CONSOLIDATED LEGISLATION

Royal Decree-Law 7/2022 of 29 March on requirements to ensure the security of fifth generation electronic communications networks and services.

Head of State
"BOE" no. 76, of 30 March 2022
Reference: BOE-A-2022-4973

CONTENTS

(Consolidated text)
Latest amendment: without modifications

Since their widespread introduction in the late 1990s, mobile networks have been a pillar of the progress of telecommunications and a basis for the introduction of information technologies in all areas of society, thanks both to the gradual extension of their coverage and, most essentially, to the development of new capabilities that have been incorporated by successive generations of mobile services.

The most recent of these, known as fifth generation or 5G, can give mobile and wireless communications a new dimension by integrating computing into the network, enabling virtual networks, offering low latency and providing services of enormous added value to society in areas such as medicine, transport and energy. For this reason, the European Union and Spain are promoting the rapid deployment of networks and the implementation of projects demonstrating their usefulness for different sectors.

The provision of advanced services to the population and industry supported by technology will become a reality over the next five or ten years. However, in order for 5G networks to develop their potential, it is necessary to generate the necessary confidence in their continued operation and in their protection against leaks or manipulations of data or communications. Without that trust, individuals and entities that can seize the opportunities offered by 5G networks will not make use of them, and 5G technology will not produce the expected benefits of it.

5G networks have comparative advantages in security over previous generations. But they also present specific risks arising, for example, from their more complex network architecture, open and disaggregated, and their ability to transport huge volumes of information and allow the simultaneous interaction of multiple people and things. Their interconnection with other networks and the transnational nature of many of the threats have an impact on their security, and the foreseeable widespread use of these networks for functions essential to the economy and society will increase the potential impact of the security incidents they suffer.

Hardware and software are of particular importance in 5G networks as their characteristic features, such as edge computing or multiple network slicing, are oriented towards paradigms specific to computing and cloud computing services, moving away from the traditional approach to electronic communications network architectures. The operation of these networks will depend to a large extent on IT systems and services provided by third-party providers to operators (collectively referred to in this royal decree-law as “providers”), creating a dependency on them which could increase the level of risk to which they are exposed.

The architecture of the 5G networks described above and the new security requirements entail the necessary evolution of traditional strategies, which were based on ensuring their availability, confidentiality and integrity against attacks from outside.

The technical complexity and the new technological paradigm implied by the inclusion and generalisation of the telecommunications market and in many other economic sectors of 5G technology means that the security challenges around 5G networks cannot be fully addressed with the rules on security and integrity of electronic communications networks contained in Law 9/2014 of 9 May 2014, General Telecommunications, nor with Royal Decree-Law 12/2018 of 7 September 2018 on the security of networks and information systems, nor with Law 8/2011, of 28 April 2011, which establishes measures for the protection of critical infrastructures.

The regulated matter requires a legislative decree, as it establishes some obligations for companies and administrative powers that must be established by law. These limitations and powers justify the importance for society of ensuring the regular functioning of essential services that could depend on 5G networks and services in the future. The opening of the network to a multitude of uses and applications increases the points of attack to the network, and the importance of the role of suppliers in its architecture and management advises to take precautions to avoid possible incidents attributable to their performance.

In this respect, suppliers are subject to strict security controls to ensure their technical reliability and independence from external interference, leading to risk analysis and measures to be carried out by operators and the Government.

On the technical side, the application of international and European standards and European certification schemes resulting from the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on Cybersecurity is given precedence. In addition, operators should put in place a supplier diversification strategy to minimise the risks and impact of contingencies affecting them.

In the strategic area, the risk profile of the most important suppliers of 5G network and service operators in Spain will be examined, in particular from the point of view of their protection against attacks and their exposure to external interference;even identifying specific users or restricted functions of networks where qualified suppliers cannot act as high risk or medium risk may be identified.

To create them and strengthen the 5G industry in Spain, research, development and innovation will be promoted around 5G technology, including 5G cybersecurity.

This royal decree-law establishes special or additional rules to those existing in other applicable security laws, including Law 9/2014 of 9 May 2014, General Telecommunications Law, Law 8/2011 of 28 April 2011 establishing measures for the protection of critical infrastructures, Law 36/2015 of 28 September 2015 on national security, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Regulation on the protection of personal data), the Organic Law 3/2018 of 5 December 2018 on the protection of personal data and the guarantee of digital rights or Royal Decree-Law 12/2018 of 7 September 2018 on network security and information systems.

In drafting this law, the European Commission’s Recommendation (EU) 2019/534 of 26 March 2019 of the European Commission on cybersecurity of 5G networks, coordinated risk analysis of Member States and the ‘toolbox’ agreed by Member States as a common basis for the secure development of 5G technology in Europe has been taken into account. This Royal Decree-Law includes the key recommendations of the European Commission's Communication of 29 January 2020 "Secure Deployment of 5G in the EU -Implementation of the EU Toolbox” (COM/2020/50 final) to Member States on the use of the ‘toolbox’.

Article 86 from the Constitution allows the Government to dictate decrees-laws ‘in cases of extraordinary and urgent necessity’, provided that they do not affect the organisation of the basic institutions of the State, the rights, duties and liberties of the citizens regulated in the title I of the Constitution, to the regime of the Communities Autonomous or general electoral law.

The Constitutional Court has declared that the situation of extraordinary and urgent necessity required, as an enabling premise, by Article 86(1) of the Spanish Constitution, can be deduced "from a plurality of elements", including "those reflected in the statement of reasons for the law" (STC 6/1983, 4 February 1983),

In this sense, STC 61/2018, of 7 June 2018 (FJ 4), requires, on the one hand, "the explicit and reasoned presentation of the reasons that have been taken into account by the Government for its approval", and on the other, "the existence of a necessary connection between the emergency situation defined and the specific measure adopted to remedy it".

In any case, the Constitutional Court requires for the use of this type of rule that the situation to be regulated be in line with the "political or opportune judgement that corresponds to the Government" (STC 182/1997, 30 October 1997).

Therefore, in accordance with the jurisprudence of the Constitutional Court, the reasons that justify the extraordinary and urgent need to incorporate into Spanish law, by means of a Royal Decree-Law, the recommendations contained in the European Union's "toolbox" on 5G cybersecurity, through the approval of this Royal Decree-Law on requirements to guarantee the security of fifth generation electronic communications networks and services, are set out below.

On 24 February 2022, Russian armed forces launched a full-scale aggression against Ukraine from Russia, from Belarus and from areas not controlled by the Ukrainian Government. As a result, significant areas of Ukrainian territory have become zones of armed conflict.

The European Council condemned in the strongest terms in its conclusions of 24 February 2022 Russia's military aggression against Ukraine and stressed that it is a serious violation of international law and the principles of the UN Charter. The European Council demanded that Russia fully respect the territorial integrity, sovereignty and independence of Ukraine within its internationally recognised borders, including Ukraine's right to choose its own destiny. In solidarity with Ukraine, the European Council agreed additional sanctions, called for further work on preparedness at all levels and invited the European Commission to come forward with emergency measures.

As a consequence, the conflict is having major implications for the European Union, including a significant increase in the risk of geo-strategically motivated cyber-attacks, which was already referred to in the 'Threat Landscape 2021' report published by the European Union Agency for Cybersecurity (ENISA) in October 2021.

On 14 January, 15 February and 23 February 2022, cyber-attacks were reported that severely affected government and banking services in Ukraine. Furthermore, in recent weeks, several alerts have been received from the US Cybersecurity and Infrastructure Agency (CISA), highlighting the need to strengthen the protection of European countries against potential cyberthreats.

Consequently, taking into account the international conflict situation derived from the aggression against Ukraine and the high risk of cyber-attacks against 5G networks and services already deployed in our country or with deployment planned for the coming months, within the "political or opportunity judgement" which, in accordance with the aforementioned STC 182/1997, of 30 October, corresponds to the Government, it is considered that the reasons of extraordinary and urgent need referred to in Article 86 of the Spanish Constitution for the processing of this bill as a Royal Decree-Law are met.

This will guarantee the rapid entry into force of those measures that make it possible to prohibit or limit the activity in the market of suppliers that have been considered high or medium risk by the government, based on technical criteria and strategic aspects that may have an impact on security, such as the level of exposure to interference from third countries, with the possibility of identifying specific users or restricted functions of the networks where these suppliers classified as high or medium risk cannot operate.

In conclusion, it is considered that the significant increase in the risk of cyber-attacks against 5G networks deployed or about to be deployed in our country justifies the extraordinary and urgent need to adopt measures as soon as possible that, in accordance with the provisions of the aforementioned toolbox, guarantee the cybersecurity of 5G technology and the reinforcement of the European Union's technological autonomy and sovereignty.

The approval of the so-called "5G Cybersecurity Law" (with which this Royal Decree-Law is identified) is included as one of the reforms (Reform C15R2) of Component 15 of the Recovery, Transformation and Resilience Plan dedicated to "Digital connectivity, boosting cybersecurity and 5G deployment", with "the entry into force of the 5G Cybersecurity Law" being specifically foreseen as Milestone CID 235.

The principle of necessity is respected as this royal decree-law is enacted to ensure good of general interest, such as security and confidence in electronic communications;it complies with the principle of proportionality as the measures are appropriate to the risks identified in each case;it complies with the principle of legal certainty because the existing regulatory framework on security is recognised and only appropriate requirements and controls are added to the uniqueness of 5G networks and services and their risks. The principle of transparency is respected since the interested parties have been able to participate in the procedure for drafting this law. Finally, it complies with the principle of efficiency as administrative burdens have been limited to the minimum necessary to achieve the desired aim of safety.

By virtue thereof, making use of the authorisation contained in Article 86 of the Spanish Constitution, at the proposal of the Minister for Economic Affairs and Digital Transformation, and following deliberation by the Council of Ministers at its meeting of 29 March 2022,

THE FOLLOWING IS DECREED:

CHAPTER I
General provisions

Article 1. *Object.*

This royal decree-law establishes security requirements for the installation, deployment and operation of electronic communications networks and the provision of electronic and wireless communications services based on fifth generation (5G) technology.

Article 2. *Objectives.*

This royal decree-law pursues the following objectives:

a) Drive end-to-end security of the ecosystem generated by 5G technology.
b) Strengthen security in the installation and operation of 5G electronic communications networks and in the provision of mobile and wireless communications services that rely on 5G networks.
c) Promote a sufficiently diversified supplier market in 5G electronic communications networks and services in order to ensure security based on technical, strategic and operational reasons and to avoid, for these reasons, the presence of suppliers with a high risk or medium risk rating in certain network elements or areas.
d) Strengthen the protection of national security.
e) Strengthen industry and foster national R&D and innovation activities in cybersecurity related to 5G technology.

Article 3. *Definitions.*

1. For the purposes of this Royal Decree-Law, the following definitions shall apply:

a) "5G operator": a natural or legal person that installs, deploys or operates 5G public networks or provides publicly available 5G services over, in whole or in part, 5G networks, whether or not it has its own 5G network, and has notified the Operator Registry of the commencement of its activity or is registered in the Operator Registry.
b) “5G networks” or “5G-based networks”: the integrated set of network elements or infrastructure, whether hardware or software, transmission systems, switching or routing equipment and other facilities, including associated facilities and digital infrastructure, that enable the transport of signals to provide mobile and wireless connectivity and, through it, to provide electronic and wireless communications services to users and enterprises with advanced features, incorporating the functions and capabilities and meeting the use cases in Recommendation ITU-R M.2083, of the International Telecommunication Union, or in the technical standard of the 3GPP organisation (*3rd Generation Partnership Project*: Third Generation Collaboration Project).

These advanced features include, inter alia, grid-embedded computing, high speed transmission of large volumes of data, minimal latency in communications, high reliability and the ability to connect a massive number of devices to the network, or the provision of specific services for specific uses or applications.

All network elements, infrastructure, facilities and network functions used to provide services with the above capabilities are considered to be part of 5G networks, even if they are also used in electronic communications networks and services of previous mobile generations.

c) “Risk”: any reasonably identifiable circumstance or fact that has a potential adverse effect on the security of 5G networks and services.
d) “Security”: the capacity of 5G networks and services to resist, with a given level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of said networks and services, of the data stored, processed or transmitted, or of the accessible services through them.
e) “5G Services”: electronic and wireless communications services, as defined in Directive 2018/1972 of 11 December 2018 of the European Parliament and of the Council establishing the European Electronic Communications Code, their associated services and other related services aimed at providing functionalities and operability to the above, such as cloud computing or edge computing, the provision of which uses 5G networks.
f) "5G supplier": the manufacturer, authorised representative, importer, distributor, logistics service provider or any other natural or legal person subject to obligations in connection with the manufacture of products, their placing on the market or putting into service of telecommunications equipment, suppliers of hardware and software and providers of ancillary services involved in the functioning or operation of 5G networks or in the provision of 5G services.
g) "5G corporate user": a natural or legal person who installs, deploys or operates private 5G networks or provides 5G services over, in whole or in part, 5G networks, for professional purposes or on a self-provisioned basis.

2. The definitions set out in Law 9/2014 of 9 May 2014 on General Telecommunications and in the European Communications Code shall also apply.

Article 4. *Scope of application.*

This Royal Decree-Law applies to:

a) 5G operators.
b) 5G providers.
c) 5G corporate users that have been granted rights to use the public radio domain to install, deploy or operate a private 5G network or to provide 5G services for professional or self-provisioned purposes.

Article 5. *Comprehensive safety treatment.*

1. The parties referred to in Article 4 must carry out a comprehensive approach to the security of the networks, elements, infrastructures, resources, facilities and services for which they are responsible, for which purpose they must carry out, using a holistic method, an analysis of the vulnerabilities, threats and risks affecting them as economic agents and of the components listed above, as well as an adequate and comprehensive management of these risks by using the appropriate techniques and measures to mitigate or eliminate them and achieve the ultimate objective of the secure exploitation and operation of 5G networks and services.

To this end, the parties referred to in Article 4 must duly comply with the provisions of this Royal Decree-Law, with the provisions of the National Security Scheme for 5G networks and services and with the acts issued in implementation of both provisions.

2. In order to achieve this comprehensive treatment of security, the parties referred to in Article 4 must provide the information required under the provisions of this Royal Decree-Law or the National Security Scheme for 5G networks and services or that required by the Ministry of Economic Affairs and Digital Transformation in the exercise of the functions assigned to them in this area.

Said information is considered confidential, so that it may not be used for any purpose other than compliance with the objectives and obligations established in this Royal Decree-Law, in the National Security Scheme for 5G networks and services and in the acts issued in implementation of both provisions.

3. The National Security Scheme for 5G networks and services will also carry out a comprehensive treatment of the security of 5G networks and services, considering the contributions to the scope of each agent in the 5G value chain, as well as the regulations, recommendations and technical standards of the European Union, the International Telecommunications Union (ITU) and other international organisations, in order to guarantee the ultimate objective of secure exploitation and operation of 5G networks and services in our country.

CHAPTER II
Risk analysis

Article 6. *Risk analysis of 5G operators.*

1. 5G operators shall analyse the risks of 5G networks and services, identifying vulnerabilities and threats that affect them both as an economic actor and through the network elements, infrastructures, resources, facilities and services they use or provide in the installation, deployment and operation of 5G networks or in the provision of 5G services.

2. 5G operators owning or managing network elements of a 5G public network shall, in their risk analysis, carry out a detailed and individualised study of threats and vulnerabilities affecting at least the following elements, infrastructures and resources of a 5G public network:

a) Those relating to the functions of the network core.
b) Transport and transmission functions.
c) The access network.
d) Control and management systems and support services.
e) The functions of edge computing, network virtualisation and management of its components.
f) Those relating to traffic exchanges with external networks and the internet.
g) Other essential components and functions identified for this purpose in the 5G Network and Service Security Scheme.

3. These are critical elements of a public 5G network:

a) Those relating to the functions of the network core.
b) Control and management systems and support services.
c) The access network in those geographical areas and locations to be determined.

4. The risk analysis carried out by a 5G operator should take into account at least the following factors:

a) Parameterisation and configuration of network elements and functions.
b) Software integrity and updating policies.
c) Permission strategies to access physical and logical assets.
d) Dependencies from certain suppliers in elements critics from the network 5G.
e) External agents, including organised groups capable of attacking the network.
f) Computer equipment and devices connected to the network.
g) Elements of corporate users and external networks connected to the 5G network.
h) The interrelationship with other services essential to society.

5. In order to comprehensively address the security of 5G networks and services, the 5G operator shall collect from its suppliers the security practices and measures that have been adopted in the products and services supplied to them, taking into account the risk factors identified in this chapter and the supplier's risk profile. This information shall be provided by the suppliers and its treatment shall be confidential, so that it may only be used by 5G operators for risk analysis and management and by the Ministry of Economic Affairs and Digital Transformation and other competent public bodies for the application of the provisions of this Royal Decree-Law for the exclusive purposes of this Royal Decree-Law.

6. The 5G operator's risk analysis shall include a prioritisation and hierarchy of risks based on the following parameters:

a) Affectation to an element critic from the network public 5G.
b) Type of resource, infrastructure and service that may be affected.
c) Affecting the integrity and technical maintenance of the network or the continuity of service.
d) Detection and recovery capacity.
e) Number and type of users affected.
f) Type of information whose integrity may have been compromised.

7. The risk analysis by the 5G operator must be carried out every two years and submitted to the Ministry of Economic Affairs and Digital Transformation.

Article 7. *Risk analysis by 5G providers.*

1. 5G providers must analyse the risks of telecommunication equipment, hardware and software and ancillary services involved in the operation or operation of 5G networks or in the provision of 5G services, detecting vulnerabilities and threats that affect both the management of the company and such equipment, hardware, software and services.
2. 5G providers shall provide this risk analysis to the Ministry of Economic Affairs and Digital Transformation upon request.
3. Notwithstanding the previous paragraph, 5G suppliers that have been assessed as high risk or medium risk shall submit to the Ministry of Economic Affairs and Digital Transformation a risk analysis of their equipment, products or services involved in 5G networks and services within six months of being assessed as high risk or medium risk.
4. 5G suppliers that are classified as high risk or medium risk must carry out the risk analysis every two years and submit it to the Ministry of Economic Affairs and Digital Transformation.

Article 8. *Risk analysis by 5G corporate users.*

1. 5G corporate users that have been granted rights to use the public radio domain to install, deploy or operate a 5G private network or provide 5G services for professional or self-provisioned purposes shall analyse the risks of 5G networks and services, detecting vulnerabilities and threats affecting the network elements, infrastructure, resources, facilities and services they employ or provide in the installation, deployment and operation of 5G private networks or in the provision of 5G services for self-provisioned purposes.
2. The 5G corporate users referred to in paragraph 1 shall provide this risk analysis to the Ministry of Economic Affairs and Digital Transformation upon request.

Article 9. *Risk factors to be analysed by the subjects referred to in Article 4.*

The National Security Scheme for 5G networks and services shall identify the risk factors to be analysed by the parties referred to in Article 4 in accordance with technological developments, the incorporation of new technological advances, functionalities and standards, the situation of the electronic communications market and the supply market, and the emergence of new threats and vulnerabilities.

Article 10. *Confidentiality of risk analysis information.*

The Ministry of Economic Affairs and Digital Transformation may request from the parties referred to in Article 4 the information necessary for the risk analysis.

The information provided by the aforementioned parties on risk analysis is considered confidential, so that it may not be used for any purpose other than compliance with the objectives and obligations established in this Royal Decree-Law, in the National Security Scheme for 5G networks and services and in the acts issued in execution of both provisions.

CHAPTER III
Risk management

Article 11. *Duty to manage security risks.*

The parties referred to in Article 4 must adopt appropriate technical and organisational measures to manage the risks involved in the installation, deployment and operation of 5G networks and the provision of 5G services, based on the provisions of this Royal Decree-Law, the National Security Scheme for 5G networks and services and the acts issued in implementation of both provisions.

Article 12. *Security management by 5G operators.*

1. 5G operators shall ensure the secure installation, deployment and operation of 5G public networks and the secure provision of publicly available 5G services through the implementation of operation and monitoring techniques and procedures that guarantee the security of 5G networks and services, as well as compliance with the provisions of this Royal Decree-Law.
2. 5G operators have the following security obligations aimed at mitigating risks:

a) Adopt technical and operational measures to ensure the physical and logical integrity of 5G networks or any of their elements, infrastructures and resources, as well as the continuity in the provision of 5G services.
b) Adopt specific contingency plans and measures to ensure the continuity of other essential services for society that rely on 5G networks and services.
c) Select and identify persons who can access the physical and logical assets of the network, and perform access log maintenance.
d) Maintain user credentials for network access in the possession of the operator.
e) Use only products, resources, services or systems certified for the operation of 5G networks, or any parts or elements thereof.
f) Compliance with standards or technical specifications applicable to networks and information systems.
g) Comply with European certification schemes for products, services or systems, whether or not specific to 5G technology, that are used in the operation or exploitation of 5G networks and services.
h) Undergo, at their own expense, a security audit conducted by a public entity or a private entity accredited for this purpose.
i) Require their suppliers to comply with security standards, from the design of products and services to their commissioning.
j) Control their own supply chain and the diversification strategy they have designed.

3. In particular, 5G operators owning or operating critical elements of a 5G public network additionally have the following obligations:

a) They must design a diversification strategy in the supply chain of telecommunication equipment, transmission systems, switching or routing equipment and other resources that enable the transport of signals in a 5G public network, so that such equipment, systems or resources are provided by at least two different suppliers.

For these purposes, suppliers are deemed not to be different if they all belong to the same group of companies, in accordance with the criteria set out in Article 42 of the Commercial Code.

b) They may not use in critical network elements telecommunications equipment, transmission systems, switching or routing equipment and other facilities that permit the transport of signals, hardware, software or ancillary services of suppliers that have been classified as high risk.

c) Telecommunication equipment, transmission systems, switching or routing equipment and other resources, which enable the transport of signals, hardware, software or ancillary services of suppliers that have been classified as high risk, may not be used in the access network of a 5G public network in those radioelectric stations that provide coverage to nuclear power plants, centres linked to National Defence and those locations and centres which, due to their link to national security or to the maintenance of certain essential services for the community or strategic sectors, are determined by the National Security Council, following a report by the Ministry of Economic Affairs and Digital Transformation. The determination and dissemination of these locations shall be treated as classified matters in accordance with the regulation established in Law 9/1968, of 5 April 1968, on official secrets.

d) They shall locate the critical elements of a 5G public network within the national territory.

4. In the event that, as a result of business concentration operations, the number of suppliers included in the supply chain diversification strategy is reduced, which means that the minimum limit of two different suppliers established in section 3.a) of this article, the 5G operator shall notify the Ministry of Economic Affairs and Digital Transformation, which shall encourage the Government, by means of an agreement adopted in the Council of Ministers, after hearing the 5G operators and 5G suppliers affected, to decide whether it is possible to maintain a single supplier, taking into account the specific conditions of the business concentration operation, the market situation of the suppliers, and the situation of the suppliers in the market, the alternatives for the supply of viable substitute equipment and products, the deployment of such equipment and products in the operator's 5G network, especially in critical 5G network elements, the supplier's qualification as high risk, the intrinsic difficulty in carrying out equipment replacement, the equipment upgrade cycles, the migration from non-stand-alone to stand-alone 5G networks, as well as their economic impact.

5. 5G operators that own or operate critical elements of a 5G public network shall submit the supply chain diversification strategy to the Ministry of Economic Affairs and Digital Transformation within six months of the entry into force of this Royal Decree-Law.

Likewise, the supply chain diversification strategy must be submitted to the Ministry of Economic Affairs and Digital Transformation each time it is modified.

Equally, 5G operators that own or operate critical elements of a 5G public network shall submit to the Ministry of Economic Affairs and Digital Transformation information each year on the status of implementation of the supply chain diversification strategy.

6. 5G operators shall submit to the Ministry of Economic Affairs and Digital Transformation every two years a description of the technical and organisational measures designed and implemented to manage and mitigate risks.

Article 13. *Security management by 5G providers.*

1. 5G suppliers must guarantee the security of the telecommunications equipment, hardware, software or ancillary services they provide and which are used by 5G networks and services.

2. 5G providers have the following security obligations aimed at mitigating risks, which will be specified and developed in the National Security Scheme for 5G networks and services:

a) Comply with security standards from the design of equipment, products and services until they are put into operation.

b) Reinforce software integrity, updating and patch management.

c) Certify the certification of IT products and services used in 5G networks and services.

d) Ensure the implementation of standard technical and organisational security measures through a certification system.

e) Perform a safety audit of your equipment, products and services.

f) Provide information on possible third party interference in the design, operation and functioning of its equipment, products and services.

g) Collaborate with 5G operators and 5G corporate users by providing information and

accrediting compliance with security standards for the equipment, products and services they supply.

3. 5G suppliers shall provide the Ministry of Economic Affairs and Digital Transformation with a description of the technical and organizational measures designed and implemented to manage and mitigate risks, when required to do so.

4. Notwithstanding the provisions of the previous paragraph, 5G suppliers that have been classified as high risk or medium risk shall submit to the Ministry of Economic Affairs and Digital Transformation a report on the technical and organisational measures designed and implemented to manage and mitigate the risks within six months of being classified as high risk or medium risk.

5. High-risk and medium-risk 5G suppliers shall submit to the Ministry of Economic Affairs and Digital Transformation every two years a description of the technical and organisational measures designed and implemented to manage and mitigate risks.

Article 14. *High-risk and medium-risk 5G suppliers.*

1. The Government, by means of an agreement adopted by the Council of Ministers, following a report from the National Security Council and after hearing the affected 5G operators and 5G suppliers for a period of 15 working days, may classify certain 5G suppliers as high risk.

For this purpose, the Government will analyze both the technical guarantees of operation and operability of their equipment, products and services and their exposure to external interference.

2. In relation to the analysis of the technical measures and technical guarantees for the functioning and operability of its equipment, products and services, aspects relating to compliance with standards or technical specifications, their verification through certification schemes, or the passing of security tests or audits carried out by independent entities will be assessed.

3. In relation to the analysis of strategic measures and exposure to external interference, the following aspects will be assessed:

a) The links of suppliers and their supply chain with third country governments.

b) The composition of its share capital and the structure of its governing bodies.

c) The power of a third State to exert pressure on the action or location of the undertaking.

d) The characteristics of the third State's cyber defence legislation and policy and its compliance with international law and United Nations resolutions and agreements.

e) Cooperation agreements on security, cybersecurity, cybercrime or data protection signed with the third country concerned, as well as international treaties in those matters to which that State is a party.

f) The degree of adaptation of the regulations of the third State on personal data protection to those of Spain, to the General Data Protection Regulation approved by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC adopted by the European Union and to any other applicable regulations on the security of information and telecommunications networks and systems.

4. The agreement of the Council of Ministers classifying certain 5G suppliers as high-risk suppliers shall determine the time frame within which 5G operators shall carry out the replacement of the equipment, products and services provided by such supplier in the 5G operator's network and services, where necessary, taking into account the market situation of the suppliers, the alternatives for the provision of viable substitute equipment and products, the deployment of such equipment and products in the operator's 5G network, especially in the critical elements of the 5G network and depending on which critical elements are specifically affected, the intrinsic difficulty in carrying out equipment replacement, equipment upgrade cycles, the migration from non-standalone to standalone 5G networks, as well as their economic impact, although in no case shall this period be less than one year.

5. The resolution of the Council of Ministers classifying certain 5G suppliers as high-risk puts an end to the administrative process and may be directly appealed before the contentious-administrative jurisdiction, without prejudice to the possibility of filing an appeal for

reconsideration prior to the contentious-administrative appeal.

6. High-risk suppliers whose telecommunication equipment, hardware, software or ancillary services provided are used solely and exclusively in private 5G networks or for the provision of 5G services on a self-provisioned basis are qualified as medium-risk suppliers.

Article 15. *Security management by 5G corporate users.*

1. 5G corporate users that have been granted rights of use of the public radio domain to install, deploy or operate a 5G private network or to provide 5G services for professional or self-provisioning purposes shall ensure the secure installation, deployment and operation of 5G private networks and secure provision of 5G services for self-provisioning by implementing operation and monitoring techniques and procedures that guarantee the security of 5G networks and services.

2. The aforementioned 5G corporate users shall provide the Ministry of Economic Affairs and Digital Transformation with a description of the technical and organisational measures designed and implemented to manage and mitigate risks, when required to do so.

Article 16. *Conditions for compliance with the obligations.*

In complying with the obligations established in the previous articles, the parties referred to in article 4 shall take into account and apply the provisions of this Royal Decree-Law, the National Security Scheme for 5G networks and services and the acts issued in implementation of both provisions.

Article 17. *Security management by public administrations.*

1. Public administrations shall adopt appropriate technical and organisational measures to manage the risks involved in the installation, deployment and operation of 5G networks and in the provision of 5G services.

2. In particular, public administrations wishing to undertake the installation, deployment and operation of 5G networks, whether public or private, or the provision of 5G services, whether publicly available or self-provisioned, shall not, for reasons of national security, use equipment, products and services provided by high-risk or medium-risk suppliers.

Article 18. *Compliance with foreign investment and competition regulations.*

The obligations established in the preceding articles are understood to be without prejudice to the application of the instruments of control over foreign direct investment in the persons referred to in Article 4 who are of Spanish nationality, as well as to the application of the regulations on the defence of competition.

Article 19. *Confidentiality of information on risk management.*

The Ministry of Economic Affairs and Digital Transformation may request from the parties referred to in Article 4 the information necessary for risk management.

The information provided by the aforementioned parties on risk management shall be considered confidential, such that it may not be used for any purpose other than compliance with the objectives and obligations established in this Royal Decree-Law, in the National Security Scheme for 5G networks and services and in the acts issued in execution of both provisions.

CHAPTER IV
National Security Scheme for 5G networks and services

Article 20. *Content of the National Security Scheme for 5G networks and services.*

1. The National Security Scheme for 5G networks and services will carry out a comprehensive and global treatment of the security of 5G networks and services, considering the contributions to the scope of each agent in the 5G value chain in order to guarantee the continuous and secure operation of the 5G network and services.

2. The National Security Scheme for 5G networks and services shall conduct a national risk analysis on the security of 5G networks and services as well as identify, specify and develop measures at national level to mitigate and manage the analysed risks.

Article 21. *Approval and review of the National Network Security Scheme and 5G Services.*

1. The Government shall approve, by Royal Decree, at the proposal of the Ministry of Economic Affairs and Digital Transformation, following a report from the National Security Council, a National Security Scheme for 5G networks and services.
2. The National Security Scheme for 5G networks and services shall be reviewed at least every four years or whenever circumstances so advise.

Article 22. *Risk analysis in the National Network Security Scheme and 5G Services.*

1. The National Security Scheme for 5G networks and services shall conduct a national risk analysis on the security of 5G networks and services.
2. This national risk analysis shall identify, inter alia, the following aspects:

a) The overall risk analysis of 5G networks and services, taking into consideration the information collected from the subjects referred to in Article 4.
b) Examination of vulnerabilities linked to the 5G networks and services supply chain.
c) Assessment of the degree of dependence of suppliers of all 5G networks and services in Spain, taking into account the risk analyses and supplier diversification strategies submitted by 5G operators, as well as the risk of supply disruption due to economic, corporate or commercial circumstances affecting suppliers.
d) The assessment of the effectiveness of the security measures implemented until the approval of each national risk analysis to mitigate the risks highlighted by such analysis.

3. The National Security Scheme for 5G networks and services shall establish a hierarchy of risks on the basis of the risk analyses carried out by the parties referred to in Article 4 and on the basis of the shortcomings identified in the assessment of the effectiveness of the measures implemented.

Article 23. *Risk management in the National Security Scheme for 5G networks and services.*

1. The National Security Scheme for 5G networks and services shall establish, specify and develop criteria, requirements, conditions and deadlines so that the parties referred to in Article 4 may comply with the obligations imposed on each of these categories of economic agents by this Royal Decree-Law.

To this end, the national risk analysis included in the National Strategy itself and the assessment of the effectiveness of the measures previously applied by the parties referred to in article 4 to mitigate and manage the risks in 5G networks and services shall be taken into account.

2. The National Security Scheme for 5G networks and services may make the use of a particular piece of equipment, programme or service by a 5G operator, 5G supplier or 5G corporate user provided for in Article 4 subject to the prior obtaining of a certification established under Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on cybersecurity.
3. The National Security Scheme for 5G networks and services, regardless of the supply chain diversification strategies that 5G operators may have, may carry out a specific analysis and may propose objectives for the diversification of 5G suppliers in the supply chain in 5G networks and services for the State as a whole, for which purpose it may arbitrate objective, proportionate and non-discriminatory measures aimed at meeting these objectives, always within the framework established in this Royal Decree-Law.
4. The National Security Scheme for 5G networks and services will also contain measures to mitigate or manage the risks arising from the market for terminal equipment and connected devices.

The manufacture, import, distribution, placing on the market and marketing of terminal equipment and devices to connect to a 5G network and to be able to provide 5G services will be conditional upon compliance with the applicable essential requirements related to cybersecurity, adopted in accordance with European regulations, in particular in relation to the protection of personal data, privacy, and protection against fraud.

Article 24. *Duty to collaborate in the approval and implementation of the National Security Scheme for 5G networks and services.*

All parties referred to in article 4, as well as manufacturers, importers, distributors and those who place on the market and market terminal equipment and devices to connect to a 5G network and to be able to provide 5G services shall cooperate and submit the information required for the preparation, approval and implementation of the National Security Scheme for 5G networks and services.

Article 25. *International cooperation.*

1. The Government shall cooperate closely with other Member States of the European Union and with the institutions of the European Union in the definition and implementation of the National Security Scheme for 5G networks and services and, in general, shall collaborate with the various specialised international organisations in order to be able to carry out a comprehensive and global treatment of the security of 5G networks and services.
2. In particular, the Government and the Ministry of Economic Affairs and Digital Transformation may share information related to the analyses carried out by the institutions of the European Union and with other Member States of the European Union, preserving, as appropriate in law, the security, commercial interests and confidentiality of the information gathered in the preparation of the analysis, as well as making use of the information sent to it by other States or the institutions of the European Union for its performance. It may also carry out these analyses jointly with other Member States of the European Union.

Article 26. *Support for research, development and innovation in 5G Cybersecurity*

The National Security Scheme for 5G networks and services shall include the outlines and priorities of any public support that may be granted to promote research and development in the field of security in 5G networks and services and for the training of specialised personnel.

Article 27. *Promoting interoperability.*

The National Security Scheme for 5G networks and services shall promote the interoperability of equipment and programmes related to the management of 5G networks and services, as well as the participation of public and private actors in the development of standards on the operation of 5G networks and services.

Article 28. *Powers for the application of the National Security Scheme for 5G networks and services.*

1. The Ministry of Economic Affairs and Digital Transformation shall be the competent department to implement the National Security Scheme for 5G networks and services and to exercise the other functions attributed to it by this Royal Decree-Law.
2. The Ministry of Economic Affairs and Digital Transformation shall coordinate with the other competent bodies in matters of cybersecurity and critical infrastructures to ensure consistent application of the National Security Scheme for 5G networks and services.
3. The Ministry of Economic Affairs and Digital Transformation, in the exercise of the functions assigned to it by this Royal Decree-Law, may exercise, among others, the following powers:

a) To develop, specify and detail the content of the National Security Scheme for 5G networks and services.
b) Formulate requests for information to the parties provided for in article 4, which must be answered within 15 working days from the day following notification, in order to be able to exercise the functions assigned to it by this Royal Decree-Law and its implementing regulations and, specifically, to verify and control compliance with the respective obligations that this Royal Decree-Law and its implementing regulations impose on the parties provided for in article 4.
c) Carry out audits or order them to be carried out in order to verify and control compliance with the respective obligations that this Royal Decree-Law and its implementing regulations impose on the parties provided for in Article 4.
d) Carry out inspections by the civil servants assigned to the Secretary of State for Telecommunications and Digital Infrastructure and exercise the power to impose penalties under the terms indicated in the following chapter.

e) Grant public aid.
f) Exercise its other functions under applicable legislation.

CHAPTER V
Inspection and sanctioning regime

Article 29. *Faculties from inspection.*

The Ministry of Economic Affairs and Digital Transformation shall exercise in the application and supervision of the provisions of this royal decree-law all the powers of the inspection function provided for in Title VIII of General Telecommunications Law 9/2014 of 9 May 2014.

Article 30. *Penalties*

1. The sanctioning regime laid down in Title VIII of Law 9/2014, of 9 May shall apply, with the exception of the specialities laid down in this royal decree-law.

2. In addition, the following offences are classified as very serious, serious and minor.

3. Failure by 5G operators owning or operating critical elements of a public 5G network to comply with the obligations set out in Article 12(3) is a very severe infringement.

4. The following shall constitute serious offences:

a) Failure by 5G operators to comply with the obligations set out in Article 12, except for those set out in Article 12(3), which are very serious infringements.
b) The non-compliance by the 5G suppliers of the obligations established in the Article 13.
c) Failure by 5G corporate users referred to in Article 4 to comply with the obligations set out in Article 15.
d) The non-compliance by the administrations public from the obligations established in the Article 17.
e) Failure to comply with stipulations established in the National Security Scheme for 5G networks and services when they are directly enforceable.
f) Failure to comply with the information requirements formulated in accordance with article 27(3)(b) when one month has passed since the end of the period given for compliance.

5. Minor infringements are defective compliance or partial non-compliance with conduct classified as serious infringements.
6. The penalties to be applied are those established in article 79 of Law 9/2014, of 9 May 2014.
7. The criteria for determining the amount of the sanction are those established in article 80 of Law 9/2014, of 9 May 2014.
8. The exercise of the sanctioning power corresponds to the head of the Secretary of State for Telecommunications and Digital Infrastructure.
9. The prior measures and precautionary measures established in articles 81 and 82 of Law 9/2014, of 9 May 2014, may be applied when appropriate in accordance with the regulations contained in said articles.

Article 31. *Inspection and sanctioning regime of the General Telecommunications Law.*

In all matters not provided for in this Royal Decree-Law, the provisions of the regulations contained in the inspection and sanctioning regime of Title VIII of Law 9/2014, of 9 May 2014, General Telecommunications Law, shall be applicable.

First additional provision. *Remission to the Ministry of Economic Affairs and Digital Transformation of the risk analyses of 5G operators and of the technical and organisational measures to mitigate them.*

Within six months of the entry into force of this Royal Decree-Law, 5G operators shall submit a risk analysis of their 5G networks and services or of those to be deployed in the next two years and a report on the technical and organisational measures designed and implemented to manage and mitigate the risks.

Second additional provision. *Referral to the Ministry of Economic Affairs and Digital Transformation of the diversification strategies in the supply chain.*

5G operators that own or operate critical elements of a 5G public network shall submit their supply chain diversification strategy to the Ministry of Economic Affairs and Digital Transformation within six months of the entry into force of this Royal Decree-Law.

Third additional provision. *Declaration of high-risk suppliers.*

Within three months of the entry into force of this Royal Decree-Law, the Government, by means of a resolution adopted by the Council of Ministers, following a report from the National Security Council and after hearing the 5G operators and 5G suppliers affected for a period of 15 working days, may classify certain 5G suppliers as high risk.

To this end, the Government shall analyse both the technical guarantees of operation and operability of their equipment, products and services and their exposure to external interference under the terms indicated in Article 14.

Fourth additional provision. *Determination from centres and locations where equipment, products or services from high-risk suppliers may not be used.*

Within a period of three months from the entry into force of this royal decree-law, the National Security Council, following a report from the Ministry of Economic Affairs and Digital Transformation, will determine the locations and centres in which, by virtue of the established in article 12(3)(c), due to its connection to national security or the maintenance of certain essential services for the community or strategic sectors, 5G operators that own or operate critical elements of a public 5G network will not be able to use in the access network of a 5G public network telecommunications equipment, transmission systems, switching or routing equipment and other resources that allow the transport of signals, hardware, software or auxiliary services from high-risk suppliers.

Fifth additional provision. *Application of the royal decree-law to successive generations of electronic communications.*

This royal decree-law is applicable to guarantee the security of electronic communications networks and services of generations after the fifth generation as long as there is no specific standard for them.

Single transitional provision. *Replacement of equipment, products or services provided by 5G suppliers declared high risk.*

If the declaration of high-risk suppliers occurs in the terms indicated in the fourth additional provision and this results in the 5G operators having to replace the equipment, products or services provided by said 5G suppliers, the 5G operators will have a period five years from when 5G suppliers have been classified as high risk to carry out said replacement in critical network elements related to the core functions of the network and control and management systems and support services, as well as a period of two years from when the 5G suppliers have been classified as high risk to carry out said replacement in the critical network elements related to the access network in those geographical areas and locations in accordance with the provisions of article 12(3)(c).

First final provision. *Attribution of powers.*

This royal decree-law is issued under the provisions of article 149(1)(21) and article 149(1)(29) of the Constitution, which attribute to the State, respectively, exclusive competence in matters of the general telecommunications regime and in matters of public safety.

Second final provision. *Supplementary implementation of the rules on security and integrity of electronic communications networks.*

1. In everything that is not regulated in this royal decree-law, the provisions of Law 9/2014, of 9 May 2014, General Telecommunications, and its implementing regulations will be of supplementary application.
2. In matters not regulated in Law 9/2014, of 9 May 2014, General Telecommunications, and its implementing regulations, Royal Decree-Law 12/2018, of 7 September 2018, on security

of networks and systems, will be supplementary application. of information, and Law 8/2011, of 28 April 2011, which establishes measures for the protection of critical infrastructures, as well as their respective development regulations.

Third final provision. *Authorisation to pass legislation.*

1. The Government is empowered to develop regulations as provided for in this royal decree-law and, in particular, to approve the National Security Scheme for 5G networks and services.
2. The first National Security Scheme for 5G networks and services must be approved within six months from the entry into force of this royal decree-law.

Fourth final provision. *Entry into force.*

1. This royal decree-law will come into force on the day following its publication in the "Official State Gazette."
2. The obligations contained in articles 12, 13, 15, 16 and 17 will come into force within one month from the day of their publication in the "Official State Gazette."

Given in Madrid, on 29 March 2022.

FELIPE R.

The Chairman of Government,
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN

Related information

- Royal Decree-Law 7/2022, of 29 March 2022, has been validated by Congressional Agreement of the Members, published by resolution of 28 April 2022. Ref. BOE-A-2022-7313