assessment, this AI system will be considered high risk and subject to the specific requirements of Chapter 3, Sections 2 and 3, AI Act.<sup>13</sup>

The second group lists uses that can present risk to health, safety and fundamental rights. Only one use on this list is relevant for a 6G network: the use of AI systems as a safety component in critical digital infrastructure. 6G networks will be considered critical digital infrastructure according to the NIS-2 Directive.<sup>14</sup> Critical digital infrastructure includes publicly available electronic communications networks and services and others listed in Annex I NIS-2 Directive. According to Annex III (2) AI Act, in the case of critical digital infrastructure, an AI system is considered high risk if it is used as a safety component in management and operation of such infrastructure.

From the above, it follows that in the context of AI use in 6G networks, the notion of a safety component is central. Both for radio equipment and for the networks themselves, it is important to understand what a safety component is. If an AI system is used to automate this safety component, such an AI system is subject to additional requirements of the AI Act. Whether the AI system is general-purpose or not is irrelevant for this set of requirements, it is only important that AI fulfils a function of a safety component.

---

<sup>10</sup> In 2023, the European Commission issued a mandate to the European Standardisation Organisations (e.g. CEN/CENELEC) to develop a standard covering a number of subjects related to the requirements for high-risk AI systems. The subjects to be covered correspond to the requirements to high-risk AI systems in Articles 8-15 AI Act. Once adopted, the harmonised standard will become mandatory for the EU market. See Commission Implementing Decision of 22.5.2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence - [Standardisation request M/593](#).

<sup>11</sup> CE marking is a mark by which the manufacturer indicates that the product is in conformity with the applicable requirements of the EU harmonisation legislation for a specific product (in the case of high-risk AI systems – the AI Act). See, in particular, Articles 3 (24) and 48 AI Act.

<sup>12</sup> Article 2 (1) Nr. 1 of the Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive, RED), OJ L 153 22.5.2014.

<sup>13</sup> More specifically, Articles 8 – 15 AI Act are always applicable to high risk AI systems, but depending on who puts them on the market, some of the requirements of Articles 16 – 27 AI Act are additionally applicable.

<sup>14</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 333 27.12.2022.

If such an AI system is a simple rule-based system (i.e. an if-then algorithm), it is excluded from the scope of the AI Act.

## 2.2. In search of a safety component in 6G

A safety component is defined by the AI Act as a “component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property” (Article 3 (14) AI Act). As explained in Section 2.1.2., an AI system that is a safety component is high risk when it is present in radio equipment or in the critical digital infrastructure. In the context of 6G, we need to consider both situations because radio equipment may be an element of critical digital infrastructure, like electronic communications networks and services.<sup>15</sup> The fact that electronic communications networks and services contain or rely on radio equipment means that an AI system as a safety component may be present twice. There may be a safety component in the radio equipment that is an element of the network, and there may also be a safety component for the network as a whole. One can also envisage an AI system consisting of AI-components, where safety components of radio equipment in the mobile network jointly amount to a safety component of the whole network. Therefore, there is a chance that the safety component of the radio equipment is simultaneously a safety component of a mobile network, which would mean that one and the same safety component must be assessed for conformity twice, possibly by different organisations (such as, in the case of mobile networks, a third party on behalf of a radio equipment vendor and a network operator).

### 2.2.1. In radio equipment

The Radio Equipment Directive (RED)<sup>16</sup> is one of the main legislations on radio equipment and contains requirements and processes for admitting such equipment to the EU market. For years, this Directive focused on safety of radio equipment, which was understood as “protection of health and safety of persons and of domestic animals and the protection of property”.<sup>17</sup> This understanding of safety is similar to that in the AI Act.

However, recently, the European Commission adopted a Delegated Regulation 2022/30<sup>18</sup> that interpreted the essential requirements of Article 3 (3) (d)-(f) RED in a broader manner equating them to cybersecurity. The said Delegated Regulation applies to “internet-connected radio equipment” which is understood as

---

<sup>15</sup> An electronic communications network is a transmission system which may have switching or routing equipment, network elements that permit conveyance of electromagnetic signals by radio or other electromagnetic means. An electronic communications service is a service of transmission of content over electronic communications networks. While such services are intangible, they may use radio equipment (e.g. mobile phones) in the service delivery and reception. See Article 2 (1) and (4) of the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018.

<sup>16</sup> Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive, RED), OJ L 153 22.5.2014.

<sup>17</sup> See, for instance, Recitals 4, 26 and 46 and Article 3 (1) RED. Also see the most recent [Guide to the Radio Equipment Directive 2014/53/EU](#), Version of 19 December 2018.

<sup>18</sup> Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive, OJ L 7, 12.01.2022.



radio equipment that can directly or via other equipment communicate itself over the internet. Certain radio equipment used in 6G networks can be considered internet-connected radio equipment. The Delegated Regulation requires that internet-connected radio equipment, among other things, does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service; incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; and supports features ensuring protection from fraud. All these essential requirements relate to cybersecurity and not safety.

Against this backdrop, a contradiction with the requirements of the AI Act emerges as Article 3 (14) AI Act and its accompanying Recitals clearly relate only to safety of persons and property. While AI Act sees a safety component as fulfilling a safety function and excludes components fulfilling only cybersecurity function, the RED understands safety for internet-connected radio equipment in some instances as only cybersecurity. If the view on safety of the RED is accepted for safety components that are AI systems in radio equipment, this may lead to the contradiction of the understanding of the term “safety component” within the AI Act not only in relation to 6G but also more broadly.

It needs to be considered how this contradiction will play out in practice where the critical digital infrastructure (6G network) consists of or relies on radio equipment as its elements. For example, when an AI system is used as a safety component in an antenna, it needs to be assessed when it is put on the market or in use. If this antenna is then integrated in a 6G network and the AI system of the antenna becomes a safety component for the network, the AI system as part of the given 6G network must be assessed again. Hence, it may be possible that one and the same element is assessed twice and differently depending on whether it is already integrated in the network or not. At the same time, it must be ensured that the standards under the RED and AI Act are fully aligned. This question is not trivial because the conformity assessment for a safety component in radio equipment must be performed by a third party, but for critical digital infrastructure the AI provider itself performs the conformity assessment.

## 2.2.2. In critical digital infrastructure such as 6G networks

In the context of critical digital infrastructure, Recital 55 AI Act provides more explanations on what the term “safety component” means. A safety component in critical infrastructure is a system used to directly<sup>19</sup> protect the physical integrity of critical infrastructure or the health and safety of persons and property but which are not necessary in order for the system to function. It is further explained that failure or malfunctioning of such components might directly lead to risks to the physical integrity of critical infrastructure and thus to risks to health and safety of persons and property. Recital 55 AI Act specifies that components intended solely for cybersecurity are explicitly excluded from the definition of safety components.

---

<sup>19</sup> We note that the term “directly” in Recital 55 AI Act needs further clarification as it may become central for the understanding of safety component. The current wording does not make it clear whether the term points to direct causality between malfunctioning and harm or whether the reach is broader and covers indirectly caused harm. In the latter case, the question emerges where the line should be drawn on such indirect causality. The clarification of this terminology would contribute to the better understanding of the scope of application of the AI Act vis-à-vis other relevant legislations, such as the NIS-2 Directive and Critical Entities Resilience Directive.

These explanations raise three concerns. Firstly, Recital 55 seems to suggest that AI systems that serve both safety and cybersecurity should be treated as safety components and therefore as high-risk systems. Secondly, there may be a contradiction with the understanding of the safety component for radio equipment (as discussed in Section 2.2.1). Thirdly, the explicit exclusion of components intended only for cybersecurity is made only in the context of critical digital infrastructure and not for other types of safety components (e.g. in cars, planes, elevators and others).<sup>20</sup> All this leads to the confusion about the understanding of the term “safety component” within the AI Act and is likely to cause legal uncertainty of AI providers.

The presence of a safety component within critical digital infrastructure that is a mobile network is questionable. A mobile network and services as such cannot be regarded as presenting a safety risk to health of persons or to property.<sup>21</sup> Only a few elements of a mobile network (i.e. radio equipment, like terminals and antennas) have the potential to cause damage to persons through emission of electromagnetic fields. However, this can only happen under certain conditions, which are guarded against by preventive measures. Such measures include exposure standards for radiofrequency energy that were developed to set permissible thresholds with additional safety margins. All radio equipment marketed in the EU must undergo conformity assessment, which is the responsibility of the equipment supplier. Furthermore, when deployed in a mobile network, there are limitations on the power emitted by the combination of the radio equipment and other components (such as antennas). Finally, the combined radio emissions from (typically multiple) mobile networks and other radio sources have to comply with the established [exposure limits to electromagnetic fields](#). These last two are the responsibility of the mobile network operator. Current terminals (antennas) have built-in relevant safety mechanisms. For example, terminals (such as smart phones) can have proximity sensors to determine whether or not the terminal is operated close to a human being and reduce output power or used bandwidth over time when they otherwise would not comply with the set exposure limit. It needs to be reminded that, as discussed in Section 2.2.1., this radio equipment needs to be assessed not just individually, but also as a part of the network. The context and configurations may be different there because a network is likely bigger than a simple sum of all components.

Against this background, the question can be raised whether safety mechanisms in terminals may be automated by using AI systems in the future 6G network, especially with new radio concepts such as beam steering and reconfigurable intelligent surfaces. For example, AI could be used to predict the amount of transmitted energy still available to comply with exposure limits and optimise the transmissions (output power, amount of data, scheduling of transmissions) to stay within the required limits. AI systems could also be used to intelligently configure the output power, active antenna system beam directions or downlink transmissions to stay within the required exposure limits. AI systems could provide the best suited approach to optimise the use of the radio resources based on new 6G technology

---

<sup>20</sup> We note that some of these products are likely to be considered “internet-connected radio equipment” in the scope of the Delegated Regulation and the RED. Nonetheless, this does not eliminate the contradiction in the understanding of safety component under the AI Act (and in the EU legislation related to safety more generally).

<sup>21</sup> Electricity supply to the mobile network is not part of this network, but part of the energy infrastructure.

and at the same time guarantee compliance with the exposure limits. It shall be noted that at the current stage of R&D, there is no such AI in trial or operation.

Whether such AI systems in 6G networks can be considered safety components in the sense of the AI Act is a moot point. According to Recital 55 AI Act, safety components in critical digital infrastructure are necessary only for safety, but not for the system to function. Hence, the AI system that is safety component would need to be separate from the network management AI system, which the theoretical scenarios described above seem to suggest. In addition, it remains to be seen whether the AI as described in scenarios would not be a more simple rule-based algorithm of the if-then kind, which would exempt it from the scope of the AI Act.

In general, the notion of a safety component is alien to mobile networks and services. It seems to be more suited for other critical infrastructure, like energy and water supply. It is also notable that the wording of the AI Act on safety component closely resembles the wording of the Machinery Regulation<sup>22</sup> on the same subject. The Machinery Regulation could be considered for better understanding of “safety component” because it applies, among other things, to robots and software used in them. Safety component is in the centre of the scope of application as per Article 1 of the Machinery Regulation. Because of this, the Machinery Regulation provides more definitions and explanations on safety component. In particular, Article 3 (4) of the Machinery Regulation defines what is the safety function, which a safety component is supposed to perform: “Safety function means a function that serves to fulfil a protective measure designed to eliminate, or, if that is not possible, to reduce, a risk, which, if it fails, could result in an increase of that risk”. Annex II of the Machinery Regulation contains an indicative list of safety components. These include:

- Protective devices designed to detect the presence of persons,
- Logic units to ensure safety functions,
- Discharging systems to prevent the build-up of potentially dangerous electrostatic charges,
- Energy limiters and relief devices,
- Software ensuring safety functions,
- Safety components with fully or partially self-evolving behaviour using machine learning approaches ensuring safety functions.

As becomes clear from the explanations and examples in the Machinery Regulation, similar safety components or elements are unlikely to exist in mobile networks. However, it is also possible that the Machinery Regulation and the AI Act will use different interpretations of the same term.

### **2.2.3. Exemption of high-risk AI system used as a safety component in critical digital infrastructure**

The AI Act foresees that AI systems that pose significant risk of harm for health, safety, or fundamental rights of natural persons may not be considered high risk under certain conditions. Such exemption

---

<sup>22</sup> Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC, OJ L 165, 29.06.2023.

applies only to an AI system that is a safety component in critical digital infrastructure, but not to AI system that is a safety component in radio equipment.<sup>23</sup>

Article 6 (3) AI Act stipulates that an AI system that is a safety component in critical digital infrastructure is not high risk if any of the following conditions are fulfilled:

- a) the AI system is intended to perform a narrow procedural task;
- b) the AI system is intended to improve the result of a previously completed human activity;
- c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
- d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

Even if we assume that an AI system can be used in 6G networks as a safety component, it is difficult to imagine how any of these exempting conditions could apply to it. Conditions (b), (c) and (d) listed above are not applicable to 6G networks because, due to the high speed of data transmission, real-time decision making across multitude of bands and channels, human involvement is impossible and AI actions are instant and not preparatory. With regard to condition (a), the notion of a “narrow procedural task” in the context of a safety component in 6G is impervious. The explanations given in Recital 53 AI Act are nonsensical for mobile networks and for the safety component.

Therefore, clarification from the legislator is necessary on how the exempting criteria apply to AI systems used as safety components in critical digital infrastructure. In its current form, provisions of Article 6 (3) accompanied by Recital 53 AI Act undermine legal certainty for companies working on R&D of AI in 6G as they may be entitled to an exemption but cannot rely on it due to it being immaterial in 6G context.

---

<sup>23</sup> See Article 6 (3) AI Act.

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.