

# Trends for 2024 in telecommunications and electronic communications

# Contents

1. The Gigabit Infrastructure Act and 5G: driving digital competitiveness in the EU	→ Saiba mais	5. Consumer protection – the regulator’s perspective and areas of focus	→ Saiba mais
1.1 What is the significance of the GIA and 5G?	→ Saiba mais	5.1 Quality of service	→ Saiba mais
1.2 How does the GIA streamline network implementation?	→ Saiba mais	5.2 Transparency of contracts	→ Saiba mais
1.3 Legislative and regulatory developments	→ Saiba mais	5.3 Portability	→ Saiba mais
1.4 The position of the European Commission	→ Saiba mais	5.4 Infrastructure sharing and 5G	→ Saiba mais
1.5 Position of the Portuguese legislature	→ Saiba mais	5.5 Digital services	→ Saiba mais
1.6 Impact of the GIA on industry and on the Portuguese market	→ Saiba mais		
2. The space sector	→ Saiba mais	6. The importance of cybersecurity in the digital age	→ Saiba mais
2.1 Amendment to the Regulation on Access to and Exercise of Space Activities	→ Saiba mais	6.1 Expanding cybersecurity measures	→ Saiba mais
2.2 Details of the changes to the RAE	→ Saiba mais	6.2 The challenges	→ Saiba mais
3. White Zones Tender: a decisive step for rural connectivity in Portugal	→ Saiba mais	7. Changes in access to metadata: impact and perspectives	→ Saiba mais
3.1 What is the initiative about?	→ Saiba mais	7.1 Main changes	→ Saiba mais
3.2 Potential candidates and covered infrastructures	→ Saiba mais	7.2 Impact on the electronic communications sector	→ Saiba mais
4. The IA regulatory revolution in the European Union: the impact of the EU Artificial Intelligence Act	→ Saiba mais		
4.1 Classification by risk: a structured approach	→ Saiba mais		
4.2 Compliance obligations: ensuring safety and ethics	→ Saiba mais		
4.3 Impact on electronic communications companies	→ Saiba mais		

# 1. The Gigabit Infrastructure Act and 5G: driving digital competitiveness in the EU

The Gigabit Infrastructure Act<sup>1</sup> (“GIA”) which replaces the 2014 Broadband Cost Reduction Directive (“BCRD”) entered into force in May 2024<sup>2</sup>. This new legislation is an important milestone in the European Union’s strategy to achieve a robust and competitive digital infrastructure by 2030.

## 5G technology has emerged as a factor contributing to the deployment of networks, a true catalyst for digital transformation

### 1.1. WHAT IS THE SIGNIFICANCE OF THE GIA AND 5G?

The main objective of the GIA is to facilitate the deployment of gigabit networks in the European Union (EU) and improve access to existing infrastructure through a simplified installation process. This aim of this initiative is to ensure that Europe maintains its global digital competitiveness, especially in a scenario where high quality connectivity is essential for industrial competitiveness and for the digital and environmental transition.

In this context, 5G technology has emerged as a factor contributing to the deployment of networks, a true catalyst for digital transformation in all sectors of the economy.

The main benefits of 5G are its ability to boost Europe’s digital competitiveness and digital inclusion. 5G has the potential to significantly reduce the digital divide, especially in rural and remote areas. Continued investment in infrastructure is essential to ensure that all citizens, regardless of their location, can benefit from ultra-fast connectivity.

Sustainability is also a priority. 5G must be energy efficient, reducing the energy consumption of networks and enabling sustainable connectivity. This energy efficiency is critical to reducing operational costs and promoting greener connectivity.<sup>3</sup>

### 1.2. HOW DOES THE GIA STREAMLINE NETWORK IMPLEMENTATION?

The GIA presents several measures<sup>3</sup> to optimise network deployment:

- **Infrastructure sharing**  
Encouraging the sharing of ducts and masts for the deployment of Very High Capacity Networks (VHCN) in order to optimise resources and reduce costs. Expanding and upgrading network infrastructure requires significant technical and financial investment. However, investing in more efficient technologies with lower operating costs, such as 5G, can reduce costs in the long term.

<sup>1</sup> [Regulation of the European Parliament and of the Council](#) on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act).

<sup>2</sup> [Press release from the Council of the European Union](#), Gigabit Infrastructure Act: Council and Parliament strike a deal for faster deployment of high-speed networks in the EU.

<sup>3</sup> [European Parliament Resolution of 1 June 2017](#) on internet connectivity for growth, competitiveness and cohesion: European gigabit society and 5G.



- **Simplifying administrative processes**  
Simplifying administrative procedures related to network deployment and access to physical infrastructure across the EU to reduce red tape and increase efficiency. This will catalyse the roll-out of gigabit and 5G networks.
- **Equipping buildings with high-speed infrastructure**  
Encouraging the provision of high-speed infrastructure in buildings and guaranteeing access to it, thus facilitating the spread and use of broadband.

### 1.3. LEGISLATIVE AND REGULATORY DEVELOPMENTS

In particular, the deployment of 5G networks continues to be a key point for the growth of the sector, with regulators considering issues related to spectrum allocation, security standards and privacy concerns related to 5G infrastructure.

The roll-out of 5G in Portugal began in 2020, following the auction of 5G licences awarded by ANACOM<sup>4</sup>. 5G coverage is already available in the main cities and operators continue to expand their networks.

The 5G Strategy Resolution<sup>5</sup> defines the guidelines for the deployment of this technology, with the aim of boosting competitiveness, facilitating the digital transition and ensuring that 5G is available in urban and rural areas, benefiting sectors such as health, industry and smart cities. The resolution also sets targets for coverage, innovation and sustainable economic development, and encourages cooperation between the public and private sectors to maximise the benefits of the new infrastructure.

<sup>4</sup> [Regulation 987-A/2020](#), Regulation of the Auction for the Allocation of Rights of Use for Frequencies in the 700 MHz, 900 MHz, 1800 MHz, 2.1 GHz, 2.6 GHz and 3.6 GHz bands.

<sup>5</sup> [Council of Ministers Resolution 7-A/2020](#) approving the strategy and timetable for the roll-out of fifth generation mobile communications.

The 5G Strategy Resolution defines the guidelines for the deployment of this technology, benefiting sectors such as health, industry and smart cities.



# The European Commission is focused on ensuring that 5G reaches the whole of Europe by 2025.

## 1.4. THE POSITION OF THE EUROPEAN COMMISSION

The continued implementation of European legislation on 5G and the concern to ensure that the networks used are secure are fundamental to the success of this initiative<sup>6</sup>. The European Commission is focused on ensuring that 5G reaches the whole of Europe by 2025, ensuring rural inclusion and territorial cohesion<sup>7</sup>. Investments must also comply with network security rules to ensure that the digital infrastructure is resilient and secure.

## 1.5. POSITION OF THE PORTUGUESE LEGISLATURE

With the support of EU funding and the public tender for the coverage of the “white zones”, the Portuguese government is prioritising and targeting the development of digital infrastructure in rural areas

The emphasis is on the need for resilience and security in electronic communications networks to ensure that all regions of the country can benefit from high-speed connectivity.

## 1.6. IMPACT OF THE GIA ON INDUSTRY AND ON THE PORTUGUESE MARKET

The GIA is expected to have a significant impact on the electronic communications sector and the single market in a number of areas:

- **Competition and consumer benefits**

The deployment of high-speed networks will increase competition between electronic communications operators, benefiting consumers who will have access to more competitive prices<sup>8</sup>.

- **New services and opportunities**

New infrastructures open the door to innovation in digital services. Businesses will generally have the opportunity to exploit these technologies and subsequently offer new products and services<sup>9</sup>.

- **Development of rural areas**

Implementing specific measures to promote the deployment of these technologies in rural areas, the GIA will contribute to the reduction of the digital dividend and to local economic development<sup>10</sup>.

- **Economies of scale and legal certainty**

Harmonising rules at European level, operators and manufacturers will be able to achieve better economies of scale, thereby reducing operating costs<sup>11</sup>.

---

6 European Commission, [Gigabit Infrastructure Act](#).

7 [The European 5G Annual Journal 2023](#).

8 GIA Recital 49.

9 GIA Recital 62.

10 GIA Recital 1.

11 GIA Recital 53.



## 2. The space sector

The space sector has become increasingly prominent on the regulatory agenda, with the European Union, the Portuguese government and private individuals working together effectively to promote growth and innovation. The European Union recognises this sector as a real driver of technological progress and economic development, as reflected in the EU Space Strategy and Programme. To consolidate Portugal's presence in the sector, the government has adopted various initiatives, such as joining the European Space Agency ("ESA") and supporting innovation centres and start-ups in the sector.

### Portugal has attracted international companies that excel in space activities, positioning itself as a strategic hub in this sector.

In addition, Portugal has attracted international companies that excel in space activities, positioning itself as a strategic hub in this sector. This development will make a significant contribution not only to the Portuguese economy, but also to the development of space technologies in Europe.

For its part, ANACOM has focused its actions on strengthening its powers and creating a regulatory framework that ensures the safe and efficient use of space. The success of ANACOM's strategy, as set out in its Strategic Plan for 2024-2026<sup>12</sup>, could not only strengthen Portugal's position in the space and communications sectors, but also serve as a model for other countries seeking convergence in the regulation of these two sectors.

### 2.1. AMENDMENT TO THE REGULATION ON ACCESS TO AND EXERCISE OF SPACE ACTIVITIES

In this context, in October 2024, ANACOM adopted a new amendment to the Regulation on Access to and Exercise of Space Activities (*Regulamento Relativo ao Acesso e Exercício de Atividades Espaciais* - "RAE")<sup>13</sup>. Prior to the amendment of the RAE, between July and September 2024, ANACOM conducted a public consultation that allowed the participation of various interested parties, including the National Civil Aviation Authority (*Autoridade Nacional da Aviação Civil* - "ANAC") and the Portuguese Space Agency. The contributions received reflected the urgency of creating a regulatory framework that not only ensures safety, but also promotes innovation and growth in the space sector<sup>14</sup>.

### 2.2. DETAILS OF THE CHANGES TO THE RAE

The consultation process allowed stakeholders to make important suggestions and comments which have been taken into account by the regulator:

- o **Special licensing arrangements**

ANACOM highlighted the need to establish special arrangements for experimental and scientific operations in order to facilitate the simplification of procedures, and this proposal was accepted. As a result, the RAE now provides for special licensing arrangements with reduced time limits and simplified procedures for scientific and experimental operations.

- o **Joint licensing**

it was suggested that there should be a single licensing procedure for operations carried out by several operators in order to increase efficiency and cooperation between the parties involved. This proposal was also accepted by ANACOM. From now on, there will be a single procedure for licensing operations carried out by multiple operators.

<sup>12</sup> See [ANACOM's Multiannual Activity Plan 2024-2026](#).

<sup>13</sup> [Regulation 1206-A/2024 of 21 October](#).

<sup>14</sup> See [Relatório da Consulta Pública sobre o Projeto de Regulamento de Alteração ao Regulamento Relativo ao Acesso e Exercício de Atividades Espaciais](#).

- **Security requirements**

as various stakeholders have stressed the importance of security plans that integrate cybersecurity and environmental considerations, ANACOM approved a number of changes that extend the requirements applicable to security plans. These must now include aspects related to cybersecurity and operational risk mitigation.

- **Coordination with other authorities**

as coordination between ANACOM and ANAC was identified as essential for the integrated and safe management of space activities, during the public consultation, ANACOM undertook to ensure this coordination with airspace regulators.

The changes approved by ANACOM aim not only to modernise and strengthen the regulatory framework for space activities in Portugal, but also to create an environment conducive to innovation and the sustainable development of the sector.

## 3. White Zones Tender: a decisive step for rural connectivity in Portugal

### 3.1. WHAT IS THE INITIATIVE ABOUT?

The White Zones Tender<sup>15</sup> is an ambitious initiative by the Portuguese government aimed at bringing fibre-optic connectivity to rural and low-density areas, known as “white zones”, which currently lack high-capacity network coverage. This project, with a total investment of approximately €425 million – around €150 million from the Regional Programmes of Portugal 2030 and the remainder from national funds – seeks to cover over 400,000 homes in different interior regions by 2026/2027<sup>16</sup>.

The White Zones Tender is an ambitious initiative by the Portuguese government aimed at bringing fibre-optic connectivity to rural and low-density areas.

The main objective of this competition is to ensure that all areas of the Portuguese mainland have access to high-capacity networks, thus promoting digital inclusion and territorial cohesion. The goal is ambitious: to achieve full coverage of the mainland by 2026/2027.

<sup>15</sup> ANACOM [Public consultation on the coverage of 'white areas' with very high capacity fixed networks.](#)

<sup>16</sup> [Concurso para cobrir zonas brancas de redes de comunicações de alta capacidade será lançado este ano - XXIII Governo - República Portuguesa.](#)

### 3.2. POTENTIAL CANDIDATES AND COVERED INFRASTRUCTURES

The participation of various players, including both Portuguese and international operators, will be fundamental to the success of this project.

The potential candidates are more likely to be electronic communications infrastructure companies. As the tender is international, there is also the possibility for foreign companies to participate.

Despite the clear interest of some operators in using the networks to be built, there has been criticism of the inclusion of 5G mobile networks in the definition of white zones, arguing that this approach may not be the most effective. Operators have also raised concerns about the potential duplication of infrastructure, which could lead to an inefficient use of available resources, and the inadequacy of subsidies to cover the costs associated with the roll-out of electronic communications networks.

The proposed technologies  
are in line with the European  
Commission's guidelines  
for the roll-out of  
high-speed networks.

In response to these criticisms, ANACOM justified the inclusion of 5G by its ability to provide services equivalent to those of fixed networks. ANACOM believes that the proposed methodology for identifying white zones aims to avoid duplication of infrastructure and that the proposed technologies are in line with the European Commission's guidelines for the roll-out of high-speed networks. ANACOM also stressed that the analysis carried out takes into account future coverage plans in order to avoid network overlaps in the event of future investments by other operators.

## 4. The IA regulatory revolution in the European Union: the impact of the EU Artificial Intelligence Act

With the entry into force of the European Artificial Intelligence Regulation<sup>17</sup> ("AI Act") on 1 August 2024, the first robust regulatory framework for the use of artificial intelligence (AI) will be created. Its purpose is to ensure that AI is used ethically, safely and in accordance with the fundamental rights of European citizens<sup>18</sup>.

### 4.1. CLASSIFICATION BY RISK: A STRUCTURED APPROACH

The AI Regulation introduces a risk classification that defines specific requirements based on the risk level of AI applications. This approach is essential to ensure that compliance measures are proportionate to the potential impact of AI technologies.

<sup>17</sup> Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

<sup>18</sup> Press release from the Council of the European Union Artificial Intelligence Act. Council gives final green light to the first worldwide rules on AI.



## 4.2. COMPLIANCE OBLIGATIONS: ENSURING SAFETY AND ETHICS

The AI Act sets out<sup>19</sup> a number of compliance obligations for providers and users of AI systems. The reason for imposing these obligations is to mitigate risks and ensure the responsible and transparent use of these technologies.

- **Risk mitigation measures**  
companies developing or using AI must conduct regular impact assessments to identify potential threats to security, privacy and fundamental rights. Recommended measures include: impact assessments, security monitoring and incident response plans<sup>20</sup>.
- **Data quality assurance**  
data quality is critical to the performance and safety of AI systems<sup>21</sup>. The IA Act requires companies to use quality data that avoids unfair or discriminatory decisions. Key obligations include: use of accurate and representative data, correction of bias, detailed documentation.
- **Proper human review**  
human oversight remains essential to ensure the ethical and safe operation of AI systems<sup>22</sup>.

## 4.3. IMPACT ON ELECTRONIC COMMUNICATIONS COMPANIES

The AI Regulation represents both a challenge and an opportunity for electronic communications companies.

These companies will need to adapt their internal AI systems to ensure that all their digital services comply with the new rules. In particular, a number of measures will need to be implemented, including risk mitigation and ensuring that the data used in the context of artificial intelligence systems is of high quality and properly supervised.



The AI Regulation represents both a challenge and an opportunity for electronic communications companies.

<sup>19</sup> Section 2 of the AI Act.

<sup>20</sup> Article 27 of the AI Act.

<sup>21</sup> Annex VII of the IA Act.

<sup>22</sup> Article 14 of the AI Act.

## 5. Consumer protection - the regulator's perspective and areas of focus

In recent years, ANACOM has intensified its supervision of electronic communications operators in Portugal, focusing on areas that the regulator considers essential for competition in the sector, such as quality of service, contractual transparency, portability, infrastructure sharing (especially 5G networks) and cybersecurity<sup>23</sup>.

In line with this action, ANACOM's Strategic Plan for 2024-2026 establishes as one of its strategic priorities to ensure the protection of the rights of communications users, especially the most vulnerable, by promoting a regulatory framework that prioritises information and transparency, and discourages and sanctions bad practices.

This more interventionist stance is reflected in the huge fines imposed by the national regulator over the last four years. In January 2024, ANACOM announced that it had decided to impose significant fines for breaches of consumer protection rules in the electronic communications sector, totalling more than €10 million<sup>24</sup>.

**ANACOM's Strategic Plan for 2024-2026 establishes as one of its strategic priorities to ensure the protection of the rights of communications users.**

### 5.1. QUALITY OF SERVICE

ANACOM closely monitors the quality of service provided by operators to ensure that consumers receive the contracted level of service. This monitoring includes checking parameters such as the speed of Internet access, the quality of fixed and mobile calls and the availability of electronic communications services.

### 5.2. TRANSPARENCY OF CONTRACTS

ANACOM has also played a significant role in monitoring the pre-contractual and contractual information made available to consumers of electronic communications services. Under the legislation in force, the principle of transparency requires operators to provide clear and comprehensible information on the terms and conditions of the services offered. This includes detailed information on prices, contract duration, cancellation conditions and any additional charges.

### 5.3. PORTABILITY

Portability – that is, the ability to change operator without losing your phone number – is a fundamental right for consumers of voice services. It is an issue that is constantly subject to regulatory intervention, and in 2024 ANACOM again introduced changes to the Portability Regulation to reduce the time needed to carry out number portability and to minimise service interruptions<sup>25</sup>.

<sup>23</sup> ANACOM, [Report on Security Breaches or Loss of Integrity](#).

<sup>24</sup> See the information on [infringements published in January 2024](#).

<sup>25</sup> [ANACOM aprova novas regras de portabilidade - Destaques - Portal do Consumidor](#).



#### 5.4. INFRASTRUCTURE SHARING AND 5G

The implementation of 5G is one of the biggest challenges and opportunities for the electronic communications sector. ANACOM has promoted the sharing of infrastructure between operators to speed up the deployment of 5G and reduce costs<sup>26</sup>. This collaborative approach not only benefits operators, but also ensures that consumers have faster access to new technologies.

#### 5.5. DIGITAL SERVICES

As part of the implementation of the Digital Services Act (“**DSA**”)<sup>27</sup> in Portugal, ANACOM has assumed a central role as the coordinator of digital services. This designation, formalised by Decree-Law 20-B/2024<sup>28</sup>, gives ANACOM responsibility for monitoring and ensuring compliance with the provisions of the DSA at national level. The DSA aims to establish clear rules for the operation of digital platforms and to strengthen transparency, responsibility and security in the online environment. This new approach has important implications for operators of digital services.

Operators will have to adapt to a demanding set of obligations arising from the DSA. This includes implementing transparency measures for content moderation, establishing clear procedures for the removal of illegal content and guaranteeing the protection of users’ rights. ANACOM, as the regulatory authority, will have the task of monitoring and supervising compliance with these obligations, thereby increasing the level of responsibility that operators will have to assume.

In addition, ANACOM will have to cooperate with other Portuguese and European authorities to ensure a harmonised and effective application of the DSA. For operators, this means being prepared to comply with Portuguese and EU legislation, which will require significant investment in processes, technology and technical training.

<sup>26</sup> [ANACOM - ANACOM provides 5G Portal](#).

<sup>27</sup> [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#).

<sup>28</sup> [Decree-Law 20-B/2024 of 2 February 2024](#), designating the competent authorities and the coordinator of digital services in Portugal.

## ANACOM will have to cooperate with other Portuguese and European authorities to ensure a harmonised and effective application of the DSA.

The impact of the DSA will be particularly significant in relation to data protection and users’ rights. Indeed, operators will need to implement robust systems to ensure the privacy and security of information in order to respond to growing public expectations for safer and more transparent digital platforms.

In short, the entry into force of the DSA represents a fundamental change for operators, who will have to focus very strongly on complying with the requirements arising from the applicable legislation in order to mitigate or even eliminate their liability towards ANACOM and end users.





## 6. The importance of cybersecurity in the digital age

In recent years, cybersecurity has become a key issue for electronic communications companies, particularly with the increase in cyber attacks. The need to increase resilience to the potential damage from such attacks is more important than ever.

### 6.1. EXPANDING CYBERSECURITY MEASURES

The proliferation of regulations and recommendations in recent years reflects the growing concern about cybersecurity. Key measures include the revised Network and Information Systems (“NIS2”)<sup>29</sup>, the Critical Entities Resilience Directive (“CER”)<sup>30</sup> and, most recently, the proposal for a Cyber Resilience Act<sup>31</sup>.

These measures aim to establish a high common level of cybersecurity in the European Union, promote the resilience of infrastructures and ensure the security of information networks.

NIS2 is a regulatory milestone that redefines the cybersecurity landscape in the electronic communications sector. By repealing Articles 40 and 41 of the European Electronic Communications Code (EECC)<sup>32</sup> with effect from 18 October 2024, NIS2 establishes new guidelines for the reporting of cybersecurity incidents. While Regulation 303/2019<sup>33</sup> already imposed reporting obligations, NIS2 introduces stricter deadlines and more detailed requirements.

The Directive clearly defines what constitutes a “significant incident”, which covers situations that cause serious disruption to operations. For operators, this means developing and implementing robust incident management strategies and promoting a security culture that prioritises protection against cyber threats.

**NIS2 is a regulatory milestone that redefines the cybersecurity landscape in the electronic communications sector.**

<sup>29</sup> [Directive \(EU\) 2022/2555 of 14 December](#).

<sup>30</sup> [Directive \(EU\) 2022/2557 of the European Parliament and of the Council of 14 December 2022](#) on the resilience of critical entities.

<sup>31</sup> [Proposal for a Regulation of the European Parliament and of the Council](#) on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

<sup>32</sup> [Directive \(EU\) 2018/1972 of the European Parliament and of the Council of 11 December 2018](#) establishing the European Electronic Communications Code.

<sup>33</sup> [ANACOM Regulation 303/2019 of 1 April](#), on the security and integrity of electronic communications networks.

Rapid reporting requirements – with initial alerts within 24 hours and detailed reports within 72 hours – will increase operators’ vigilance and operational agility. This new directive will not only require better preparation and response to incidents, but will also incentivise investment in technology and training to ensure that teams are ready to act effectively. NIS2 can therefore be seen as a catalyst for innovation and modernisation of cybersecurity systems in the sector.

## The creation of the Security Incident Response Centre will support organisations in managing cybersecurity incidents.

In addition, the updating of reporting thresholds – such as considering financial losses of more than €500,000 or 5% of annual turnover – will introduce a new risk dynamic that operators will need to manage carefully. The impact of NIS2 will be particularly noticeable in areas such as the provision of cloud services, where the unavailability of the service for more than 30 minutes will be enough to classify an incident as significant. This change could lead to increased demand for business continuity and disaster recovery services, thereby increasing the resilience of operations.

The implementation of NIS2 also represents a fundamental change for ANACOM. The creation of the Security Incident Response Centre, CSIRT-ANACOM, announced on 4 November 2024, is an important step in this process. This centre will support organisations in managing cybersecurity incidents, reflecting a growing trend towards collaboration and resilience in the sector.

The collaboration between ANACOM, the CSIRT-ANACOM and the National Cybersecurity Centre (“CNCS”) will encourage the creation of integrated incident response strategies, which are essential to combat emerging cyber threats. Operators will need to invest in technology and training that will enable them not only to comply with new regulatory requirements, but also to develop a robust security culture. This development should lead to greater resilience of networks and information systems, which is essential to ensure service continuity in an increasingly complex and challenging scenario.

### 6.2. THE CHALLENGES

The complexity and diversity of current European security policies calls for greater technical coordination based on concrete data on the measures needed to respond to security concerns.

The European Recommendation on Cybersecurity of 5G Networks<sup>34</sup> highlights the main challenges for the deployment of 5G networks, such as the significant costs for network operators and delays in network deployment. In particular, the Recommendation highlights the need to balance the implementation of security measures with the economic and operational viability of operators, both in terms of competitiveness and resilience.

At a national level, Portugal has faced a number of significant cyber attacks in recent years, affecting both the public and private sectors. Most recently, in October 2024, the AMA (Agency for Administrative Modernisation) suffered a cyber attack that led to the disruption of several essential digital services<sup>35</sup>.

These incidents underline the continued importance of cybersecurity and the need for robust policies to protect both critical infrastructure and citizens’ personal data. In this context, cooperation between public authorities, operators and experts is essential to develop effective and sustainable policies. Only through joint efforts will it be possible to ensure a secure and resilient digital infrastructure that can withstand the challenges and seize the opportunities of digital transformation.

<sup>34</sup> [European Commission Recommendation on Cybersecurity of 5G Networks, 2019.](#)

<sup>35</sup> [Chave móvel digital e plataformas do Estado bloqueadas por ciberataque contra AMA - Expresso.](#)

## 7. Changes in access to metadata: impact and perspectives

Law 18/2024 of 5 February<sup>36</sup> regulates access to electronic communications metadata for criminal investigation purposes.

The latest amendments aim to balance the need for access to data for criminal investigations with the protection of citizens' fundamental rights, ensuring that the storage of and access to such data is carried out in a transparent and secure manner.

### 7.1. MAIN CHANGES

Law 18/2024 establishes clear rules for the storage, judicial authorisation and security of data, promoting the responsible and transparent processing of citizens' information. The following rules stand out:

- **Data retention**

Electronic communications companies must retain for one year (i) data relating to the civil identification of subscribers or users of publicly available communications services or a public communications network; (ii) other basic data; and (iii) IP protocol addresses assigned to the source of a connection.

- **Judicial authorisation**

The retention of traffic and location data requires judicial authorisation, which must be decided within a maximum of 72 hours. This authorisation is essential to ensure that data is retained only for the purposes of criminal investigations.

- **Security and data protection**

Appropriate technical and organisational measures must be taken to ensure a high level of security, taking into account the risks to the rights and freedoms of individuals.

### 7.2. IMPACT ON THE ELECTRONIC COMMUNICATIONS SECTOR

The implementation of Law 18/2024 poses several challenges, but also represents an opportunity for electronic communications companies. The need to retain data for one year will require investment in storage and security infrastructure. In addition, companies will need to ensure that judicial approval processes are efficient to avoid delays in criminal investigations.

The law also promotes transparency and consumer confidence in electronic communications services. The provision that data must be accessed and stored securely allows electronic communications companies to brand their products and services with trust, giving them another tool to strengthen their reputation and relationship with end users.

The latest amendments aim to balance the need for access to data for criminal investigations with the protection of citizens' fundamental rights.

<sup>36</sup> [Law 18/2024 of 5 February](#), which amends Law 32/2008 of 17 July, transposes into national law Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.



# About PLMJ

→ Who we are

“PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us.”

CLIENT REFERENCE FROM  
CHAMBERS AND PARTNERS

# About the Technology, Media and Telecommunications

→ What we do

---

## KEY CONTACTS



Pedro  
Lomba

Partner

(+351) 213 197 412  
pedro.lomba@plmj.pt



Nádía da Costa  
Ribeiro

Senior counsel

(+351) 213 197 412  
nadia.costaribeiro@plmj.pt

