Playbook

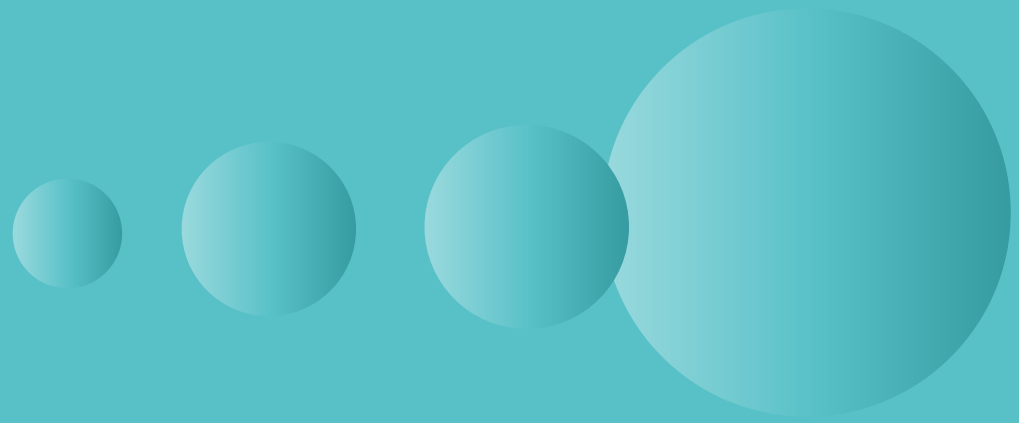
Technological Innovation

2025

Telefónica

Technological Innovation

Innovation is part of Telefónica's identity. Our innovative vision and entrepreneurial spirit have allowed us to reinvent ourselves throughout our history, bringing new opportunities to people and driving the digital, social and economic transformation of the countries in which we operate.



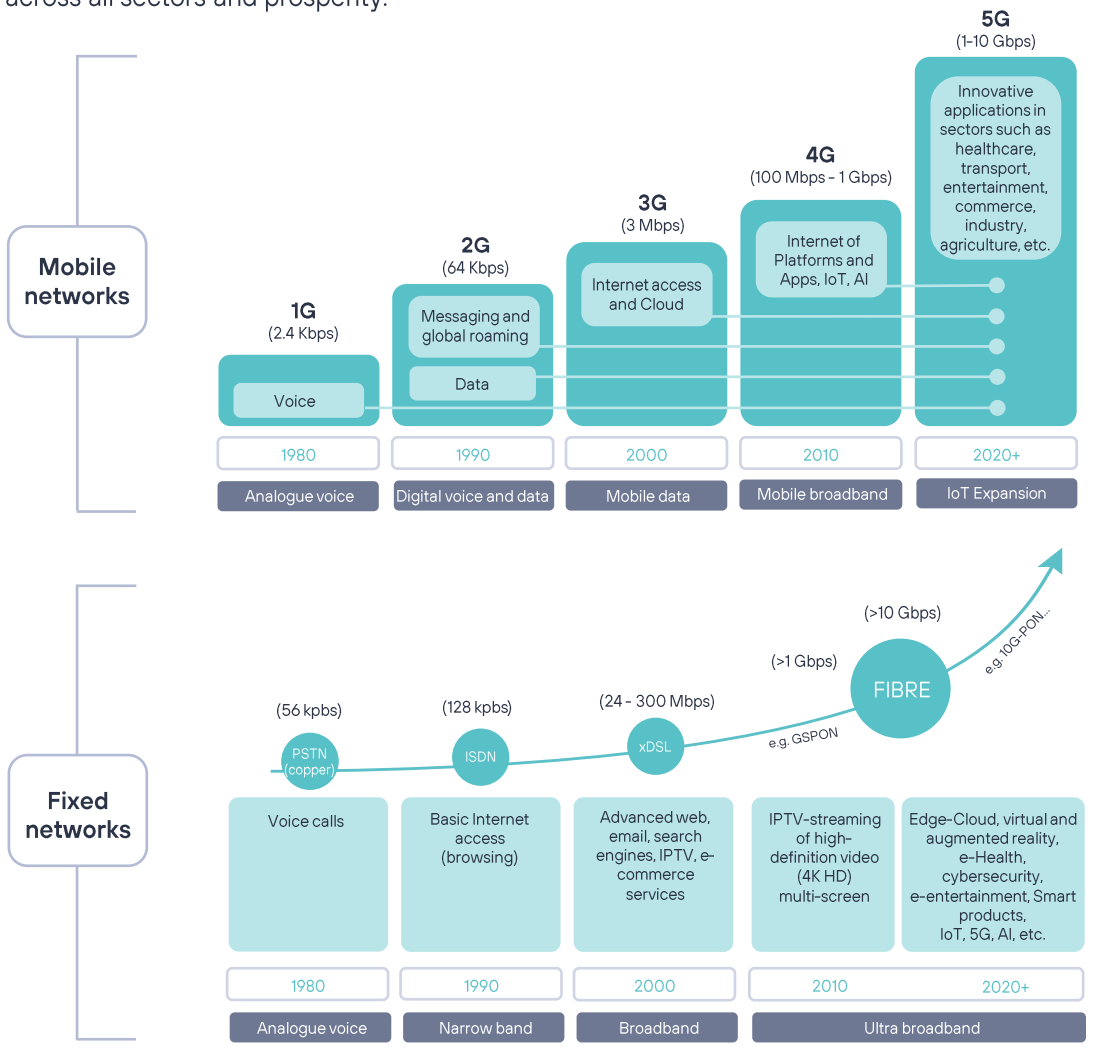
07

Connectivity: The Transformative Power of Telecommunications and its Impact on Innovation

Telefónica

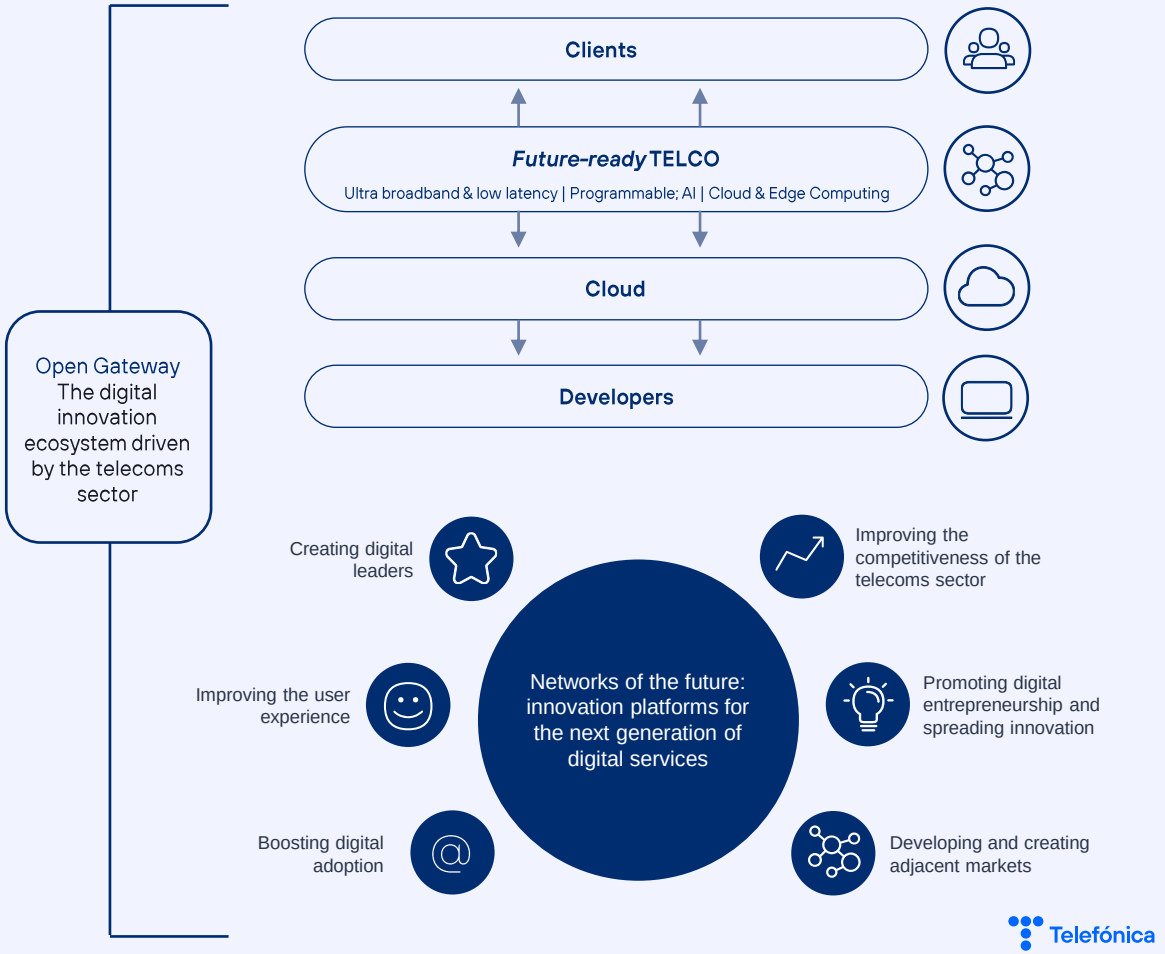
The Impact of Connectivity Transformation on Innovation

Continued investment in the telecoms sector is driving technological innovation in its networks, enabling advanced digital experiences and new opportunities for technological innovation across all sectors and prosperity.



Towards a New Era of Digital Innovation

Without investment, innovation will stagnate. A favourable investment environment must be fostered to adapt networks to the new digital era.



Telefónica

Evolve towards an enabling investment environment to transform the network and drive digital innovation and a new generation of digital services

1 Promote sustainable market structures

Reduce the fragmentation of telecommunications markets at national level to allow operators to achieve the scale necessary to strengthen the sector's capacity for investment and thus innovation.

2 Establish a regulatory framework to free up resources to speed up the deployment and transformation of networks

Reduce the administrative burden and associated costs, including tax burdens, and simplify bureaucratic procedures for deployment and transformation.

3 Encourage an investment-friendly spectrum policy

Provide certainty for license renewals and increase the harmonized supply of spectrum in the mid and low bands for terrestrial mobile networks and ensure its allocation on reasonable terms, seeking to maximize the value of spectrum for end-users.

4 Evolve the regulatory framework to foster innovation and a level playing field in the digital ecosystem

Address asymmetries with horizontal frameworks covering aspects such as competition, consumer rights, or taxation, eliminating sectoral approaches.

Restore balance to the digital value chain by fostering a fair relation between players.

Provide additional guidance on net neutrality to enable innovative use cases such as those enabled by 5G network slicing or Open Gateway.

5 Recognise the key role of connectivity to boost the green transition

Encourage the redirection of investment flows towards the deployment of more efficient networks, such as fibre and 5G.

Do you want to know more?
Read our positioning
Access related content

Context

The competitiveness of societies depends directly on the strength and modernisation of the companies present in a country or region, especially technology companies. The investment effort of these companies is essential to promote innovation, enrich the social fabric and strengthen the competitiveness of the economic structure through sustainable technological advances that are accessible to all people and businesses.

The telecoms sector is particularly important in the digital age. The development of a competitive economy and a digital society is inextricably linked to the availability of meaningful connectivity provided by high-capacity fixed and mobile networks. This connectivity is key to the digitalisation of all segments of society: businesses, public administrations and individuals. But it is also a fundamental pillar for the development of new technologies and the drive for digital innovation, enabling increasingly sophisticated digital services and experiences that promote competitiveness, sustainability and welfare.

The telecoms sector has maintained a process of continuous innovation in its systems, business strategies and especially in the development of fixed and mobile networks. As a pioneer of technological evolution, the sector plays a key role in providing meaningful connectivity to drive prosperity.

The constant flow of investment in the sector, which, for example, according to Connect Europe amounts more than EUR 50 billion per year in Europe, enables the continuous delivery of advanced digital experiences to citizens and businesses, while opening up new opportunities for technological innovation in all sectors, thus contributing to the transformation and prosperity of societies.

Challenges

Innovation in the telecoms sector cannot stand still in the face of the constantly evolving digital needs and demands of citizens and businesses.

Digital services based on technologies such as 5G, IoT, cloud computing, artificial intelligence and virtual worlds will create new economic and welfare opportunities. However, to make the most of this potential, improvements in network capabilities such as increased computing power and lower latency are needed.

In this context, the telecoms sector faces a fundamental challenge: investment. Without it, innovation will stagnate. It is imperative to invest in the modernisation of fixed and mobile networks in order to anticipate and meet growing digital demand and drive a new era of digital opportunity.

Open Gateway represents the next evolution of infrastructures by standardising network functions through softwarisation and virtualisation, transforming telecommunications infrastructures into programmable digital platforms. This will open up an innovation environment accessible to all developers, creating new opportunities and encouraging their adoption and further digital transformation.

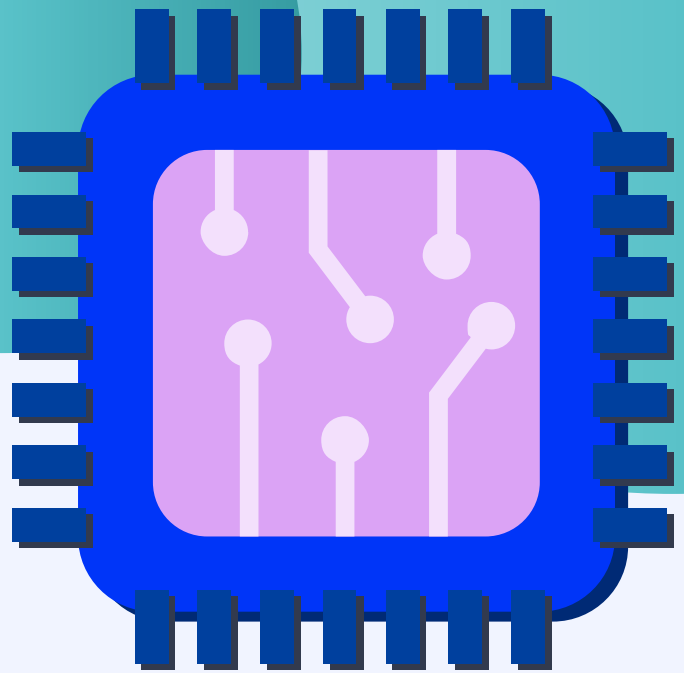
Operators see three key areas of investment for network transformation: edge computing for efficient processing close to the user; low latency technologies such as 5G and fibre; and programmable networks through global, standardised APIs. To achieve this, an environment is needed that enables operators to sustain their investment efforts, transform and innovate, helping to drive digital leadership and innovation for the benefit of society.

Recommendations

The transformation of networks into programmable platforms for digital innovation requires a favourable environment for investment. This starts with recognising the strategic role of the telecoms sector, in particular connectivity, in driving innovation, competitiveness and prosperity. It is therefore recommended to:

1. **Promote sustainable market structures**. Reduce fragmentation of markets at national level to allow operators to achieve the scale necessary to strengthen the sector's capacity for investment and thus innovation.
2. **Establish a regulatory framework to free up resources to speed up network deployment and transformation**. Reduce the administrative burden and associated costs, including taxation, and simplify bureaucratic procedures for deployment and transformation.
3. **Encourage an investment-friendly spectrum policy**. Provide certainty for license renewals and increase the harmonized supply of spectrum in the mid and low bands for terrestrial mobile networks and ensure its allocation on reasonable terms, seeking to maximize the value of spectrum for end-users.
4. **Evolve the regulatory framework to foster innovation and a level playing field in the digital ecosystem**. Address asymmetries with horizontal frameworks covering aspects such as competition, consumer rights, or taxation, eliminating sectoral approaches. In addition, restore balance to the digital value chain by fostering a fair relation between players. Furthermore, provide additional guidance on net neutrality to enable innovative use cases such as those enabled by 5G network slicing or Open Gateway.
5. **Recognise the key role of connectivity in driving the green transition**. Encourage the redirection of investment flows towards the deployment of more efficient networks, such as fibre and 5G.

08



Governance of *Artificial Intelligence* for the Future

Telefónica

AI has the potential to improve people's well-being, digital inclusion, sustainability and preserve cultural heritage, as well as being a key competitive lever in digital economies.

AI as a Factor in Competitiveness

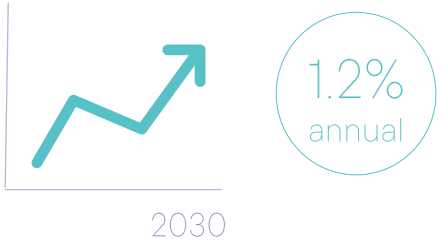
Artificial Intelligence allows...

- Customise the experience
- Minimise operating costs
- Increase productivity

+ Business competitiveness + Economic growth

Additional Global Economic Activity [1]

Additional World GDP growth [1]



The Challenges of AI Governance

The need for a harmonised governance model

In order to develop and adopt responsible, human-centred and trustworthy Artificial Intelligence, a holistic vision combining international cooperation, self-regulation, the establishment of appropriate public policies and a risk-based regulatory approach is needed.

Global fragmentation

Global concern about the challenges of AI and the need for a rapid response to ensure responsible design and use has given rise to a complex public policy environment.

Socio-economic gaps

Unequal access to AI, whether at micro or macro level, can aggravate socio-economic gaps as not all individuals or countries will be able to benefit equally from its opportunities.

Develop AI governance that ensures a balance between innovation, economic growth and the responsible use

1 Promote international definition, governance and global cooperation

Adopt an internationally recognised definition of AI, such as that of the OECD, and strengthen international cooperation to establish common principles and avoid regulatory fragmentation. A widely accepted definition of AI would provide legal certainty in the overall regulatory and policy approach, while promoting regulatory convergence.

2 Develop horizontal and risk-based regulation

Develop uniform regulation that covers all sectors and focuses on the use of AI, not just on the technology itself. This regulation should be risk-based, focusing on mitigating high risks while encouraging innovation.

Establish regulatory sandboxes and testbeds to test new technologies and regulations in controlled environments.

3 Foster self-regulation and ethical governance

Promote self-regulation so that companies assume ethical responsibility and transparency from the design of AI systems, supporting initiatives that establish internal standards and oversight processes to ensure responsible development and use.

4 Strengthen institutional governance, legal certainty and regulatory coherence

Define clear governance to avoid legal uncertainties and fragmentation of the application of regulations that could negatively impact the competitiveness of companies and the protection of individuals' rights.

Ensure consistency between AI regulation and others (GDPR, Due Diligence, etc).

5 Maintain a continuous dialogue between the public and private sectors

Maintain a continuous dialogue between the public and private sector that fosters continuous innovation while protecting Fundamental Rights, Democracy and the Rule of Law. Strike a balance between innovation and regulation.

Do you want to know more?

Read our positioning

Access related content

Context

Artificial Intelligence (AI) stands as the most influential technology of the 21st century, with unprecedented potential. Through advanced machine learning techniques, AI can autonomously analyse large volumes of data, facilitating decision-making and providing innovative and effective solutions.

Its impact is key to driving innovation and industrial competitiveness, transforming sectors, enabling new business models, and redefining labour skills. AI optimises processes, minimises operational costs, personalises the customer experience, and increases productivity, thereby boosting business competitiveness.

In global terms, AI could add $13 trillion to global economic activity in 2030, increasing global GDP by around 1.2% per year. AI has the potential to improve people's well-being. For example, by improving healthcare, education and inclusion in the workforce; promoting sustainability by maximising efficiency; streamlining humanitarian response by analysing data and developing scenarios to maximise impact; and preserving cultural heritage through intelligent management and predictive analytics. Sector applications are diverse.

In the case of telecoms operators, AI has the potential to improve the quality of service and customer care, as well as the security and efficiency of their networks.

Challenges

AI presents both opportunities and challenges, particularly in terms of its design and responsible use. From the outset, there has been a public debate in which the key challenge is to promote the development and adoption of responsible, human-centred and trustworthy AI. This means fostering innovation while ensuring a high level of protection of safety, fundamental rights, democracy, the rule of law and the environment from potentially harmful effects. This would foster trust in the technology.

Moreover, the regulatory debate requires a holistic view that combines international cooperation, self-regulation, the establishment of appropriate public policies and a risk-based regulatory approach.

AI-driven automation also entails the risk of job displacement in easily automatable sectors, which could have a significant socio-economic impacts on workers and the wider economy.

Furthermore, digital inequality could be exacerbated by unequal access to AI technology, widening existing socio-economic gaps and limiting equitable access to its benefits.

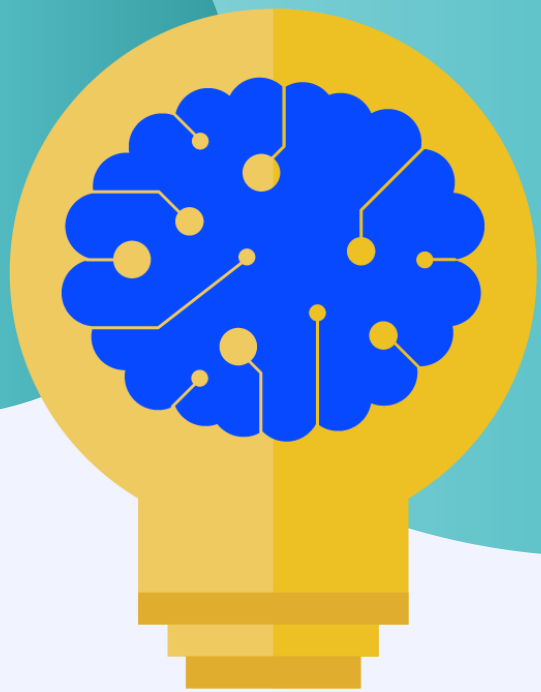
Finally, concerns about the challenges, especially in terms of their design and responsible use, have given rise to a complex public policy environment of governance. At the multilateral level, we can find UNESCO conventions, definitions of ISO standards or proposals in the UN General Assembly. At the plurilateral level, there is the work of the OECD, the EU (the Artificial Intelligence Act), the Council of Europe, the G7, the G20 or the US-EU TTC Joint Roadmap on AI. Finally, at the national level, there are initiatives such as the US White House Executive Order on AI, the US NIST Risk Management Framework or the UK's AI Principles.

Recommendations

It is imperative to develop AI governance that ensures a balance between innovation, economic growth and responsible use that respects and protects people's rights and safety. It is therefore key to:

1. **Promote international definition, governance and global cooperation**. Adopt an internationally recognised definition of AI, such as that of the OECD, and strengthen international cooperation to establish common principles and avoid regulatory fragmentation. A widely accepted definition of AI provides legal certainty in the global regulatory and policy approach, while promoting regulatory convergence.
2. **Develop horizontal and risk-based regulation**. Develop uniform regulation that covers all sectors and focuses on the use of AI, not just on the technology itself. This regulation should be risk-based, focusing on mitigating high risks while encouraging innovation and having a clear institutional governance model. In addition, establish regulatory sandboxes and testbeds to test new technologies and regulations in controlled environments.
3. **Foster self-regulation and ethical governance**. Promote self-regulation so that companies assume ethical responsibility and transparency from the design of AI systems, supporting initiatives that establish internal standards and oversight processes to ensure responsible development and use.
4. **Strengthen institutional governance, legal certainty and regulatory coherence**. Define clear governance to avoid legal uncertainties and fragmentation of the application of regulations that could negatively impact the competitiveness of companies and the protection of individuals' rights. Ensure consistency between AI regulation and others (GDPR, Due Diligence, etc.).
5. **Maintain a continuous dialogue between the public and private sectors**. Encourage a continuous dialogue between the public and private sector that fosters continuous innovation while protecting Fundamental Rights, Democracy and the Rule of Law. Strike a balance between innovation and regulation.

09



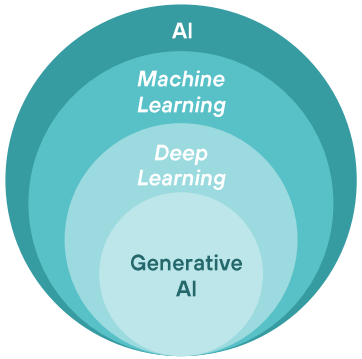
Generative AI: Competition, Intellectual Property and the Labour Market

Artificial Intelligence has the potential to revolutionise the social and economic dynamics of countries, emerging as a key competitive differentiator.

The Advent of Generative Artificial Intelligence

AI drives innovation and productivity, enabling new business opportunities and economic growth for companies and countries.

Generative models are the latest development in the field of Artificial Intelligence. However, we are still in the early stages. We are far from seeing their full potential.



It is estimated that Generative AI has the potential to generate an annual value equivalent to between $2.6 and $4.4 trillion [1] in global corporate profits.

75% of the value [1] created by Generative AI will come from:

- Transactions with clients
- Marketing and sales
- Research & Design
- Software engineering

The Challenges of Generative Artificial Intelligence

Guaranteeing Human Rights and Democratic Values

Irresponsible use of Generative AI could potentially undermine Fundamental Rights and democratic principles on which our societies are based through disinformation, attacks on privacy or mass surveillance, among others.

Fair Market Competition and Competitiveness

With access to resources such as data, computing power, finance and experts concentrated in a few companies, there is a risk of abuse of dominance, limiting innovation.

Industrial property and copyright

Input AI training with pre-existing works

Output Protection and ownership of the work created with AI

Impact on the labour market

Automation of routine and repetitive tasks + Retraining to use AI as a tool

Develop policies and regulations that promote a positive impact on intellectual property, fair competition and labour market

1 Establish policies that promote fair competition, foster innovation, and strengthen regional capacities

Ensure compliance with Competition Law to avoid abuses of dominance.

Promote the variety of business models and innovation through support for start-ups.

Strengthen local capacities through training programmes.

Stimulate investment.

2 Foster flexible regulatory environments and promote public-private dialogue in the field of intellectual and industrial property

Understand the challenges related to intellectual and industrial property in the development of Generative AI, promoting flexible and adaptable environments in different regulatory frameworks.

Encourage a continuous dialogue between the public and private sectors to balance and address the challenges arising from the implementation of this technology.

3 Prioritise investment in skills development and establish policies to limit the digital skills gap in the workplace

Focus on education, training and life-long learning programmes to equip the workforce with skills needed for an AI-driven economy.

Developing policies for digital inclusion and retraining programmes to support workers affected by automation, ensuring a transition to new employment opportunities.

Do you want to know more?
Read our positioning
Access related content

Context

Artificial Intelligence generative models (GenAI) represent the latest breakthrough in the field of machine learning, enabling the generation of a wide variety of content, from text and images to music and video, by identifying patterns in huge data sets.

This technological evolution has attracted significant interest due to its potential to drive innovation and generate new business opportunities across industries. According to estimates, generative AI has the potential to generate an annual value equivalent to between $2.6 and $4.4 trillion in global corporate profits, with 75% of this value attributed to use cases in customer operations, marketing and sales, software engineering, and Research & Development.

However, despite the excitement generated by the capabilities of generative AI, we are still in the early stages of its development and practical application. A number of challenges and concerns have been identified, ranging from ethical and privacy issues to potential data biases and the need to understand and mitigate the risks associated with the widespread use of these technologies.

In this context, the importance of effective governance of AI and GenAI becomes paramount. This governance framework includes a variety of approaches, from government regulation to self-regulation by entities involved in the development and use of AI. Government regulation seeks to establish clear standards and guidelines for the ethical and responsible use of AI, while self-regulation by companies and organisations promotes the adoption of ethical and transparent practices in the development and deployment of AI systems.

Challenges

While GenAI can be a powerful tool for improving access to education, healthcare and other vital services, we also face a number of ethical, regulatory and social challenges that we must address with urgency and determination.

Non-responsible use of this technology can undermine Fundamental Rights and democratic principles on which our societies are based. Some examples of non-responsible use are disinformation, attacks on privacy or mass surveillance.

In terms of developing and deploying AI models and applications, including GenAI, only a few technology companies have the technical capabilities and financial resources to develop the most advanced models. This can create imbalances by creating barriers to entry for smaller companies and concentrating power in the hands of a few large corporations.

In the field of Intellectual and Industrial Property, rapid advances in GenAI have resulted in a wide range of affordable and easily accessible tools for the generation of all kinds of content. However, it raises challenges related both to its forms of training for the use made of pre-existing works (input) and to the protection and ownership of the results obtained by its use (output). This has given rise to a debate on the copyright of the content created and on the ownership of patents on industrial products.

Finally, GenAI has the potential to automate routine and repetitive tasks, which can increase efficiency, but also raises concerns about job losses and the need for retraining for more specialised positions.

Recommendations

The governance model for AI, including GenAI, must ensure a balance between innovation, economic growth and responsible use of AI. It is therefore recommended:

1. **Establish policies that promote fair competition, foster innovation, and strengthen regional capacities**. Ensure compliance with competition law to avoid abuses of dominance, promote the variety of business models and innovation through support for start-ups, strengthen local capacities through training programmes, and stimulate regional investment.

2. **Foster flexible regulatory environments and promote public-private dialogue in the field of intellectual and industrial property**. Understand the challenges related to intellectual and industrial property in the development of Generative AI, promoting flexible and adaptable environments in different regulatory frameworks. In addition, continuous dialogue between the public and private sector should be encouraged to balance and address the challenges arising from the implementation of this technology.

3. **Prioritise investment in skills development and establish policies to limit the digital skills gap in the workplace**. Focus on education, training and lifelong learning programmes to equip the workforce with skills needed for an AI-driven economy, while developing policies for digital inclusion and retraining programmes to support workers affected by automation, ensuring a transition to new employment opportunities.

10

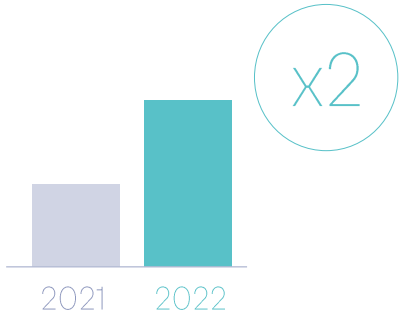
Telecoms Networks and *Virtual Worlds:* A New Internet Era

Expectations for Growth of the Metaverse [1]

59% of consumers would move their daily activity (social interaction, gaming, travel, commerce...) to the Metaverse.

2022

Investments in the development of the Metaverse doubled over the previous year, reaching $120 billion globally

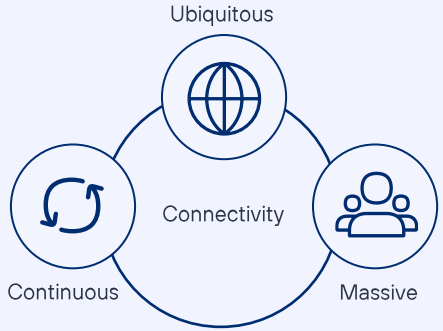


2030

It is estimated that the Metaverse could generate up to $5 trillion globally in business and consumer applications.

For Virtual Worlds to reach their full potential, it is necessary to be able to offer a continuous, ubiquitous, and massive experience.

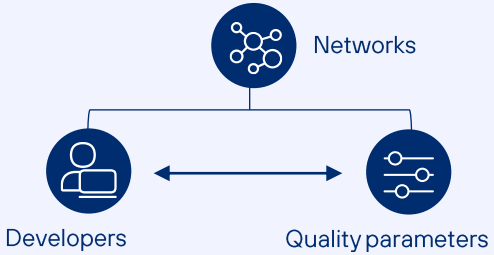
This will require networks to evolve towards a programmable, decentralised, end-user model.



Evolution of Telecommunications Networks

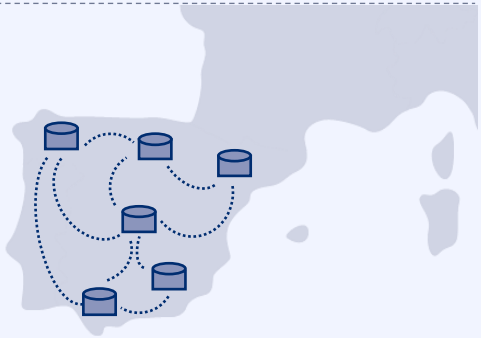
API-fication of networks

Developers of Metaverse applications and services will be able to program and define the quality parameters required for their service through interfaces (APIs).



Content Delivery Networks (CDN) model

CDNs bring content closer to users from various geographical locations, enabling new business models where the CDN provider is compensated for delivering higher-quality content.



Evolve telecommunications networks to make the Metaverse and Virtual Worlds a reality

1. Avoid the automatic extension of traditional regulation to the new technological paradigm of Virtual Worlds

Design regulation adapted to new technologies, services and business models. Incorrect interpretations, or those influenced by non-technical criteria, could create uncertainty.

2. Promote a level playing field for the harmonious development of Virtual Worlds

Establish a level playing field for all players in the digital value facing similar regulatory situations, enabling the creation of appropriate incentives for everyone involved.

3. Avoid hasty regulatory decisions

Exercise extra caution in regulatory decisions before intervening in this market, considering the impact such interventions may have on the efficiency and effectiveness of resource allocation driven by APIs.

4. Facilitate collaboration between operators in standardisation

Provide homogeneous interfaces from the operators to the developers of Virtual Worlds is a prerequisite for the success of this new era.

Do you want to know more?

Read our positioning

Access related content

Context

In 2021, Facebook's rebrand to Meta sparked the 'boom' of the Metaverse. Until then, the Metaverse had been a science fiction concept far removed from reality. However, the wave of innovation triggered by Meta prompted major tech companies to race to create the first Virtual World in the Metaverse.

The Metaverse is a network of virtual spaces accessed through different devices where users can interact, socialise, work, play and consume in an immersive digital environment that mirrors many of the habits in the real world.

Today, companies continue to innovate and invest in technologies that will support the Metaverse, such as virtual and augmented reality, gradually bringing us closer to a first version of what Virtual Worlds will be.

The economic value of Virtual Worlds is expected to increase in the coming years due to technological improvements, consumer demand for new experiences and new business opportunities for companies. According to a study conducted by McKinsey, 59% of consumers would move their daily activity (social interaction, gaming, travel, commerce...) to the Metaverse. Moreover, investments in the Metaverse doubled in 2022 compared to 2021, reaching $120 billion. By 2030, it is estimated that the Metaverse could generate between $4 trillion and $5 trillion in business and consumer use cases.

The European Commission's Virtual Worlds initiative aims to position Europe at the forefront of Virtual Worlds development. The Commission will ensure that it reflects the EU's fundamental values and rights and fosters innovation for European business and society.

Challenges

The Metaverse must offer a continuous, ubiquitous and massive experience. This means that telecommunications networks must ensure quality of service with the same requirements of continuity, ubiquity and predictability.

Therefore, the new era of the Internet will be characterised by a more personalised, faster, and lower-latency experience. However, the current internet model is constrained by the principles of best effort (which do not guarantee any specific quality) and service agnosticism (where there is no need to identify the services being offered).

Telecommunications networks will need to evolve towards a programmable, decentralised, end-user model.

Firstly, the 'API-fication' of networks will foster a new relationship between telecommunications networks, applications, and services. In this context, developers of Virtual Worlds applications and services will be able to program and define the quality parameters necessary for their services to function properly.

Secondly, by leveraging the existing model of Content Delivery Networks (CDNs), content can be delivered more efficiently by bringing it closer to users from various geographical locations, thereby improving the quality of service. This also paves the way for new business models, where content owners pay third parties (CDNs) to ensure content is delivered closer to users. In this model, it is not the end user who bears the cost of improved content delivery and quality, but rather the service providers who make this decision and handle the payment.

Recommendations

For a new Internet era characterised by the proliferation of Virtual Worlds or Metaverses to be possible, telecommunications networks need to evolve. It is therefore recommended that:

1. **Avoid the automatic extension of traditional regulation to the new technological paradigm required by Virtual Worlds**. Design regulation adapted to new technologies, services and business models. Incorrect interpretations, or those influenced by non-technical criteria, could create uncertainty.

2. **Promote a level playing field for the harmonious development of Virtual Worlds**. Establish a level playing field for all players in the digital value facing similar regulatory situations, enabling the creation of appropriate incentives for everyone involved.

3. **Avoid rushing regulatory decisions so as not to distort the functioning of Virtual Worlds**. Exercise extra caution in regulatory decisions before intervening in this market, considering the impact such interventions may have on the efficiency and effectiveness of resource allocation driven by APIs.

4. **Facilitate collaboration between operators on standardisation**. Making homogeneous interfaces available from the operators to the developers of Virtual Worlds is a prerequisite for the success of this new era.

11

Cybersecurity: Strengthening Resilience and Trust in a Global Digital World

The Importance of Cybersecurity

Top 10

Cyber-insecurity, one of the top 10 risks [1]

x2

Cyber-attacks doubled since the pandemic [2]

$9.5 Tn

... is the global cost of cyber-attacks in 2024 [3]

29%

... of organisations suffered a cyber-incident in the last year [2]

41%

... of cyber-incidents originate from the supply chain [2]

91%

... of managers expect a high impact cyber-incident in next two years [2]

There is a growing gap between cyber-resilient and non-cyber-resilient organisations

They think they lack the necessary cyber-resilience [2]

x2 SMEs vs. large companies

They have cyber insurance [2]

< 25% SMEs vs 75% large companies

In this new world, cybersecurity plays a key role in protecting businesses and governments against risks.

Obstacles to Achieving a Cyber-safe Environment

The companies with the highest risk exposure are those that:

- are in sectors digitised and connected, but without adequate protection
- have more interesting assets for attackers
- are in countries with higher strategic risk and/or worse cyber-legislation

The benefits of investment in cybersecurity are not being realised

Unlike other investments, and as in the case of R&D, it is not easy to justify the cost-effectiveness of investments in improving the resilience that cyber security offers.

Regulatory frameworks are fragmented and complex

Policy and regulation is now emerging as a fragmented, complex, cross-cutting and constantly evolving framework.

There is a shortage of specialised staff

In 2023, the gap of cybersecurity professionals amounted to approximately 4 million worldwide [4].

The profession needs to almost double to be at full capacity.

Build cyber resilience and increasing digital trust for inclusive digitisation, through better collaboration, appropriate frameworks, capacity building and incentives

Do you want to know more?
Read our positioning
Access related content

1. **Enhance multilateral cooperation against cybercrime**
   Prevent, identify and contain incidents, from investigation to legal action, by improving international and multilateral coordination against cybercrime and providing necessary resources and capabilities.

2. **Promote best practices in cybersecurity**
   Promote minimum standards including the development of independent cybersecurity agencies with resources, strategies and cybersecurity plans, encouraging private and public use of international security frameworks (e.g. ISO) and recognised certificates to facilitate transparency and harmonisation.

3. **Improve harmonisation, coherence and multi-stakeholder coordination**
   Avoid overlapping or inconsistent regulations and implementations and address coordination between competent authorities and with businesses, consistency in incident reporting systems, as well as cyber-intelligence sharing.

4. **Explore new funding mechanisms and tax incentives**
   Explore new funding mechanisms and incentives, including tax incentives, for investment in cybersecurity, resilience, capacity building and cyber security culture.

5. **Define and monitoring new key indicators at the international level**
   Define and monitor at international level new indicators for investment in cyber-security and specialised personnel, in the absence of reliable monitoring statistics in the field of cybersecurity.

6. **Establish minimum requirements to strengthen the quality of cyber rating agencies**
   Define requirements for transparency, information, sound methodology to reinforce the quality of cyber rating agencies, with regulation similar to that of credit rating agencies, and establish an official register of authorised cyber rating agencies to give more confidence to the whole ecosystem.

Context

Accelerating digitalisation, combined with rising geopolitical tensions, has been accompanied by increasing polarisation, erosion of trust and cyber-insecurity. The World Economic Forum identifies cyber-insecurity as one of the top 10 risks, and cyber-attacks are one of the top three concerns for the public and private sectors worldwide.

Since the pandemic, the number of cyber-attacks has doubled. 29% of organisations have experienced one in the last year, and 91% of executives believe a high-impact cyber-incident could occur in the next two years. The supply chain and organisational ecosystem are particularly relevant, with 41% of cyber-incidents originating from third parties. More worryingly, there is a widening gap between organisations that are cyber resilient and those that are not, as evidenced by the fact that less than a quarter of SMEs have cyber insurance compared to 75% of large organisations, and more than twice as many SMEs as large organisations report that they lack the cyber resilience needed to meet their critical operational requirements, which could slow their progress in the digital world.

The cost of cyber-attacks or leaks is rising: the average cost per incident for large organisations is $4 million. The global cost will be around $9.5 trillion by 2024, equivalent to the world's third largest economy after the US and China.

Cyber-insecurity entails direct and indirect costs, risks to people's safety and privacy, costs resulting from the disruption of services, including those critical to society, ransom payments, loss of data and relevant information, legal liability to third parties, sanctions or loss of reputation, with consequent impact on business valuation or even viability.

Challenges

Progress in digitalisation can only go hand in hand with adequate cyber resilience, fostering trust and inclusion across the productive fabric. Companies in more connected sectors or with more interesting assets for attackers, with less protection (such as SMEs), in countries with higher geostrategic risk or with poorer regulation, are at greater risk.

Since the greatest successes of cybersecurity are silent, companies may struggle to justify the return on investment in resilience. In fact, actors tend to strengthen their cyber defences after an incident, suggesting that a dynamic learning process is taking place. As with other investments, such as R&D, private incentives to address cybersecurity risks may differ from the social optimum.

Cybersecurity policy and regulation to enhance cyber resilience is currently emerging as a fragmented, complex, cross-cutting and constantly evolving risk-oriented framework in a global digital world with geopolitical tensions, where new technologies are emerging.

The motives for attacks vary, although attackers are often driven by money (organised gangs), but also by political or social causes and recognition. It is not enough to increase cyber resilience (improving the shield), but it is imperative to make effective progress in the fight against transnational cybercrime.

In this environment, cyber insurance plays a key role in risk protection. The cost of cyber insurance is rising and cybersecurity rating agencies, unlike credit rating agencies, are gaining prominence in a context of lack of transparency and regulation.

Finally, there is a serious lack of cybersecurity expertise and culture. Improving cyber resilience requires almost twice as many professionals as there are today

Recommendations

In an increasingly connected world, developing cyber resilience and increasing digital trust, for inclusive digitisation, requires better collaboration, appropriate frameworks, capacity building and incentives. It is therefore recommended:

1. **Enhance multilateral cooperation against cybercrime**, Prevent, identify and contain incidents, from investigation to legal action, by improving international and multilateral coordination against cybercrime and providing necessary resources and capabilities.

2. **Promote best practices in cyber security**. Promote minimum standards including the development of independent cybersecurity agencies with cybersecurity resources, strategies and plans, encouraging the use of international security frameworks (e.g. ISO) and recognised certificates, promoting transparency and harmonisation.

3. **Improve harmonisation, coherence and multi-stakeholder coordination**. Avoid overlapping or inconsistent regulations and implementations and address coordination between competent authorities and companies, consistency in incident reporting systems, and cyber-intelligence sharing.

4. **Explore new funding mechanisms and fiscal incentives for improving cyber resilience, capacity building, and culture** to address the necessary investments and shortage of cyber professionals.

5. **Define and monitor new key indicators at international level**. Of investment in cybersecurity and specialised personnel, in the absence of reliable statistics.

6. **Establish minimum requirements to reinforce the quality of cyber rating agencies**. Define requirements for transparency, information, methodology, with regulations similar to those for credit rating and set up an official register of authorised cyber-rating agencies to increase confidence.

12

Early Warning Systems: A Vital Shield Against Natural Disasters

In 2022, 387 natural hazards and disasters were recorded worldwide, causing the loss of 30,704 lives and affecting 185 million people. [1]

95% of the global population is covered by a mobile network and there are 5.6 billion unique mobile phone subscribers worldwide. This network plays a vital role in disseminating and communicating early warnings of risks. [1]

Early Warning Systems with the Mobile Network as a Channel

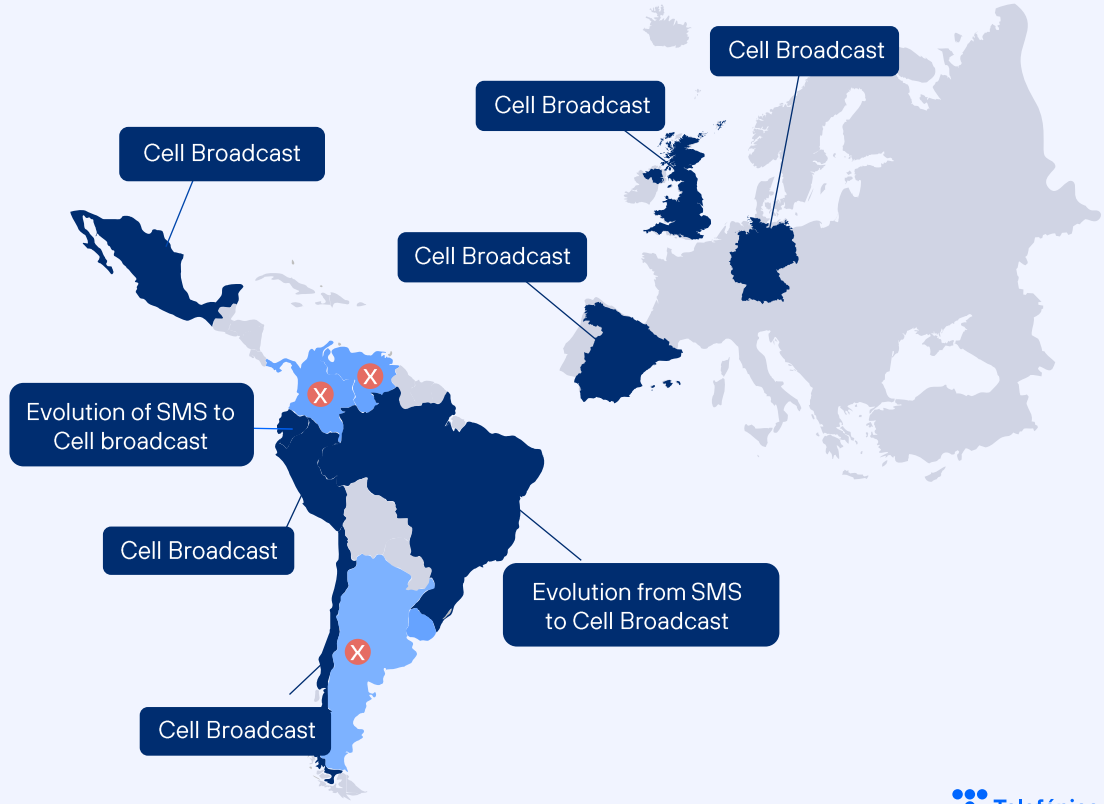
Cell Broadcast: the Most Efficient Technology

Early Warnings for All

The UN's Early Warning for All initiative aims to ensure that by 2027 the world's entire population is covered by an early warning system that provides universal protection against hydro-meteorological, climatological and hazardous environmental events.

Telecoms Operators' Commitment to Early Warning Systems

Cell Broadcast is the most widely used technology in the Telefónica footprint



Telefónica

Accelerate the deployment and effectiveness of early warning systems by integrating mobile networks as a critical and complementary communication channel within a multi-channel approach

Do you want to know more?
Read our positioning
Access related content

1 Foster public-private partnerships

Share knowledge and best practices between operators, device manufacturers, software manufacturers, government officials, international organisations, emergency experts and others. In particular, mobile operators provide technical expertise and knowledge and make their equipment available to emergency centres.

2 Establish regulatory frameworks aligned with the financing of these services

Establish a regulatory framework that creates certainty and incentives for the deployment of early warning systems.

Explore innovative financing solutions that are viable in the long term and ensure funding of up-front and ongoing costs.

3 Promote the adoption of the most effective technological solution based on national, regional or local realities

Consider the technologies and range of devices available in each country/area. However, cell broadcast technology should be prioritised for its advantages and integrated into existing contingency plans.

Promote the homologation of devices to ensure their compatibility with the early warning service.

Promote the multi-channel approach for dissemination through different channels and the development of a common protocol to ensure consistency of the alert across channels, thereby increasing its reach.

4 Raise public awareness

Prepare the population and increase their confidence and familiarity through regular simulations and awareness campaigns. These exercises and campaigns are key to ensuring the effectiveness of the warning service and should be led by the government, as it is a public service, while emphasising the role of operators as an additional channel for disseminating warnings.

Context

The increase in natural disasters linked to climate change has highlighted the urgency of implementing technological solutions to quickly alert people to impending hazards. The UN's "Early Warning for All" initiative, launched in 2022, aims to ensure that everyone in the world is covered by an early warning system by 2027, guaranteeing universal protection against hydro-meteorological, climatological and environmental hazards.

A comprehensive and efficient early warning system integrates four key functions: risk assessment; monitoring and forecasting of natural disasters; communication and dissemination of warnings; and response capacity.

In this context, the availability of broadband and the widespread use of internet-enabled mobile devices make operators and their mobile networks an important channel for disseminating warnings. Today, the most effective early warning systems are characterised by a multi-channel approach. Thanks to technological advances, the mobile network and mobile devices have been integrated into these systems, complementing traditional means of disseminating warnings such as radio, TV, newspapers, billboards or sirens, increasing their reach and improving the effectiveness of this public service for the benefit of communities and the safety of individuals.

Cell Broadcast is the most effective and reliable technology for mass delivery of mobile alerts in seconds and is the most widely used technology in the world. Unlike SMS, this technology sends the alert to all connected mobile phones in a given geographical area, including roaming phones, without the need to know the number, preserving privacy, saving lives and reducing damage.

Challenges

Several challenges need to be addressed to increase the deployment and effectiveness of these systems. First, many countries, especially developing countries, lack the necessary infrastructure for early warning systems, or if they do have it, it does not integrate mobile networks as a warning dissemination channel.

This is compounded by a lack of knowledge about the technologies involved and/or technology partners, as well as the uneven availability and quality of mobile networks and compatibility issues between mobile devices and the early warning service.

Similarly, securing long-term funding and establishing sustainable funding models is critical to the viability of these systems. It is important to note that while government agencies are responsible for issuing alerts, telecommunications operators only provide the network infrastructure and act as a transmission channel. However, the deployment of these systems requires significant investment in infrastructure, technology and human resources, which affects both government agencies and mobile operators.

On the other hand, the lack of a regulatory framework to encourage the deployment of these systems is another challenge. The dependence of this public service on mobile networks puts the focus on regulation to speed up its implementation and integration into emergency plans. Article 110 of the European Electronic Communications Code, for example, has highlighted the crucial role of regulation in accelerating deployment in European countries.

Finally, lack of knowledge about the service or lack of awareness among the population can lead to ineffective warnings.

Recommendations

The modernisation of early warning systems for potential natural disasters involves the integration of mobile networks as a crucial communication channel. It is therefore recommended:

1. **Foster collaboration between the public and private sectors**. Share knowledge and best practices between operators, device manufacturers, software manufacturers, government officials, international organisations, emergency experts and others. In particular, mobile operators provide technical expertise and knowledge and make their equipment available to emergency centres.

2. **Establish regulatory frameworks aligned with the financing of these services**. Establish a regulatory framework that creates certainty and incentives for the deployment of early warning systems and explore innovative financing solutions that are viable in the long term and ensure funding of up-front and ongoing costs.

3. **Promote the adoption of the most effective technological solution based on national, regional or local realities**. Consider the technologies and the range of devices available in each area. However, cell broadcast technology should be prioritised for its advantages and integrated into existing emergency plans. Also, promoting the homologation of devices is key to ensure the effectiveness of warning dissemination, as well as combining different channels (multi-channel) and promoting the development of a common protocol for the coherence of warning between channels.

4. **Raise public awareness**. Prepare the population and increase their confidence and familiarity through regular simulations and awareness campaigns. These exercises and campaigns are key to ensuring the effectiveness of the warning service and should be led by the government, as it is a public service, while emphasising the role of operators as an additional channel for disseminating warnings.

References | Technological innovation

07 *Connectivity:* The Transformative Power of Telecommunications and its Impact on Innovation

(1) Telefónica (2024). The transformative power of telecommunications and its impact on innovation. Available at: https://www.telefonica.com/en/wp-content/uploads/sites/5/2023/12/transformative-power-telecommunications-impact-innovation-positioning-2023.pdf
(2) Telefónica: #Connectivity. Available at: Articles and news Connectivity – Telefónica

08 A Governance of *Artificial Intelligence* for the Future

(1) McKinsey (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. Available at: https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy
(2) McKinsey (2023). AI could increase corporate profits by 4 trillion a year according to new resech. Available at: https://www.mckinsey.com/mgi/%20overview/in-the-news/ai-could-increase-corporate-profits-by-4-trillion-a-year-according-to-new-research
(3) Telefónica (2023). Artificial Intelligence: Innovation, ethics and education. Available at: https://www.telefonica.com/en/wp-content/uploads/sites/5/2023/06/Positioning-Artificial-Intelligence-innovation-ethics-and-regulation.pdf
(4) Telefónica: #Artificial Intelligence. Available at: https://www.telefonica.com/en/tag/artificial-intelligence/

09 *Generative AI:* Competition, Intellectual Property and the Labour Market

(1) Telefónica (2024). Artificial Intelligence and Generative AI: governance, competition, intellectual property and labour market. Available at: https://www.telefonica.com/en/wp-content/uploads/sites/5/2024/09/Artificial-Intelligence-and-Generative-AI.-Position-paper-2024-3.pdf

10 Telecommunication Networks and *Virtual Worlds:* A New Internet Era

(1) McKinsey (2022). Value creation in the Metaverse. Available at: www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20Metaverse/Value-creation-in-the-Metaverse.pdf
(2) Telefónica (2023). Telecommunications networks and the Metaverse. Available at: https://www.telefonica.com/en/wp-content/uploads/sites/5/2023/02/Politicas-Publicas-Telecommunication-Networks-and-Metaverse.pdf

11 *Cybersecurity:* Strengthening Resilience and Trust in a Global Digital World

(1) World Economic Forum (2024). The Global Risk Report 2024. Available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
(2) World Economic Forum (2024). The Global Cybersecurity Outlook 2024. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
(3) Esentire (2023). 2023 Official Cybercrime Report. Available at: https://www.esentire.com/resources/library/2023-official-cybercrime-report
(4) World Economic Forum (2024). Bridging the cyberskills gap. Available at: https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home
(5) International Monetary Fund (2024). The Last Mile: Financial Vulnerabilities and Risks (Chapt. 3). Available at: https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024
(6) Cisco (2024). Cybersecurity Readiness Index Available at: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf
(7) Telefónica (2024). Cybersecurity: building resilience and trust in a digital world. Available at: Cybersecurity: building resilience and trust in a digital world - Telefónica
(8) Telefónica. #Cybersecurity. Available at: https://www.telefonica.com/en/tag/cybersecurity/

12 *Early Warning Systems:* A Vital Shield Against Natural Disasters

(1) OECD (2024). Towards disaster-resilient infrastructure in Latin America: financing and governance. Available at: https://www.oecd-events.org/infrastructure-forum/session/03b28633-64b5-ee11-bea0-000d3a49ee24/breakout-6b-towards-disaster-resilient-infrastructure-in-latin-america-financing-and-governance-
(2) European Environment Agency (2023). Economic losses from weather- and climate-related extremes in Europe. Available at: https://www.eea.europa.eu/en/analysis/indicators/economic-losses-from-climate-related
(3) GSMA (2023). Cell Broadcast for Early Warning Systems. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2023/11/Cell-Broadcast_R.pdf
(4) Telefónica (2023). Early Warning Systems: a vital shield against natural disasters. Available at: Early warning systems: A vital shield against natural disasters - Telefónica

Telefónica

Follow the conversation...

Blog

LinkedIn

Newsletter

2025

Digital Public Policy, Regulation and Competition

Telefónica