OECD publishing

COMMUNICATION REGULATORS OF THE FUTURE

OECD DIGITAL ECONOMY PAPERS

October 2022 **No. 333**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report on "Communication Regulators of the Future" was prepared by the Working Party on Communication Infrastructure and Services Policy (WPCISP). It explores the critical role communication regulators play in an increasingly connected society and identifies the objectives, challenges, measures to face these challenges, and capabilities of communication regulators of the future.

This report was authored by Maximilian Reisch, Inmaculada Cava Ferreruela, and Hokuto Nakagawa, with contributions by Lauren Crean, Alexia González Fanfalone, and Verena Weber of the OECD Secretariat and WPCISP delegates regarding their country experiences. The section on the "Capabilities of the communication regulator of the future" was drafted by Martha Baxter and Vincent van Langen of the Regulatory Policy Division (REG) of the Directorate for Public Governance (GOV) of the OECD Secretariat and was discussed by the OECD Network of Economic Regulators. The report was prepared under the supervision of Verena Weber.

This report was approved and declassified by the Committee on Digital Economy Policy (CDEP) on 27 September 2022 and was prepared for publication by the OECD Secretariat.

This publication is a contribution to IOR 1.3.1.3.2 "Regulators of the Future" of the 2021- 22 Programme of Work of the CDEP.

Note to Delegations:

This document is also available on ONE as:

DSTI/CDEP/CISP(2022)2/FINAL

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

EXECUTIVE SUMMARY

This report on "Communication Regulators of the Future" explores the critical role communication regulators play in an increasingly connected society. It identifies the challenges stemming from the digital transformation of our societies, the main policy objectives pursued by communication regulators, measures to address current and future challenges, as well as the importance of strengthening the capabilities of communication regulators of the future. The main takeaways are the following.

The digital transformation is posing new challenges to current roles and mandates of communication regulators to which regulators need to adapt

The communication sector is undergoing high-paced developments driven by the digital transformation of our economies and societies. Given a rapidly changing external context, communication regulators have come under increased scrutiny, raising the question of whether they are adequately equipped to fulfil their mandate of expanding the benefit of communication services for all in society. As a consequence, countries need to guarantee that communication regulators have the appropriate mandate, functions and powers to ensure they can deliver on policy objectives. The underlying policy objectives of communication regulators are the compass guiding the adaptation process to face current and future challenges.

The key question for OECD policymakers is no longer whether regulatory structures need to change, but rather how

Technological and market developments have important effects on how communication regulation will need to be shaped in the future as the boundaries between traditional communication markets and broader digital markets and players are blurring with new issues arising in areas such as competition, content, or consumer protection. Addressing the challenges posed by the digital transformation requires that communication regulators ensure there is coherence in regulatory approaches.

Technological convergence has led to an evolving competitive landscape. Furthermore, new challenges arise from the handling of personal data, including ensuring privacy and safety online. In addition, communication regulators are increasingly acknowledging the positive and negative effects of communication infrastructures and services on the environment. Moreover, there is a growing need to ensure the resilience of networks, stemming partially from the effects of climate change. Nevertheless, the lack of legal mandates for the communication regulator to be able to intervene with regard to the environmental sustainability of communication networks can often be identified as a constraint to take further actions beyond knowledge building and the collection of information.

To address the challenges stemming from the digital transformation, OECD countries may follow several approaches, which are not mutually exclusive. Countries may opt to promote changes in legislation that adjust or partially expand communication regulators' responsibilities or oversight concerning new issues arising from the digital transformation. For example, there is an increasing integration of responsibilities on communication and broadcasting in one regulatory body in many OECD countries. At present 15 out of 38 OECD countries (39%) have a converged communication and broadcasting regulator, and 45% of communication regulators in the OECD, Brazil, and Singapore report to have partial responsibilities related to digital security. Furthermore, countries may navigate current regulatory frameworks to adapt them to an environment characterised by convergence. Finally, some countries are engaging in early discussions regarding a new type of regulatory body to tackle digital issues in a holistic manner, which includes questions of how this new body would interact with existing communication regulators. In addition, countries may increase regulatory co-operation with other agencies and government bodies.

"Back to the basics": Existing "traditional" communication regulations will only become more relevant as networks continue to evolve

Countries can help ensure that high-quality broadband connectivity reaches most of the society by strengthening regulatory frameworks that foster investment and promote competition. Adapting existing regulations to foster the deployment of the next evolution of broadband networks will become increasingly relevant. In this context, regulations that were originally designed for the transition to a liberalised market, such as wholesale access regulation, are being adapted to favour investment in high-speed, fibre and 5G- based networks. With the same objective, regulatory measures on infrastructure sharing are increasingly relevant, in particular to favour deployment in higher cost areas. Fostering infrastructure sharing and co-investment practices can furthermore help reduce the environmental impact of network deployment. Overall, there is a trend towards fine-tuning regulations to intervene in the market only where necessary and in the most effective way possible (e.g. by segmenting markets), which undoubtedly requires advanced regulator capabilities.

To meet future challenges, equipping communication regulators with new skills and digital tools, adopting data-driven regulatory approaches, as well as enhancing collaboration with other agencies, will be crucial

Communication regulators of the future will need commensurate capacity and capabilities to deliver upon their mandate, in a context where market evolutions and the rise of the digital transformation are reshaping functions and expectations. Three areas are critical in this regard.

First, “future-proof” regulators should enhance their capabilities by continually investing in their skills to keep pace with technological developments and market transformation. This may require bringing in new skills – in particular data and digital skills – via a number of means (recruitment, training and professional development, outsourcing) and conducting foresight exercises to anticipate developments. Regulators may sometimes benefit from more flexibility in the ability to bring in skills, which in some cases may be constrained by public administration rules and frameworks regarding recruitment and remuneration.

Second, regulators are increasing their use of digital tools and big data to improve their impact. Data-driven regulatory approaches have the potential to bring benefits through the automation of processes and the empowerment of consumers with real-time information on sector performance; however, these approaches depend on appropriate powers for data collection and publication and fit-for-purpose data governance structures. Digital tools and better data could also enable a shift to outcome-focused regulations.

Third, regulators need the capacity and legal clarity for regulatory co-operation, both at the domestic and international level. In practice, communication regulators across OECD countries rely on both informal and formal co-operation mechanisms to support the achievement of objectives, which will become increasingly important in light of the blurring of traditional market boundaries.

Table of contents

Tables

Figures

Boxes

Communication Regulators of the Future

Introduction

The communication sector is in constant evolution and undergoing high-paced developments. These include changes in network infrastructure and architecture, upgrades to new technologies, the convergence of fixed and mobile networks, an increased integration of the communication sector into all sectors of the economy, the emergence of new business models, and an increasing interlinkage between communication networks, Artificial Intelligence (AI) systems, the Internet-of-Things (IoT), distributed ledger technology (DLT) and digital security.

These trends are accompanied by a continued increase of expectations around coverage and quality-of-service of broadband networks. In addition, not least since the COVID-19 pandemic, broadband connectivity has been recognised as one of the key enablers of economic continuity and social interaction in times of crisis and, as such, will be key for economic recovery and social welfare. Consequently, the necessity of ubiquitous access to high-quality broadband connectivity for the digital transformation has become even more evident.

Communication regulators have an important role in an increasingly connected society and economy to contribute to the achievement of the goal of expanding broadband connectivity and quality of communication services. Given the changing communication landscape and the increased integration of broadband connectivity into all sectors of the economy, countries have started to reassess and adjust the mandates, roles, and tools of communication regulators to face current and future challenges.[1]

This report discusses key challenges communication regulators are facing and the state of play concerning suitable competencies, regulatory measures and required capabilities to oversee and regulate the communication sector in a larger sense. The document is divided into five parts.

- The first section ("The digital transformation driving an evolving communication regulatory landscape"), sets the scene by presenting the current context driven by the digital transformation, how it is evolving, and the challenges it poses for communication regulators.
- The second section ("Policy objectives of communication regulators of the future") presents some of the objectives that may be considered when characterising communication regulation at present and in the future.
- The third section ("Communication regulators meeting the challenges stemming from the digital transformation") assesses selected trends in the communication sector, the challenges these trends raise for regulators, and how communication regulators around the OECD are facing them at present and going forward. The selected trends include convergence, new business models stemming from the digital transformation, increasing security threats on networks, more complex privacy concerns, and a higher awareness of the environmental sustainability of communication networks.
- The fourth section part ("Adapting existing regulations to face the challenges of the future") explores existing regulations that will become increasingly important in the near future. It analyses regulatory measures that are considered especially relevant to achieve identified policy objectives,

such as promoting competition and fostering investment. Namely, the regulations discussed are wholesale access regulation, infrastructure sharing and co-investment.

- The fifth section of the report ("Capabilities of communication regulators of the future") sheds light on how regulators are adapting their skills and capacity to exploit digital tools and data-driven approaches as well as the importance of regulatory co-operation in facing the challenges of the future.

The digital transformation driving an evolving communication regulatory landscape

Without broadband connectivity there is simply no digital transformation. As such, communication regulators are responsible for the key enabler of digital transformation – communication networks. High-quality, resilient, and affordable broadband connectivity is required for the provision of a broad array of digital services, including Industry 4.0, the use of AI systems and the IoT, which is placing new demands on communication networks. The latter will not only determine the competitive advantages of the economy stemming from the use of the latest generations of fixed and mobile networks, but will also play an important role in bridging persisting and new digital divides. Therefore, high-quality broadband connectivity needs to reach everyone in society for a successful and inclusive digital transformation.

With an accelerated digital transformation, not least during the pandemic, networks have been increasingly converging linking previously distinct sectors (e.g. communication and broadcasting), and services delivered over IP networks have been converging, starting with the more "traditional" digital services such as digital content (e.g. video), or social media. In addition, trade activities are more and more digital and reliant on communication networks. That is, numerous sectors of the economy have been transformed as products and services move online and as many industrial services increasingly include digital elements.

These developments all have implications on how digital and communication markets are shaped and how these markets converge. This, in turn, has important effects on how communication regulation will need to be shaped in the future as the boundaries between traditional communication markets and broader digital markets and players are blurring with new issues arising in areas such as competition, content or consumer protection. In addition, as economic and social activities increasingly move online, it places higher requirements on the security and resilience of communication networks, which are two areas that communication regulators consider more and more and integrate in their work.

An evolving external context shaping communication markets and raising new challenges

New communication operator business models, changes in competition dynamics, and evolving broadband networks are leading to important changes in the broadband connectivity ecosystem. Different configurations of "operators" investing in network deployments are arising as new business models emerge (OECD, 2019[1]).[2] With the pervasiveness of technological convergence, there are new trends in communication market competition, with significant influence in the competitive landscape in OECD communication markets, as well as the incentives to invest in networks (OECD, 2021[2]). Moreover, to meet the increasing demands of applications across all sectors of the economy, from online education, telemedicine and sustainable development, to smart factories, smart hospitals to automated vehicles, networks need to continue to evolve (OECD, 2022[3]).

The complexity of the issues dealt with by communication regulators are increasing with a rapidly changing broadband connectivity ecosystem and as the digital transformation takes hold linking previously disconnected markets. For example, new forms of convergence are emerging in the communication sector that stem from the blurring of traditional communication market boundaries with broader digital services.

This includes the entry of communication operators into other sectors, such as the payment services market (e.g. Fintech), as well as greater interaction with providers in other sectors, such as the energy sector (e.g. broadband connectivity solutions for smart grids) or transport sectors (e.g. Wi-Fi and 5G connectivity solutions for connected and fully automated vehicles), to name a few examples. Moreover, there is an increasing role of "non-traditional" players, such as content providers and cloud service providers, in the broadband connectivity ecosystem. Additional complexities may arise when previously disconnected markets are connected due to technological change, where the oversight of these markets is under the remit of existing, but different regulatory bodies.

Networks of the future are moving towards greater virtualisation and openness, integration of cloud services into networks, and increased use of AI systems (OECD, 2022[3]). As such, some policy issues (e.g. digital security, privacy protection) that perhaps a decade ago may have been seen as separate from communication infrastructure, given the conceptual distinction of the application and infrastructure layer, increasingly become embedded in how networks are deployed. Furthermore, the next evolution of broadband networks will require important investments to reach broadband connectivity goals. In this sense, promoting competition and reducing network deployment costs to foster investment in broadband networks will be crucial to fully reap the benefits of the digital transformation and bridge connectivity divides.

Policy responses in light of these challenges

Given this rapidly changing external context, with the convergence between formerly distinct sectors, the increasing complementarity of fixed and mobile networks, the evolution of fixed and mobile networks (i.e. 5G and high-capacity fixed networks), new questions in the area of communication policy and regulation are arising.

Communication regulators are faced with the need to adapt to fulfil their policy objectives. However, the key question in policymakers' minds is how to do so? While OECD countries are facing common challenges stemming from rapid technological developments, every country has a unique "regulatory journey". As a first step in the pursuit of answering the complex question of "how to adapt", the ambition of this report is to present the state of play of how OECD countries are responding to these challenges by either adapting the mandates of communication regulators or by navigating current frameworks.

OECD countries are responding to the challenges arising from the digital transformation in several ways, which are not mutually exclusive.

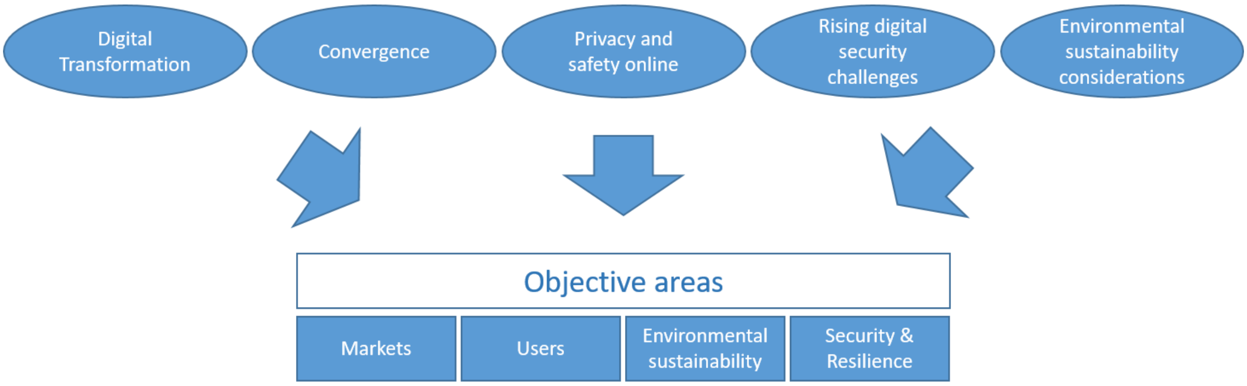
- Countries may opt to promote changes in legislation that adjust the mandate (and legal powers) assigned to communication regulators to enable them to respond to developments in the communication sector (see Convergence changing the "playing field"). This may also include partial responsibilities of communication regulators in broader digital economy issues.
- Countries may adapt the existing communication regulatory framework to adapt it to a convergent environment and evolving connectivity ecosystem. For example, the next evolution of networks will require important investments with an effect on the competition dynamics, where facilitating network sharing, incentivising co-investment, and enabling wholesale access are key regulations (see Adapting existing regulations to face the challenges of the future).
- Finally, countries may invest in regulatory capacity building and upskilling (see Skills for the future) and foster regulatory co-operation with other agencies and government bodies (see Regulatory co-operation).

Countries have taken stock of the accelerated digital transformation and have addressed the relationship between the communication sector and the broader digital transformation in their digital country strategies. For example, the Slovak Republic's vision for digital economy as set out in the *Strategy on Digital transformation (2030)* puts forward the role of regulation, its support to develop innovative services and respective needs for its simplification (Office of the Deputy Prime Minister for Investments and Informatisation of Slovakia, 2019[4]).

Communication regulators across the OECD are adapting to these new developments. Some undertake this through integrating new areas of work and some are reshaping internal structures. The German Federal Network Agency (*Bundesnetzagentur*, BNetzA), for example, has established a new subdivision dealing with "digitalisation, internet and market analysis" composed of different units. The tasks of these units include, among others, data and platform economy, Internet economy, the analysis of new services and technologies (e.g. the use of Blockchain and AI systems), net neutrality issues and geo-blocking. In addition, one unit accompanies the digitalisation process for small and medium-sized enterprises, and another unit implements the GAIA-X funding programme[3] (Bundesnetzagentur, 2022[5]).

The following areas shed more light on the convergence of regulatory authorities as well as some selected additional areas of work that some regulators in OECD countries have taken on: privacy and safety online, digital security and the environmental sustainability of communication networks. For example, moving more and more economic and social activities online puts higher requirements on the security and resilience of communication networks which are two areas that communication regulators increasingly consider and integrate in their work. In addition, the convergence of digital services over IP networks also raises the question of a need for a converged approach towards regulation (Figure 1). The next section of the report highlights the policy objectives sought by communication regulators, and then will present these areas of work throughout the different sections of the report.

Figure 1. Selected trends shaping the communication regulatory landscape and the objectives of communication regulators


Digital Transformation
Convergence
Privacy and safety online
Rising digital security challenges
Environmental sustainability considerations
Objective areas
Markets
Users
Environmental sustainability
Security & Resilience

Source: OECD

Objectives of communication regulators of the future

In a highly dynamic environment and a constantly evolving context, there is a need to clarify the actual objectives of communication regulation. While the objectives of communication regulation also undergo changes and depend on specific circumstances of countries, they give continuity to the work of regulators and serve as a compass to help define the role of communication regulators now and in the future.

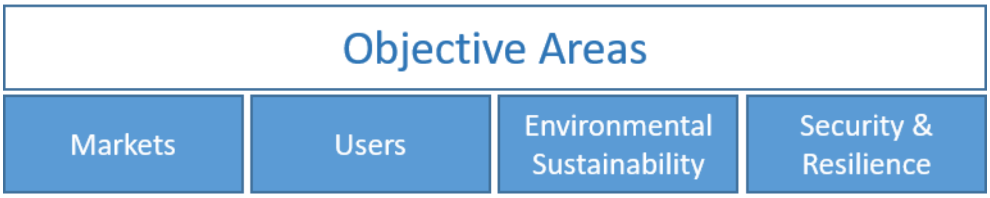
In a context in which countries have moved away from direct governmental provision of goods and services towards a greater reliance on the market to provide them and ensure economic growth (OECD, 2021[6]), governments intervene through regulation and other policy instruments in the public interest, that is, to meet other societal demands in different areas including, such as social policy, the environment, or individual rights. To this end, governments may intervene in the operation of markets for economic efficiency when they fail to achieve optimal outcomes, as in the case of "market failures", but also to achieve other objectives, such as the equitable distribution of income and wealth, environmental protection, consumer rights, privacy and personal data protection (OECD, 2002[7]).

Regulation in its many forms – from parliamentary law to ministerial orders to municipal ordinances – is one of the most powerful forms of intervention available to governments to achieve the above-mentioned policy objectives (OECD, 2021[8]). As the OECD Recommendation of the Council on Regulatory Policy and Governance sets out, regulation should start from a policy objective and an informed comparison of a variety of regulations and other policies, to proceed to draft and adopt regulation through evidence-based decision-making (OECD, 2012[9]).

The underlying objectives of regulation in the field of broadband connectivity are largely common among OECD countries, although their emphasis may differ, reflecting different specific economic and political circumstances. This section aims to present a broad overview of these shared objectives, based on the analysis of the objectives of the different countries, and brings together the different options in a structured way. These objectives are also contained in the Recommendation on Broadband Connectivity (OECD, 2021[10]), which was developed following an exhaustive participatory process involving all OECD countries and other stakeholders.

The policy objectives identified after this process can be grouped along the dimensions of markets, users, environment, and security and resilience.

Figure 2. Objective areas of communication regulation



Source: OECD

Markets

Market objectives include the improvement of the efficiency and performance of communication markets, which are the primary providers of broadband connectivity. Given that the public interest of connectivity lies in the benefits it brings to the economy and society, the ultimate goal of regulation in this area is to achieve widespread deployment of high-quality networks as well as ubiquitous and affordable access to communication services, including in areas with low profitability such as rural areas.

Objectives in the area of markets can be further broken down into promoting competition in all markets for high-capacity network infrastructures and services, fostering investment in high-quality broadband network deployment, reducing barriers to network deployment, fostering innovation to improve broadband connectivity, and efficient spectrum management for long-term societal and economic benefits.

Objectives

Promoting competition in all communication markets

Since the liberalisation of the communication sector in the early 90s, fostering competition has been at the heart of communication regulation. Well-designed, evidence-based regulatory intervention to foster competition not only avoids potential market failures of a sector typically consisting of a small number of players, but it also fosters investments and innovation in communication markets, as well as having an important role to ensure the affordability of communication services.

Fostering investment in high-quality broadband network deployment

The transition to the next evolution of broadband networks requires significant investments. Therefore, regulatory measures that make these investments more cost-effective can boost future deployments. In particular, co-investment and infrastructure sharing practices are increasingly playing a central role to facilitate a quick and efficient network rollout of these networks (see Infrastructure sharing and co-investment). Depending on the objectives of the regulator in a given market, allowing or requiring co-investment and infrastructure sharing may be useful tools to reduce network deployment costs and thus foster incentives to invest.

Reducing barriers to network deployment

The densification of infrastructures inherent to the deployment of high-capacity networks increases the intensification of civil works and with it, the need to obtain permits and rights of way. It also implies a greater need for the use of third-party facilities subject to their own regulations, usually depending on different administrative levels (e.g. local or regional). These circumstances often pose significant barriers to network deployment, such as administrative costs, or delays. Therefore, reducing network deployment barriers by streamlining administrative procedures, increasing transparency or simplifying the administrative complexity (e.g. through one-stop-shops), is a relevant policy objective for communication regulation. However, the challenge is that this regulation should be addressed jointly, involving all relevant bodies, at all administrative levels.

Fostering innovation to improve broadband connectivity

Innovation in the communication sector has the potential to drive the expansion of networks, the demand for communication services as well as network quality and new services. Innovation in communications has also multiplier effect in other sectors. Regulators have thus an important role in encouraging innovation, research, and development to improve broadband connectivity, its use, and its applications.

Efficient spectrum management for long-term societal and economic benefits

Maximising the value of the efficient use of spectrum, a scarce public resource, for long-term societal and economic benefits, is another relevant dimension of the markets' objective for wireless communications. To this purpose, communication regulators have important roles in increasing the availability of spectrum and fostering its efficient use, while balancing the needs of all stakeholders with differing sectoral interests and the overall public interest (see also the report on "Developments in Spectrum Management for Communication Services" (OECD, forthcoming[11])).

The objectives related to improving the efficiency and performance of markets is at the core of regulation in virtually all OECD countries. For example, the Federal Communications Commission (FCC) in the United States includes in its competences, promoting competition, innovation and investment in broadband services and facilities, as well as encouraging the highest and best use of spectrum domestically and internationally (FCC, 2022[12]). Reducing barriers to the deployment of broadband networks was endorsed, for example, by the European Union within the framework of the Digital Agenda 2010-2020, resulting in the Broadband Cost Reduction Directive (BCRD) (European Commission, 2021[13]), which was transposed into legislation in each member state.

Users

Legal and regulatory frameworks establish and protect the rights of people and businesses, as users of communication services. Policies and regulation protecting users continue to be of utmost importance for communication regulation and an important objective of regulators. This area includes promoting equal access to high-quality broadband and strengthening consumer rights as users of broadband connectivity services.

Objectives

Promoting equal access to high-quality broadband

Promoting access for all and fostering the adoption and effective use of advanced broadband services accessible for everyone, including all locations, genders, abilities, and socioeconomic circumstances, is a generally accepted objective, to achieve territorial and socially inclusive development. In the area of connectivity regulation,[4] this objective is fundamentally addressed by universal service, but other types of regulatory measures such as the imposition of coverage obligations for granting of licences or authorisations (e.g. for the use of spectrum), or the collection and analysis of information about network infrastructures to identify gaps to design further actions, are also part of this objective.

For example, the Canadian Telecommunications Act includes the Telecommunications Policy objectives which entail, among others, to render reliable and affordable communication services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada (Government of Canada, 1993[14]).

Strengthening consumer rights as users of broadband connectivity services

Establishing and protecting the rights of consumers in a private market, is a core objective of communication regulation. The more ambitious policy objective of strengthening these rights can be achieved through regulatory measures that increase transparency to better inform consumer choice, remove information asymmetries, and empower consumers in their relations with communication service providers. In addition, consumer protection laws provide important tools for regulatory flexibility while dealing with emerging issues.

The widespread use of devices such as smartphones and tablets to access the Internet and the rising popularity of the app format has raised discussions about protecting users' freedom of choice to access and share services and content on their devices. Regulators have started to analyse the issue of 'device neutrality' in recent years (Arcep, 2018[15]; BEREC, 2021[16]) and the concept has been included in some legislative texts.

For example, the European Union's Digital Markets Act (DMA), currently under approval, states that providers of core platform services ("gatekeepers") "should not restrict the free choice of end users by technically preventing switching between or subscription to different software applications and services", in particular by the "mere offering of a given product or service by means of pre-installation" (Recital 41) (European Commission, 2020[17])[5]. Korea also included provisions in the field of 'device neutrality' in the amendment to the Telecommunications Business Act in December 2018 (Korea Communications Commission, 2018[18]). The act prohibits "unduly restricting the deletion of software that is not essential for realizing the functions of the telecommunication device or installing, operating, or suggesting software that unreasonably restricts the installation of other software" (The Telecommunications Business Act, Article 50, Paragraph 1, sub-paragraph 8) (Korea Communications Commission, 2018[18]).

Furthermore, there is a wide variety of situations and practices in the digital environment that may pose a threat to individual rights, such as the right to privacy, to reputation, or to control over the use of their personal data. Therefore, regulation to establish and protect these rights is of utmost importance to maintain in the digital environment the standards set in other areas of economic and social activity.

Some countries are further adapting their regulations to enhance and strengthen consumer protection rules. This is, for example, the case in Japan, where this was one of the objectives of the amendment of the telecommunications law (Act Partially Amending the Telecommunications Business Act (Government of Japan, 1984[19])), and where the "Basic Policy on Supervision of User Protection Regulations in the Telecommunications Business" was formulated to ensure the effectiveness of consumer protection systems (Ministry of Internal Affairs and Communications, Japan, 2021[20]).

Environmental sustainability

Communication regulation can embrace environmental goals, as both the sector itself, and in its role as an enabler of other sectors, can play a key role in achieving these goals. Therefore, environmental objectives such as the reduction of greenhouse gas emissions and of consumption of natural resources, and the protection of biodiversity should, where possible, be translated into policy objectives of communication regulation. While the objective area is very recent and only emerging across first communication regulators in the OECD area, it is likely to gain in importance for regulators of the future.

Objectives

Minimising negative environmental impact of communication network

Regulators may through different measures (e.g. licensing conditions, incentives) and according to the national legal and regulatory frameworks they operate in promote environmentally responsible practices to be adopted by operators, manufactures or other market players in the communication sector, in order to minimise negative impacts of communication networks. As a consequence, the environmental objectives of communication regulation could therefore include, among others, the reduction of energy consumption of network operations and the usage of renewable energy sources; the reduction of pollution, radiation and other hazards of networks; the adoption of environmentally responsible policies for network construction such as land use policies, cell tower construction, and data processing centres; the reduction of environmental impacts of electronic equipment and terminals once discarded e-waste[6], by adopting proper recycling and safe disposal practices; and the creation of more sustainable products, utilising a minimum of hazardous materials and allowing for longer useful lives rather than planned obsolescence (Arcep, 2022[21]).

The policy objective of reducing the environmental impact for communication regulators is gaining importance among OECD communication regulators. In France, for example, several independent administrative or public authorities, including the Electronic Communications, Postal and Print media distribution Regulatory Authority (*Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse,* Arcep), point out the need to take climate urgency into account when defining and carrying out their missions (Autorité de la concurrence, AMF, Arcep, ART, CNIL, CRE, CSA, HADOPI, 2020[22])

Security and resilience of networks

1. This area includes the objectives aimed at improving the security and resilience of communication networks, as they represent a critical infrastructure upon which the functioning of our economies and societies increasingly depends on.

Objectives

Secure communication networks and make them resilient

Digital security, when applied to communication networks, can be viewed through the triad of ensuring availability, integrity and confidentiality ("AIC" triad) of communication services. As more aspects of life move online, the potential impact and scale of digital security attacks have increased. Therefore, in order to protect this critical infrastructure, a key objective is to secure communication networks and make those networks resilient to digital security risk.

Beyond cyberattacks, there are other growing threats of disruption of communication services, in particular natural disasters – related to the climate crisis (e.g. floods, fires). There is therefore a growing need to make the network more resilient to failures (e.g. through the provision of backup power supplies, or the design of the network to place sufficient diversity and redundancy in the network topology), and to enhance coordination between governments and operators.

Some governments are already addressing these issues. For example, the Ministry of Internal Affairs and Communications of Japan has been holding the "Liaison Committee on Securing Communications Services in the Event of Disaster" since October 2018, to verify the functioning of frameworks for cooperation between Ministry of Internal Affairs and Communications and key communication operators (Ministry of Internal Affairs and Communications - Japan, 2021[23]).

Communication regulators meeting the challenges stemming from the digital transformation

Technological and market developments have led to new challenges in the communication regulators pursuit of their markets', users', environmental, and security and resilience objectives. Communication regulators have come under increased scrutiny, raising the question of whether they are adequately equipped to increase the benefit of communication services for the economy and society. Communication regulators "only" dealing with regulating the traditional communication sector may be restrained in adequately pursuing their objectives and need to collaborate with a multitude of other institutions or regulators (see Regulatory co-operation).

In addition, it is important to note that regulatory decisions and functions need to be conducted with the upmost integrity to maintain public confidence in the objectivity and impartiality of decisions and to encourage investment (OECD, 2014[24]). As the OECD Recommendation on Broadband Connectivity puts forward, robust legal and regulatory frameworks for connectivity need to be adopted and implemented in which decisions are made in an independent, impartial, objective (evidence- and knowledge-based), proportionate, and consistent manner (OECD, 2021[10]). The establishment of independent regulators can be seen as a way to protect the regulatory decision-making process from undue influence and signal a commitment to long-term goals beyond political cycles, and indeed in practice 84% of communication regulators in OECD countries are established in legislation as independent bodies (OECD, 2021[8]). Complementing this de jure independence, there are several institutional measures that regulatory agencies can take to protect from undue influence, including ensuring role clarity, transparency and accountability, financial independence, independence of leadership and ethical behaviour of staff (OECD, 2017[25]).

This section discusses selected trends on the horizon of communication regulators. It first looks at regulatory convergence and the role of the communication regulators in the digital transformation. It furthermore considers the increasing importance of ensuring privacy and safety online, rising security challenges, and an increased awareness of the importance of the environmental sustainability of communication networks.

Convergence changing the "playing field"

Technological convergence has enabled the provision of different services over the same IP network, which has led to an evolving competitive landscape. As a first step, convergence has blurred the contours of the communication and broadcasting sectors, as players now compete with bundles (OECD, 2021[2]). Services, such over-the-top (OTT) services, as well as fixed and mobile convergence on the network layer, have led to the commercial response by operators who have increased bundled offers in OECD countries and started to offer their own video services (OECD, 2019[1]).

Bundled communication services offers have become increasingly pervasive in the OECD. For instance, in 2020 in the OECD area, more than 76% of fixed broadband offers have been bundled with other communication services (OECD, 2020[26]). A significant aspect to consider is whether bundled, and especially fixed-mobile integrated offers, can be replicated by several players in the market. For example, fixed operators that are not integrated with a mobile network operators (MNOs) could potentially offer quadruple-play bundles if they enter into an agreement with a mobile operator (e.g. mobile virtual network operators (MVNOs)) (OECD, 2021[2]). Therefore, convergence between previously distinct parts of the communication industry, such as broadcasting, and fixed-mobile convergence, have been two main drivers for the increase of consolidation in OECD countries (OECD, 2021[2]).

Secondly, as stated above, there are new forms of convergence emerging that stem from the blurring of traditional communication market boundaries with broader digital services. Moreover, a main trend leading to new forms of convergence is the increasing role of non-traditional communication service providers, such as content providers and cloud service providers, in the connectivity ecosystem. (See section on The digital transformation driving an evolving communication regulatory landscape).

Given this rapidly changing external context, with the convergence between formerly distinct sectors, such as communication and broadcasting, and new forms of convergence brought about with the digital transformation that are gaining momentum, new challenges are arising. For example, a key issue for policy makers and regulators across the OECD area has been to look at the market structures that best deliver efficient and inclusive communication services, where the blurring of traditional communication market definitions may be a challenge (OECD, 2021[2]). Moreover, as operators and networks evolve in the future (OECD, 2019[1]; OECD, 2022[3]), regulators need to adapt to rapid technological changes while navigating existing institutional frameworks.

OECD countries have several ways to respond to convergence and meet the challenges that arise from it, which are not mutually exclusive. First, countries may opt to promote changes in legislation that adjust (or expand) the mandate i.e. legal powers assigned to communication regulators to enable them to respond to developments in the communication sector (i.e. converged communication and broadcasting regulators, multisector regulators), or that adapt the existing regulatory framework to a convergent environment (e.g. class licensing, spectrum management under one agency, etc.). Secondly, some countries may wish to partially expand communication regulators' responsibilities or oversight concerning new issues arising from the digital transformation (e.g. digital security, privacy, sustainability, etc.). Third, there are ongoing discussions in some countries regarding a new type of regulatory body to tackle digital issues in a holistic manner (e.g. see section on Looking ahead: Considering the need of “Tech Regulators”). Finally, countries may increase regulatory co-operation with other agencies and government bodies (see section on Regulatory co-operation).

Converged regulators: communication, broadcasting and media

Significant modifications in the mandates and responsibilities of communication regulators in OECD countries have been driven by the changing nature of communication markets, such as the increase in convergence. Some OECD countries are mirroring increasing convergence of the communication, broadcasting and content industries through a converged regulatory framework.

This is documented by the integration of responsibilities on communication and broadcasting in one regulatory body in many OECD countries (Table A.1 in the Annex). At present, 15 out of 38 OECD countries (39%) have a converged communication and broadcasting regulator. In Colombia, recognizing the convergence of communication services, changes in the sectoral law in 2019 (ICT Modernisation Law 1978 of 2019) created a converged regulator by merging the audio-visual broadcasting regulatory entity with the communications regulator, now under the responsibilities of the Communications Regulation Commission

(*Comisión de Regulación de Comunicaciones*, CRC) (MinTIC, 2019[27]). Following the new mandates, the structure of the CRC also changed by creating an arm for audio-visual content. In Hungary, the National Media and Infocommunications Authority (*Nemzeti Média- és Hírközlési Hatóság*, NMHH) is the independent, autonomous regulatory and supervisory body for the media, communication and broadcasting and postal sectors (NMHH, 2022[28]). The NMHH disposes separate teams for media and communication services within the organisation but is represented by an integrated entity.

Besides administrative and operational synergies, converged regulators may be better able to meet some important current and future concerns. For example, a converged regulator can benefit from the involvement of different experts regarding tendering broadcasting rights. In the field of digital platforms, communication market regulatory expertise might complement the media branch of the regulator. There may furthermore be efficiency gains in spectrum management and synergies with other sectors to reduce the cost of network deployment, thus promoting network extension.

In light of increased convergence of communication services over IP networks, some countries are adopting their existing regulatory frameworks to a converged environment. Countries aim to adapt the framework to allow market developments to be addressed holistically. At the same time, there is a need to simplify the regulatory framework and render it more transparent. One possibility to do so is through the introduction single-class licensing regimes for communication and broadcasting services. Simplifying licensing may considerably reduce transaction costs, facilitate market entry and speed up the administrative processes for network deployment. Instead of issuing individual licences requiring an authorisation for every type of communication service provided, single-class licencing models based on a "registry" can be a way to simplify the process (OECD, 2020[29]). A simple class-licensing regime for communication and broadcasting services can ease market entry and reduce regulatory burden. This simplifies the regulatory framework and increases transparency.

Multisector regulators

To achieve the objectives of communication regulation in a coordinated manner, it may be advantageous or even necessary to increase the level of co-operation across regulators (see Regulatory co-operation). Several countries have decided to go one step further and have integrated the communication regulator with regulators of other sectors into one single institution. Not least for historical reasons, competences for communication infrastructure and services are sometimes integrated with very different industries (often network industries) that may require different approaches to their regulation in so-called multi-sector regulators. For example, German BNetzA is in charge of regulating the communication sector, the energy sector, postal services and railway sector. While in energy and railway regulation it follows a symmetric approach, more asymmetric provisions are applied to the communication and post sector. In Finland, for example, the Law on Electronic Communications was reformed in 2018, and merged the communication and transport regulator into one entity, Traficom. In Hungary, besides its mandate for media, communication and broadcasting, and postal sectors, the NMHH furthermore has responsibilities in the areas of e-commerce, personal data breaches and online trust, and may therefore, at least partly, also be regarded as a multi-sector regulator.

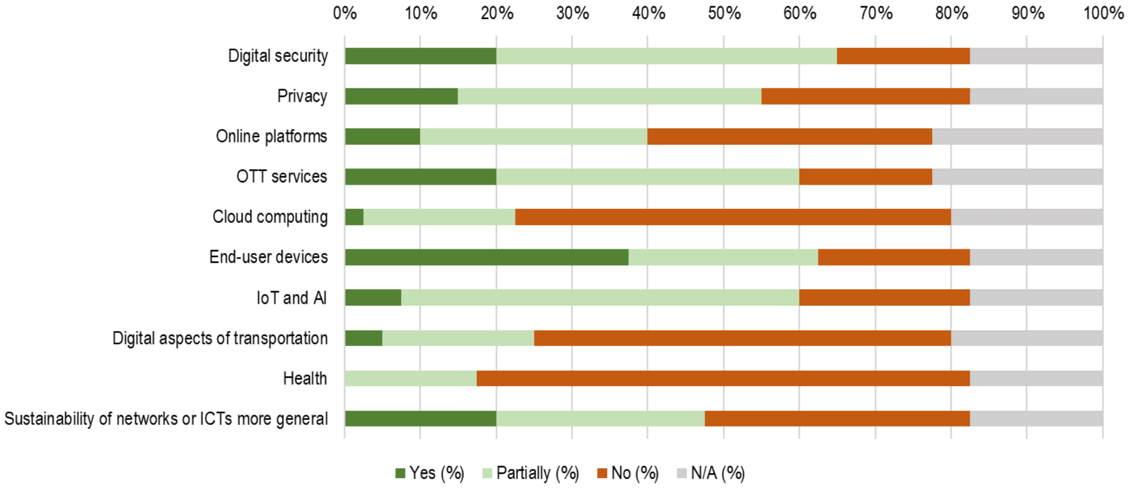
A common rationale to establish multisector regulators is to benefit from administrative synergies, economies of scale in the improvement of processes, such as their digitalisation, the transfer of best practices, and administrative synergies. The integration also allows to take advantage of a holistic oversight of different sectors and to increase the likelihood of consistent decisions. Theoretical questions and methodological approaches, such as the calculation of interest on capital, may also be determined on an overarching basis. Often, the different sectors are furthermore closely related to each other in individual objectives such as consumer protection. In addition, there may be synergies with the utilities sector (e.g. electricity and gas) or the transport sector, to facilitate the sharing of passive infrastructure (e.g. ducts, poles) or the coordination of civil works (e.g. laying networks at the same time as building or renovating a road).

As the digital transformation affects economies and societies in complex and interrelated ways (OECD, 2020[30]), synergies between the different sectors can be levied especially well when it comes to studying the effects of digitalisation. For example, the German BNetzA published several documents on the impact of digitalisation on its different branches (Bundesnetzgentur, 2022[31]). The Spanish National Markets and Competition Commission (*Comisión Nacional de los Mercados y la Competencia*, CNMC), which has competencies in communication services, media, energy, postal, transportation (rail and airports) and ex-post competition, set up a cross-sectoral "Digital Economy Working Group" in its 2021-2022 Action Plan (CNMC, 2021[32]).

An evolving mandate to face present and future challenges: New forms of "converged" regulators

Technology and market developments in the communication sector have led to new players, new services and business models, which keep constantly emerging. Consequently, the boundaries between traditional communication markets and broader digital markets and players are blurring. As a result, many countries have adapted and broadened their legal and regulatory frameworks, which led to an expansion of the sphere of influence of communication regulators. At present, there is a myriad of responsibilities that communication regulators in OECD countries, Brazil and Singapore are taking on beyond their "traditional" role (Figure 3). These include at least partial responsibilities or support (e.g. through their mandates, collaboration initiatives or lending their knowledge and experience in a whole-of-government approach) for the following issues: digital security (65%), privacy (55%), online platforms (40%), over-the-top services (OTTs) (60%), cloud computing (22.5%), end-user devices (63%), IoT and AI (60%), digital aspects of transportation (25%), health (18%), and environmental sustainability (48%).

Figure 3. Mandate of communication regulators with respect to broader digital economy issues, OECD countries, Brazil and Singapore



Note: The sample size is 40 (i.e. 38 OECD countries, Brazil, and Singapore). Countries answered the following question: "Does your national regulatory authority, with responsibility for communication/ telecommunication/broadcasting services have the mandate for the following areas: Digital security, Privacy, Platforms, OTT services, Issues related to cloud computing, Issues related to end-user devices, Issues in the area of the IoT and AI, Issues related to the digital aspects of transportation, Issues related to health, Issues related to the sustainability of networks or ICTs more general?"
Source: OECD elaboration based on questionnaire responses.

The detailed description of the responsibilities by country are depicted in Table A.2 in the Annex. The subsequent sections will explore how communication regulators increasingly take on responsibilities in the realm of OTTs, consumer and privacy protection, digital security and resilience, as well as the environmental sustainability of communication networks.

Regulatory approaches to over-the-top services (OTTs)

Converged networks furthermore led to the emergence of new players in the market, such as terminal equipment and online service providers which have also entered another area of traditional operator markets. Specifically, they offer *over-the-top services* (OTTs), i.e. content that is provided over the Internet and not over managed facilities (OECD, 2014[33]). OTTs play an increasing role in today's economies and societies with many examples ranging from voice/messaging services (Line, WhatsApp, WeChat, FB Messenger, Discord, Telegram, Signal, Kakao Talk, Skype, Viber) to video services (Netflix, Viu ("VIEW"), Disney+, Stan, Neon, TVNZ OnDemand, Amazon Prime Video). Operators are at times distributing popular OTTs (e.g., Disney+, Amazon Prime, Netflix), either included as part of its bundle or as part of a promotion (see also (OECD, 2019[34])). Furthermore, non-traditional players are more and more offering audio-visual content, especially through on-demand streaming platforms. For example, traditional players are offering audio-visual content, both in linear ways, i.e. web streaming, but also increasingly through on-demand Internet platforms ("catch-up TV").

The OTT landscape is dynamic and evolving, which is prompting continued regulatory discussions both in the OECD and abroad. Communication regulators are constantly reviewing how to foster innovation while at the same time upholding their regulatory aims, which may include the establishment of a balanced and consistent framework, furthering investment in domestic content production, and promoting healthy competition. On the one hand, OTT services are innovative and provide new services for customers, which may also drive demand for broadband adoption.

OTT services may apply competitive pressure on traditional players, encouraging them to innovate and expand offerings. However, on the other hand, some industry stakeholders argue that regulatory burdens on OTTs may be unequal to those placed on traditional players (e.g., may not be subject to the same requirements to begin service, may not be held to same regulatory requirements, such as for local content or must-carry/must-offer.) In Australia, for example, the Australian Communications and Media Authority (ACMA) has been involved in administering a code designed to help support the sustainability of the Australian news media sector by addressing bargaining power between digital platforms and Australian news businesses (ACCC, 2021[35]).

OTTs furthermore affect the clarity of regulators' roles given a potential duality among their functions. More than half of regulators (60%) in the OECD, Brazil and Singapore have or partially have a mandate for OTTs (see Table A.2 in the Annex).

Many European Union countries have, or are about to get competences in the communication sector over OTT players that qualify as so-called "number-independent interpersonal communication services" (NIICS)[7] stemming from the transposition of the European Electronic Communications Code (e.g. Austria, Hungary, France, Lithuania) (European Commission, 2018[36]). The European Electronic Communications Code (EECC) defines "interpersonal communication services" broadly to include "all types of emails, messaging services, or group chats." The Code further defines two types of interpersonal communication services: i) number-based Interpersonal Communication Services, which enables communication with a number or numbers in national or international numbering plans and ii) number-independent Interpersonal Communication Services, which does not enable communication with a number or numbers in national or international numbering plans. The free OTT Voice over IP (VoIP) applications, provided over the public Internet, would classify in general as Number-independent ICS. VoIP allows users to make a voice call over the Internet.

As a consequence, national laws are obliged to adopt this classification and services that fall under said category are subject to all laws that address communication services.[8] In France, for example, order 2021-650 extends Arcep's regulation to NIICS, which now fall within the definition of electronic communications services. This in turn expands the category of "operators" subject to Arcep's control. Some countries also have oversight over OTTs with audio-visual content. In Austria, the Communication Platform Act (*Kommunikationsplattformen-Gesetz*, KoPLG), in place since 1 January 2021, states that KommAustria, as the media regulatory authority, is the contact point in the area of supervision of video-sharing platforms and communication platforms. It aims to promote the responsible and transparent handling of reports by users about content on communication platforms and the immediate treatment of such reports (RTR, 2021[37]). In Germany, the new Telecommunications Act (*Telekommunikationsgesetz*, TKG), in force since 1 December 2021, also contains powers to regulate NIICS. Other countries are currently in the process of drafting legislation for OTTs. In Israel, a draft legislation is pending that applies content regulatory structure to OTT content providers. In Mexico, the Federal Economic Competition Law (*Ley Federal de Competencia Económica*, LFCE, 2014, article 5) establishes a procedure for specialised courts to resolve cases in which the powers of both competition authorities, the Federal Institute of Telecommunications (*Instituto Federal de Telecomunicaciones*, IFT) for the communication and broadcasting sectors, and the Federal Economic Competition Commission (*Comisión Federal de Competencia Económica*, COFECE) for all other sectors, may overlap due to the convergence between traditional and digital services (Congress of Mexico, 2014[38]). These specialised courts have determined that the IFT is competent to resolve matters related to OTT audio-visual content services (IFT, 2021[39]).

Some communication regulators are monitoring market evolution and some are considering whether OTT services are substitutes for traditional communication offers. Other countries are considering the mandate of the regulator and which agency should look at these issues (again linking back to the challenges arising with convergence). This is an evolving space and regulators in the OECD (and beyond) continue to consider the best ways to structure their policy responses. The synergies of a comprehensive approach to regulation across different sectors may be needed to achieve a consistent regulatory action towards convergence and OTTs. Furthermore, to monitor the impact of OTT's on national markets, information about the activities of OTT players is needed. However, this information is often not available to regulators.

While discussions are held in almost all countries, not all countries adapt equally to the challenges stemming from OTTs. Often, this has to do with the myriad of different bodies involved in the oversight of OTTs. For example in Brazil, the regulatory body for communications, audio-visual content, protection of personnel data and broadcasting are all separate bodies, respectively, the National Telecommunications Agency (*Agência Nacional de Telecomunicações*, Anatel), the National Cinema Agency (*Agência Nacional do Cinema*, Ancine), the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados*, ANPD), and the Ministry of Communications (*Ministério das Comunicações*, MCom). Furthermore, the complexity of the topic slows down the process of integrating OTTs in the regulatory framework. In Canada, legislation was introduced in February 2022 to update Canada's broadcasting law and require online streaming services to contribute to the creation and availability of Canadian stories and music in an equitable way. If passed into law, the legislation would ensure that online streaming services showcase Canadian music and stories, support Canadian creators and producers, and make programmes created in both official languages (English and French) more accessible to Canadians, among other policy objectives. The new bill reflects largely what was approved by the House of Commons in June 2021, but not ultimately passed into law before the dissolution of Parliament a couple of months later (Government of Canada, 2022[40]). Further, in April 2022, another bill was introduced that would ensure fair revenue sharing between digital platforms and news outlets by promoting voluntary commercial agreements between these two groups. In the 2022 federal budget, CAD 8.5 million (USD 6.8 Million[9]) was announced for this initiative to be provided to the Canadian Radio-television and Telecommunications Commission (CRTC) (Government of Canada, 2022[41]).

In light of evolving market dynamics, policy makers need to ensure a fair, competitive landscape for all players – both traditional communication service and OTT providers, while encouraging societal goals (e.g., choice of innovative and high-quality services, domestic content production and transmission). There is no one-size-fits all approach to OTTs and at only “common practices” but no “best practices” have emerged. OTTs are a constantly evolving space and regulators in the OECD (and beyond) need to consider the best ways to structure their policy responses. However, to monitor the impact of OTTs on national markets, a thorough assessment of the activities of OTT players is needed. Monitoring of these evolving trends can help regulators tailor policies to domestic situations.

Just as OTTs, digital platforms have become an essential feature of our daily lives and the world economy. However, as these platforms grow and gain in power across many sectors, their practices raise new questions regarding to specific regulatory issues. Many countries have started to tackle challenges related to digital platforms, e.g. with the DMA (European Commission, 2020[17]) and the DSA (European Commission, 2020[42]) in the EU. The involvement of communication regulators in the regulation of digital platforms ranges from the simple participation in the discussions around the topic to the full competence in regulating it. Currently 40% of communication regulator in the OECD, Brazil and Singapore report to either partially or fully be responsible for online platforms in their country (Table A.2 in the Annex). As digital platforms touch upon number of topics pertaining to the realm of different regulatory authorities, and due to the multi-national character of platforms, many communication regulators are co-operating with other regulators or governmental bodies. This is even more so in countries where there is no clear designation of competent authority. In addition, as the influence of digital platforms increases and they move more and more into the focus of policy makers, it is very likely that the co-operation between different stakeholders increases as well. While an in-depth analysis of digital platforms goes beyond the scope of this report, other recent OECD reports have addressed the issue (OECD, 2019[43]; OECD, 2021[44]).

Looking ahead: Considering the need of “Tech Regulators”

Taking the thought of convergence one step further, the emergence of innovative digital services and technologies have led to discussions concerning so-called “tech regulators”. Some OECD countries have started to think about how such an entity might be shaped to strive for a holistic regulatory approach towards digital products and services.

In the United Kingdom, for example, there has been some policy debate around the establishment of a new Digital Authority. This debate has taken place most recently by the House of Lords Communications and Digital Committee through an inquiry into the work of digital regulators (House of Lords, select committee on communications, 2019[45]). The communication regulator in the United Kingdom, Ofcom, and the other members of the Digital Regulation Cooperation Forum (DRCF), have argued that the DRCF can deliver regulatory coordination without the need for introducing an additional authority (DCRF, 2021[46]). A new overarching regulatory body would still require coordination with pre-existing regulators – e.g. in communications, media, competition, data privacy – which would need to persist given their ongoing wider (non-digital) responsibilities. This would create additional coordination interfaces and the potential need for duplication of already scarce regulatory resource, and also reduce clarity for industry and consumers on respective roles and responsibilities – particularly as digital matters are not necessarily neatly divisible from wider regulatory responsibilities. Initiatives such as the DRCF, on the other hand, based on the cooperation and coordination between existing regulators whose regimes are engaged by “digital”, enables the leveraging and sharing of existing expertise.

In Canada, the federal Broadcasting and Telecommunications Legislative Review Panel released a report that recommended expanding the CRTC into a broader communications regulator better equipped to manage new technologies (Government of Canada, 2020[47]). It also made proposals with respect to the Canada’s Copyright board and Competition Bureau. In July 2021, the federal government, prior to the announcement of the 2021 federal election, initiated a consultation on the possible creation of a new regulator to address online harms on social media services. This proposed Digital Safety Commission would oversee and enforce new rules and provide independent recourse for complaints. In March 2022, an expert advisory group was created to provide advice on a legislative and regulatory framework that best addresses harmful content online and how to best incorporate the feedback received during the national consultation held from July to September 2021 (Government of Canada, 2022[48]).

As well as addressing the challenges posed by digital regulation, communication regulators will need to ensure there is coherence in regulatory approaches. Furthermore, the global nature of online players means international regulatory co-operation is critical to promoting the development of coherent regulatory approaches around the world (see Regulatory co-operation). A coherent and clear approach towards the regulation of digital services may be beneficial in terms of providing innovative businesses with regulatory certainty and ensuring a favourable business environment with moderate regulatory burdens. These could result in a more effective delivery of services to the users and communication regulators could be a facilitator of the development of broadband connectivity and an enabling environment for the fruitful development of services and products in the digital space.

The increasing importance of ensuring privacy and safety online

With the aim of pursuing the benefit of users, communication regulators often take on an essential role in consumer protection as well as with respect to privacy protection, for which slightly more than half of communication regulators (55%) in OECD countries, Singapore and Brazil, have at least partial responsibilities (see Table A.2 in the Annex). Often, communication regulators may have partial responsibilities to ensure privacy online from the viewpoint of ensuring fundamental rights and values, as the communication between two individuals is considered their intimate private space, the violation of which would constitute a violation of fundamental rights and values.

Although privacy enforcement authorities (PEAs) are generally in charge of privacy issues under most privacy protection laws (OECD, 2013[49]), regarding privacy issues in the communication sector, PEAs and communication regulators sometimes have cross-regulatory interactions (OECD, forthcoming[50]), and the division of roles between the communication regulator and respective privacy enforcement authorities are often clarified by communication sectoral laws. For example, the Federal Office of Communications (OFCOM) in Switzerland has a responsibility for the confidentiality of communication services, the protection of personal data, and the protection of children and adolescents in communications services, based on the Telecommunications Act (Swiss Federal Council, 1997[51]). In Japan, the Act on the Protection of Personal Information, which applies to all industrial sectors including the communication sector, is under purview of the Personal Information Protection Commission. In addition, the Ministry of Internal Affairs and Communications (MIC) is in charge of securing secrecy of communication services based on the Telecommunications Business Act (Government of Japan, 1984[19]).The Personal Information Protection Commission (PPC) and MIC jointly have *Guidelines for the Protection of Personal Information in Telecommunications Business* (Ministry of Internal Affairs and Communications, Personal Information Protection Commission, 2022[52]).

Crosscutting regulation related to privacy and data protection may apply, where the role of sectoral regulators and data protection authorities is clarified. For example, based on the ePrivacy Directive (EUR-Lex, 2002[53]), some countries in the European Union have enacted domestic laws whereby communication regulators are responsible for monitoring and enforcing privacy regulations in the sector. For example, in Germany, the Act to Regulate Data Protection and Privacy in Telecommunications and Telemedia (*Telekommunikation-Telemedien-Datenschutzgesetz*, TTDSG) was issued (Bundesministerium der Justiz, 2021[54]). The Act inherits some data protection regulations of the old Telecommunications Act (*Telekommunikationsgesetz*, TKG), and stipulates the authorities of the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, BfDI) and German regulator BNetzA is set respectively (Bundesnetzagentur, 2022[55]).

BNetzA has responsibilities on enforcement about data protection and privacy protection in communication services, including platform services, such as the confidentiality obligation of communication, and handling of traffic data and location data.

Often, communication regulators are working to protect privacy in the communication field by co-operating with privacy enforcement authorities (see Regulatory co-operation). Some communication regulators hold formal or informal meetings with privacy enforcement authorities, while others have particular cooperation frameworks, for example through a Memorandum of Understanding (MoU). For example, in Canada, the CRTC entered into a MoU with the Competition Bureau of Canada and the Office of the Privacy Commissioner of Canada (OPCC) in 2013 regarding the Canada's Anti-Spam Legislation (CASL). All three agencies have quarterly meetings for the purposes of coordinating their respective agendas (OPCC, 2014[56]).

With the prevalence of over-the-top players (OTTs) and online platforms, new issues are emerging regarding consumer protection. OTTs and platforms often generate, store, deliver, or utilise user information for various purposes, including to improve the user experience or to profit financially from this information (OECD, 2020[30]). In particular, discussions are being held in some OECD countries on how to handle different consumer information, such as location information of communication terminals, information about user behaviour, and information that identifies user terminals, considering that this data is sometimes utilised or provided to third parties without the users' knowledge or consent.

A key challenge for policymakers is timely and prompt responses given rapid technological progress. In particular, some countries may be considering appropriate regulations and enforcement regarding the handling of user information, including personal data, not only in traditional communication services, but also for services delivered over online platforms. As privacy issues may concern different agencies, such as privacy enforcement authorities and competition authorities, the regulatory framework should have an efficient and appropriate division of roles. In addition, especially with large-scale OTTs and platforms, personal data may also be handled overseas. Therefore, it is desirable to take into account the viewpoint of interoperability of privacy and data protection frameworks in communication regulation (OECD, 2021[57]).

Countries are tackling consumer issues arising from online platforms and OTTs in different ways. In the European Union, a proposal for ePrivacy regulation has been put forward by the European Commission that intends to replace the current ePrivacy Directive, and in particular, complement privacy protection in the communication field as *lex specialis* (i.e. a law governing a specific subject matter) to the General Data Protection Regulation (GDPR) (European Commission, 2017[58]). The draft proposal of the ePrivacy rules aims at ensuring the same level of confidentiality of communication service for all "electronic communications", including OTTs (e.g. WhatsApp, Facebook Messenger and Skype) as well as "traditional" communication operators. The aim of the regulation is to guarantee privacy protection in respect to communication content and metadata, i.e. data that describes other data, such as author, date created and location, and to introduce simpler rules on cookies.[10] The regulation will be applied directly to European Union Member States, and proposes that the PEA responsible for enforcement of the GDPR to be responsible for the ePrivacy Regulation. In addition, communication regulators will cooperate, if necessary. In Japan, MIC has been discussing issues regarding the proper handling of user information in an online environment. Following the discussion, changes to the Telecommunications Business Act have been suggested. These include rules for communication operators regarding the appointment of user information protection managers, the publication of policies relating to handling user information, the need for regular assessment, and ensuring opportunities for confirmation by users when sending user information to third parties (Ministry of Internal Affairs and Communications, 2022[59]).

Furthermore, online safety, or protection against online harms, is also a significant consumer protection issue affecting communication users and can be closely linked to privacy protection. While services delivered over online platforms have made it easier for people to communicate and express their opinions, the distribution and amplification of various illegal or harmful content, such as privacy infringing content, online harassment, child sexual abuse and exploitation material (OECD, 2020[60]), terrorist and violent extremist content (OECD, 2020[61]), or the spread of untruths online, has become a serious societal issue.

Regarding measures against illegal or harmful content online, a challenge policymakers face is striking the right balance between protecting the safety of users (e.g. through content moderation practices) while ensuring fundamental human rights, including freedom of expression. In this sense, as both the services delivered over online platforms and the nature of the threats continue to evolve, promoting transparency on content moderation practices and how user information is handled is critical. To date, countries have usually enforced laws that stipulate exemptions for online service providers concerning their liability for the content delivered over online platforms. However, more and more draft regulations that demand proactive responses and transparency from online platforms are emerging in the OECD area.

Given the impact of large-scale online platforms on users and society, some jurisdictions are considering balanced regulations. For example, in the European Union, the DSA is being considered by the European Parliament to protect users from illegal content (European Commission, 2020[62]). The DSA proposes a set of measures against illegal content, such as the publication of terms of use and the establishment of a complaint reception system. It also calls for transparency regarding these proposed measures. The obligations would be tailored corresponding to the type or scale of digital services delivered. For example, additional obligations for large-scale online platforms are suggested, such as implementing measures based on risk assessment and ensuring transparency about recommender systems and online advertisement. Regarding the application and enforcement of the DSA, European Union Member States would have to designate one or more competent authorities.

While the online harms regime is currently beyond the remit of many communication regulators in OECD countries, there are some exceptions whereby the regulator or ministry in charge of the communication sector is taking up this responsibility. For example, in Japan the MIC is discussing appropriate measures against illegal or harmful information, such as online harassment and disinformation, and it monitors online platforms' efforts (Ministry of Internal Affairs and Communications, 2021[63]). The MIC is conducting a hearing from major online platforms and requests that those platforms appropriately respond to illegal or harmful information and report on ensuring the transparency of their measures. In the United Kingdom, the UK Government introduced new legislation in 2020 granting Ofcom power to regulate video sharing platforms that are based in the United Kingdom, and also appointed Ofcom as the regulator of the online harms regime (Ofcom, 2021[64]). In Australia, the ACMA has overseen the development of a voluntary industry code of “good practice” to reduce the risk of online misinformation (DIGI, 2021[65]).[11]

Environmental sustainability considerations

Environmental considerations have climbed up the priorities of policy agendas across the world, with many countries viewing climate change as one of the main policy and regulatory challenges to tackle in the upcoming decades. Communication services and infrastructures have an impact on the climate both negatively (e.g. the high-energy consumption of data centres) and positively (e.g. through support for other parts of the economy). Apart from their direct impact on the environment, they have an indirect or catalyst effect on other sectors.

Recent economic recovery packages have also placed emphasis on structural reforms to reduce carbon emissions by acknowledging that digital and “green” policies are intertwined, and together may help achieve this objective. For example, the Korean government launched the “New Deal” in July 2020, which places digital policies, together with sustainability, as the two key pillars of their “National Strategy for a Great Transformation”, where broadband connectivity plays a key role (Ministry of Economy and Finance of Korea, 2020[66]). While policy initiatives and some industry efforts are pointing to an increased awareness for environmental issues (see (OECD, 2022[3])), many communication regulators in OECD countries have also been active in supporting the decarbonisation of the sector, be it through their mandates, collaboration initiatives or support through knowledge and experience.

The OECD Recommendation on Broadband Connectivity highlights that for the future, the environmental sustainability of communication networks is of paramount importance (OECD, 2021[10]). In line with the OECD Recommendation on Broadband Connectivity, sustainability considerations play an increasing role in work plans and strategy statements of communication regulators. In its Electronic Communications Strategy Statement for 2021 to 2023, Irish regulator ComReg notes that increasing awareness and attention is being placed on the relationship between the communication sector and climate change (ComReg, 2021[67]). In its 2021-2022 action plan, sustainability is one of the objectives of the Spanish CNMC (CNMC, 2021[32]).

As trusted entities that possess the relevant experience and knowledge, many communication regulators have contributed to assessments of the impact of communication networks on the environment. The Irish communication regulator, ComReg, found that while the sector is enabling decarbonisation across the economy, from remote working to smart metres, greater use of communication services and devices could potentially increase waste and emissions (ComReg, 2021[68]). In France, among others, the Government commissioned Arcep and the agency for ecological transition (*Agence de la transition écologique*, ADEME) to carry out a study to qualify the current and future environmental footprint of digital technology. Arcep furthermore assessed the fixed and the mobile market. It found that one reason to further fibre deployment are sustainability considerations. Arcep cited that fixed fibre networks consumed on average 0.5 Watts (W) per line, which translates into three times less energy than an ADSL line (1.8 W) and four times less than a traditional PSTN line (2.1 W) (Arcep, 2019[69]). In another study, Arcep found that the energy efficiency gains achieved from 5G deployment will begin in 2023 and be clear by 2028 in the most densely populated areas but will be far more modest in more sparsely populated areas (Arcep, 2022[70]).[12]

At present, some communication regulators in OECD countries may have an explicit mandate related to the environment, while others are coordinating the efforts of the environmental sustainability of networks as part of a whole-of-government approach. While roughly half of communication regulators (47.5%) in the OECD, Brazil, and Singapore report to have at least a partial responsibility for issues related to the sustainability of networks or ICTs more general, only one fifth (20%) report to have an explicit mandate in this area (see Table A.2 in the Annex). For example, in Hungary, the general objectives of the 2003 Act C on Electronic Communications include the enforcement of environmental protection requirements concerning communication networks and services. Among others, the Act stipulates that NMHH may order provisional protective measures for the protection of the environment (Section 37), and that radio equipment shall be installed in accordance with environmental and nature protection regulations (Section 80). In Costa Rica, Law No. 7 593 establishes the obligation for the Superintendency of Telecommunications (*Superintendencia de Telecomunicaciones*, SUTEL) to ensure environmental sustainability in relation to the deployment of communication networks. In New Zealand, the Resource Management Regulations (National Environmental Standards for Telecommunication Facilities) from 2016 are standards that provide national consistency in the rules surrounding the deployment of communication infrastructure across New Zealand, while ensuring the effects on the environment are minimised and managed appropriately. In France, the *Circular Economy Act* requires Internet service providers to inform their subscribers about their consumption and associated greenhouse gas emissions. Arcep is currently working on the implementation of this provision alongside the French Environment and Energy Management Agency (ADEME).

In some countries, communication regulators are contributing to a green transition by general national targets guiding also the national regulatory work. In Ireland, the Climate Action and Low Carbon Development (Amendment) Act, enacted on 2 February 2021, establishes a legally binding framework with clear targets and commitments, whereby public bodies will be obliged to perform their functions in a manner consistent with national climate plans and strategies, and furthering the achievement of the national climate objective.[13] Consequently, this framework requires that the Irish communication regulator, ComReg, to perform its functions in a way that is consistent with approved national climate plans, strategies, and objectives (Government of Ireland, 2021[71]).

Many regulators that at present do not have direct mandates on environmental sustainability issues, may still share the opinion that the impacts of the communication sector are increasingly relevant. This has led to own initiatives by communication regulators, such as in Belgium, Spain, and the United Kingdom. In Belgium, sustainability competencies are not within the remit of the authority on the national level, as environmental protection is a regional competence in which the federal Institute for Postal services and Telecommunications (BIPT) cannot interfere directly. Nevertheless, in BIPT's strategic plan 2020-22, the regulator has engaged itself to support any innovative initiatives which stimulate the sustainability of communications networks such as the sharing of network elements between operators (BIPT, 2019[72]).

In the United Kingdom, the United Kingdom Regulators Network (UKRN, an association of 14 regulators from the utility, financial and transport sectors) has launched a work stream to understand how regulation can support and promote energy efficiency and carries out this work in collaboration with industry (UKRN, 2022[73]). Alongside Ofcom, this network consists of members from the United Kingdom's energy and utility sector (Ofgem, Ofwat, the Utility Regulator), as well as data protection (the Information Commissioner's Office), financial services (Financial Conduct Authority, Payment Systems Regulator, the Pensions Regulator, the Financial Reporting Council), transport (Office of Rail and Road, Civil Aviation Authority) and housing sectors (the Regulator of Social Housing). The United Kingdom's Regulatory Network strategic priorities for 2021-22 include evolving regulation to promote sustainable economic recovery and growth and enabling climate change mitigation and adapting responses that are consumer conscious (UKRN, 2021[74]).

The above shows that communication regulators throughout the OECD are actively engaging in the work on a greener future, such as through direct responsibilities, working groups or channelling their knowledge and experience in analyses. While communication regulators may infer environmental responsibilities from more general objectives and can thus for example engage in measurement initiatives or awareness raising, the lack of legal mandates for the communication regulator to be able to intervene with regard the environmental sustainability of the sector can often be identified as a constraint to take further actions beyond the knowledge building and collection of information. Efficiency (including cost savings) and innovations are two directions for the development of sustainable, modern software-driven, automated, and intelligent networks, which will help to overcome current challenges operators face. Fostering competition encourages operators to invest and operate more efficiently. Considering the role of the regulator, spectrum assignment plays a crucial role for the development of the competition. Incentives for more efficient technologies deployed by operators, as well as infrastructure sharing measures, can be regarded as possible regulations to achieve the goals (see section on Infrastructure sharing and co-investment).

Closely linked to sustainability considerations is the increasing awareness of the importance of network resilience. The resilience of a communication networks refers to the ability of a network to cope with shocks and still maintain an acceptable level of service, despite the presence of such challenges. The United States, for example, categorises the communication sector as a critical infrastructure, since it is an integral component of the economy, underlying the operations of all businesses, public safety organisations, and government (CISA, 2022[75]). The COVID-19 health emergency has further accentuated awareness of how resilient and high-quality broadband networks are becoming even more critical. Looking ahead, and considering the effects of the pandemic, the number of natural disasters, energy outages, and national security threats, measures to increase the resilience of networks will increasingly become important.

Resilience can be strengthened by ensuring network diversity and redundancy when planning and rolling out infrastructure. Some countries have started to invest in making networks more resilient. Australia, for example, set up an AUS 37.1 million (USD 25.52 million)[14] programme called "Strengthening

Telecommunications Against Natural Disasters" (STAND) to render networks more resilient in response to natural disasters (OECD, 2022[3]).

Going forward, communication regulators may play an increasing role in raising the resilience of networks. A recent event that exemplifies this need have been the catastrophic floods in western Germany in 2021. As a consequence of the floods, the revised German Telecommunications Act (December 2021) allows German regulator *Bundesnetzagentur* to consider environmental protection as one of the reasons for an imposition of shared use of infrastructures.

From a network resilience perspective, regulation may also establish measures to promote network diversity and redundancy as well as mechanisms to monitor the reliability of networks (e.g., monitoring network outages) and the effectiveness of regulation. Regulators may also aim to ensure the coordination of network operators with the other actors involved in emergency or crisis managements, including the relevant public authorities and other infrastructures operators (e.g. financial/banking, transport, and Public Protection and Disaster Relief (PPDR) services).

Rising digital security challenges

Given the crucial role communication networks play in our economies and societies, their security and resilience have become a priority for policy makers across the OECD. However, both cyberattacks on communication networks and the communication networks themselves are evolving. An overarching trend is the increasing criticality of and reliance on communication networks by the economy and society, which is changing the context of the security of communication networks. Communication networks are also evolving to take advantage of technological trends, such as increasing network virtualisation and greater use of cloud services, the shift towards more openness, including open RAN, and the use of artificial intelligence (OECD, forthcoming[76]).

These trends are shaping communication networks and bringing significant challenges to digital security risk management in communication infrastructure. First, the attack surface is expanding, with more points within the system that may be vulnerable to a cyberattack (OECD, forthcoming[76]). This expansion results from communication networks becoming more interconnected, their architecture growing more complex and their systems becoming more software-defined, cloud-based and virtualised. In particular, the shift towards virtualised, software-defined and cloud-based networks means that there are more software components in the network, increasing the risk of software vulnerabilities that could be exploited (OECD, forthcoming[76]). The number of devices connecting to these networks, which are expected to continue to grow (e.g. IoT devices), also introduces additional points of vulnerability. Second, as operators evolve, their supply chain is becoming broader and more complex (OECD, forthcoming[76]). This redistributes control and responsibility for digital security risk management along the value chain, also making it difficult to attribute responsibility in case of digital security incidents. Simultaneously, the threat landscape is changing, with attacks becoming commoditised (e.g., "ransomware-as-a-service") and malicious attacks growing increasingly sophisticated and well-funded (OECD, forthcoming[76]). In addition, as communication networks are increasingly critical, they are becoming a more interesting target for malicious attacks.[15]

Against this backdrop, regulators face several challenges regarding the digital security of communication networks. Perhaps the most important and basic question facing them is one of regulatory remit. Digital security is a crosscutting issue that, thanks in part to the digital transformation of society, affects several sectors that depend on communication networks for their proper functioning. This not only raises the stakes when it comes to the potential impact that a cyberattack could have, but also blurs the lines between the responsible regulatory body best placed to regulate digital security. There are also some digital security risks that are common across critical sectors, which may call for a harmonised national approach. In addition, digital security expertise is in many countries lacking, making it hard to find digital security experts with the necessary skills to evaluate risk and provide operational assistance.

Policy makers are facing these challenges in several ways. As digital security is a cross-sectoral issue, OECD countries have broadly taken the following approaches: *i*) one agency or body has responsibility for digital security across sectors (centralised model); *ii*) the sectorial regulator has the responsibility for digital security of the sector under its remit (decentralised model); or *iii*) a hybrid approach combining elements of the two. For instance, a hybrid approach may give the communications regulator certain responsibilities, and others to another governmental agency (e.g., a Ministry or national digital security authority). Nevertheless, all these approaches may overlap, especially with regard to inter-agency collaboration. For instance, in case of a centralised approach, the cross-sector digital security agency may collaborate with the sector-specific regulator. The regulator could provide sector-specific knowledge that would assist the broader digital security agency in understanding the unique risks that could apply to the sector and therefore better tailor policy interventions, if needed. Similarly, in a decentralised approach, a centralised agency can offer digital security support and expertise to sector-specific regulators and provide situational awareness across sectors (Bernat, 2021[77]). Additionally, there may be a split in responsibility for which agency is responsible for defining digital security policy and strategy, monitoring and enforcing compliance, and providing operational expertise to relevant companies.

Of communication regulators in the OECD, Singapore, and Brazil, 45% reported that the national regulatory authority responsible for communication services has a partial mandate related to digital security. 20% noted that the communications regulator does have a mandate for digital security, while 18% reported that the communications regulator does not have a mandate for digital security (see Figure 3 and Table A.2 in Annex). Those that reported the communication regulator had no mandate for digital security include Colombia, France, Greece, Ireland, Latvia, Portugal and Spain. In France, for example, digital security is centralised at the National Agency for the security of information systems (*Agence nationale de la sécurité des systèmes d'information*, ANSSI).

At the opposite end of the spectrum, communication regulators in Finland, Iceland, Japan, Korea, Poland, Slovak Republic, the Republic of Türkiye (hereafter "Türkiye"), and the United Kingdom reported to have a mandate covering digital security. Perhaps among the most recent of these is in the United Kingdom, which recently passed the Telecommunications (Security) Act 2021[16] giving communications regulator, Ofcom, the responsibility to monitor and enforce compliance with the newly established requirements outlined in the Act (UK Parliament, 2021[78]). The Act amends and expands Ofcom's mandate and current powers on digital security. However, while Ofcom has a mandate to monitor and enforce these requirements, it still coordinates with other relevant agencies, which may be in charge of establishing and defining policies on digital security. For example, Ofcom, the Department for Digital, Culture, Media & Sport (DCMS) and the National Cyber Security Centre are working together to develop new regulations and code of practice for the communication sector and recently consulted on their proposals (DCMS, 2022[79]).

Nevertheless, the fact that 45% of communication regulators reported to have partial responsibilities related to digital security suggests that many countries appreciate the benefits of a hybrid approach, which may combine elements of the two approaches (centralised versus sector-specific). Countries may follow such a hybrid approach to leverage the expertise of a specialised agency on digital security as well as the sector-specific knowledge and existing relationships with communication network operators from the communication regulator. In Germany, the Bundesnetzagentur, has a partial mandate on digital security for the communications sector, including on reporting obligations in case of personal data breaches and electronic trust services (Bundesnetzagentur, 2022[80]; Bundesnetzagentur, 2022[81]). Bundesnetzagentur also co-operates and works jointly with other agencies on the topic of digital security; for example, BNetzA worked with the national cyber security authority (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) and the Federal Commissioner for Data Protection and Freedom of Information to establish security requirements for telecommunications and data processing systems (Bundesnetzagentur, 2022[82]). The three agencies similarly worked jointly to define a list of critical functions for communication networks that have increased risk, which aim to help define critical components in the network that should particularly be protected and that may be subject to additional requirements (e.g., certification) (Bundesnetzagentur, 2022[82]).

Another benefit of the hybrid approach is to ensure digital security is coordinated nationwide, for example, with the help of a national coordinating body. In Singapore, the communications regulator, Info-communications Media Development Agency (IMDA) has the lead for the communications and broadcasting sectors; they have established a "cybersecurity code of practice", which imposes certain security requirements on major ISPs in the country (IMDA, 2021[83]). At the national level, Singapore's cybersecurity efforts nationwide are coordinated by the Cyber Security Agency of Singapore, which is a part of the Prime Minister's Office and managed by the Ministry of Communications and Information (CSA) (CSA, 2022[84]).

The approaches to digital security taken at the structural level can also be seen in the nature of the approach taken to policy as well. That is, policies taken to increase the level of digital security could be overarching or sectorial. As operators are increasingly considered to be operators of critical infrastructure, they can fall within the scope of public policies to protect critical infrastructure and critical activities, across several sectors. Or, more sector-specific legislation can be applied. The European Union, for example, is considering bringing communication networks under an overarching policy framework encompassing critical activities, moving away from sectoral-specific legal provisions related to digital security.[17] This would bring all operators of critical activities under the same digital security framework, and may result in some shifts in how EU Member States handle the digital security of communication network operators. Indeed, the Irish communications regulator, ComReg, notes that its role may evolve given the NIS2 discussions and others at the European level in its Electronic Communications Strategy Statement 2021-2023 (ComReg, 2021[68]).

A similar move to include the communication sector under legislation related to critical infrastructure took place in Australia with the passage of the Security Legislation Amendment (Critical Infrastructure) Act in December 2021 (Parliament of Australia, 2021[85]), as part of the Government's broader Cyber Security Strategy (Australian Government. Department of Home Affairs, 2021[86]). The legislation has been implemented in two tranches – the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 implements the second tranche of the Government's enhanced critical infrastructure security framework, building on the amendments introduced by the Security Legislation Amendment (Critical Infrastructure) Act 2021 (the SLACI Act) (Australian Government. Department of Home Affairs, 2022[87])

Many regulators acknowledge both the importance of digital security for the communication sector and recognise the challenges to keep regulation at pace with technological advancements. Additionally, as the digital security of communication networks becomes increasingly important, regulators are actively considering their policy approach to encourage digital security, with some recently amending their regulation (e.g. Australia, United Kingdom, and the European Union). As shown in the above examples, there is a variety of different approaches to regulating digital security in communication networks. However, a key component across the approaches (centralised, decentralised, hybrid) is cross-agency collaboration to leverage the expertise of relevant bodies to create fit-for-purpose policies. Additionally, establishing clear mandates and avoiding regulatory overlaps is another important aspect of a country's digital security framework that will provide clarity for private stakeholders and allow regulators to put in place an enabling environment to enhance digital security.

Adapting existing regulations to face the challenges of the future

To ensure an inclusive digital transformation, a key objective among OECD countries, removing barriers to infrastructure deployment and getting the regulatory measures right, becomes even more crucial with the next evolution of networks. Policy makers can help ensure that high-quality broadband connectivity reaches most of the society by strengthening regulatory and policy frameworks that foster investment and promote competition. Therefore, going forward, adapting existing regulations to foster the deployment of the next evolution of broadband networks will become increasingly relevant.

This section explores trends and potential adaptation of communication regulations in the near future, to steer market activity towards desired policy objectives of the communication regulator of the future. While several regulations have been discussed in recent OECD work (see (OECD, 2022[3])), this section analyses three regulatory measures that have an impact on policy objectives relating to the market, users and the environment are analysed in more depth: wholesale access regulation, infrastructure sharing and co-investment. These three measures primarily aim at improving the efficiency and performance of markets and thus favouring network deployment (market dimension). They additionally aim at reducing costs and eliminating barriers to market entry, which may benefit network deployment in areas where deployment is typically more expensive, such as rural areas. Thus, they contribute to the objective of equal access to high-quality broadband (user dimension). In the environmental field, favouring infrastructure sharing and co-investment practices helps to reduce the environmental impact of network deployment.

Wholesale access regulation

For the purposes of this report, ‘wholesale access regulation’ is defined as the mandatory offering by network operators of specific wholesale elements of their network to other operators, on terms approved by a regulator or sanctioned by a court. It requires the incumbent to allow rivals to lease or grant access to certain individual building blocks that make up a communication network (network segments or layers). This concept is distinct from the concept of ‘network sharing’, which refers to an agreement between operators for the shared use of network elements, which may be subject to regulatory measures.

Wholesale access regulation aims to establish or restore conditions that provide effective competition, primarily by removing or reducing barriers to market entry. It allows competing operators to enter the market and rollout services with significantly less investment, ensures non-discriminatory access at appropriate fees to network elements that are essential and cannot be easily duplicated (essential facilities) to increase retail-based competition. Since wholesale access regulation has an important impact on market dynamics, regulators should be market-responsive to avoid undesirable effects, in particular disincentives to investment and innovation by both incumbents and entrants.

Wholesale access regulation is based on the regulatory approach of gradually offering potential entrants different levels of access to the incumbent network. Entrants begin with acquiring access at a level which requires little investment to provide their services and, as the entrants’ customer bases grow, they are encouraged to invest in the network elements to acquire access at the next level, and so on (‘ladder of investment’) (Cave, 2006[88]). This approach has been widely adopted in European countries and partially in other regions (e.g. Japan, Canada, and Australia), although early abandoned in the United States in favour of reliance on infrastructure based competition. There is an ongoing debate on the application of this approach to achieve successively higher levels of infrastructure investment by competitors (Cave, 2014[89]).

In the context of the roll-out of high-quality networks, in particular full-fibre networks, countries are implementing wholesale access regulation to incentivise investment. Compared to legacy copper-based networks, investments in fibre networks are still ongoing, in addition to the different network architecture itself. Some countries, such as Germany and Italy, have opted for regulated access at different wholesale levels, and differentiated pricing for each level of wholesale access to incentivise investment by alternative operators while at the same time aiming to adequately reward the investment risk of the regulated company. On the other hand, some countries, such as Portugal and Spain, have regulated wholesale access applied to passive infrastructure (“ducts and poles access (DPA) first” approach) that, coupled with forbearance on fibre access regulation contrasts with the regulatory strategy pursued in France, that placed more emphasis on the promotion of retail-based competition.

In line with the regulatory forbearance approach, there is a general tendency to focus on wholesale access regulation where it is needed, and to remove regulation in those parts of the market where it is no longer necessary. This is done by segmenting the market and designing regulation adapted to the competitive situation in each segment (segmented regulation), including deregulation if the necessary conditions are met. In particular, trends towards segmented access regulation are observed in the geographic and product (consumer and time) dimensions of market definition.

Geographic dimension

Since the liberalisation of communication markets, the development of infrastructure-based competition has been geographically heterogeneous. End-to-end competition based on two or more infrastructures may be possible in dense urban areas with relatively low deployment costs and high demand but is unlikely to be feasible elsewhere, creating continuing challenges for effective competition. High-speed network deployments may further increase this geographic heterogeneity of markets. Thus, among others, the greater availability of fibre and siting alternatives (e.g. street furniture, lighting poles etc.) further benefit the development of 5G in urban areas, both mobile and fixed wireless access (FWA), increasing their competitive gap with less densely populated areas.

Moreover, the economies of scope between mobile and FWA deployments may substantially increase infrastructure competitiveness in these areas, which can be hidden by a lack of geographic market segmentation. Geographical units subject to market analysis have a major impact on the outcome of this analysis and therefore on the regulatory remedies to be applied. Although the circumstances described above seem to recommend sub-national segmentation, its practicability is limited, partly due to the cost of implementation and supervision (BEREC, 2019[90]).

For example, Ofcom, which, in the context of the review of the physical infrastructure market for the period 2019 – 2021, undertook a very granular assessment of the presence of alternative infrastructure across the United Kingdom, defined four sub-national markets based on network presence. However, in its conclusions for the period 2021-2026, Ofcom considered that the advantage of BT's ubiquitous physical communication infrastructure would continue to result in a level playing field in all areas and decided to define a single national geographic market excluding the Hull area (Ofcom, 2021[91]).[18]

At the European level, only 14 national regulatory authorities applied geographic segmentation in their market analyses, in eleven cases they differentiated remedies geographically and in only two cases geographic segmentation of remedies was applied in a sub-national market (May 2018) (BEREC, 2018[92]). There are also differences in the criteria for setting the geographic boundaries for segmentation. Here, regulators consider not only the existence of parallel broadband networks, but also an assessment of the potential for infrastructure competition in the future. In some countries this competition prospecting is done based on theoretical considerations on the replicability of networks. This is the case in France, where the main criteria used by Arcep to designate prospectively competitive areas were housing type, population density and other factors it considered to affect the viability of deployment, as well as announcements by operators on the generalisation of deployment. In other countries such as Portugal and Spain, the regulator left an initial period of regulatory forbearance, and then carried out an analysis based on a combination of actual coverage and competitive factors. This second approach allows the analysis to be based on actual data rather than predictions about competitive fibre deployment, thus avoiding the risk that regulation could itself affect incentives and outcomes. It also allows to take into account the impact of commercial deals (including arrangements for co-investment and access) on competition in the market, as provided for in the European framework legislation (Godlovitch et al., 2019[93]).

Finally, it is worth noting that geographically segmented regulation may lead to deregulation in some markets such as last-mile fibre, but may also lead to a different approach to regulation, e.g. access to passive infrastructure or access to backhaul or transport network fibre.

Product market dimension

In terms of the market products, competition analysis usually considers networks with specific architectures and technologies, generally fixed networks as in the copper era. However, the deployment of wireless networks such as FWA results in services that may substitute those offered by fixed networks, at least in certain geographical segments (Box 1). These developments may become more pronounced with the further deployment of 5G networks (OECD, 2021[2]).

In this context, a market definition based on technologically neutral products (e.g. services instead of networks) could lead to a more accurate competition analysis and thus to avoid over-regulation and investment disincentive.

Box 1. 5G-based FWA services

In certain areas, 5G-based FWA services could be alternatives to fixed-line broadband networks. A major player is Verizon in the United States. In areas where Verizon has not deployed its FiOS (FTTP) network, it is marketing 5G residential services. Verizon and other operators are deploying “home” and “mobile” 5G networks simultaneously, benefitting from economies of scope in deployment and from the fact that costs can be recovered both from mobile and home broadband customers.

Also notable is the Italian operator Fastweb that is deploying its Ultra Fixed Wireless Access (FWA) network. Fastweb’s offer combines the fibre with 5G with up to 1 Gpbs throughput in areas with less infrastructure in the country. Fastweb's Ultra FWA network currently reaches 500 Italian municipalities. Fastweb has also announced a 5G FWA expansion plan, with funding of EUR 3 billion (USD 3.55 billion[19]) over five years, which will increase the share of homes and businesses covered by Fastweb's own ultra-wideband network from 30% as of 2022 to 60% in 2024.

Source: (OECD, 2019[94]; Fastweb, 2022[95])

Infrastructure sharing and co-investment

Infrastructure sharing is the process whereby several operators agree to share network elements to reduce the costs of infrastructure deployment to what is considered to be a commercially viable and economically efficient level. The regulator’s role to encourage infrastructure sharing can take on the following types:

- Measures to impose passive infrastructure sharing. This is, for example, the case of the regulation derived from the transposition of the Broadband Cost Reduction Directive[20] in the European Union which establishes an obligation for passive infrastructure sharing between operators, as well as with other types of networks (utilities, transport).
- Supervision in the field of competition law enforcement. In this sense, regulators carry out ex-ante monitoring within the framework of merger control, and ex-post monitoring and enforcing competition law. This group also includes prior notification and authorisation measures whereby regulators assess proposals on a case-by-case basis, depending on how such sharing arrangements may affect competition.
- Measures to incentivise network sharing. These incentives may take the form of favourable conditions for frequency allocation, fiscal incentives, or exemptions from administrative fees.
- Dispute resolution. In the event of disputes between operators, the regulator can impose cost sharing fees as well as the terms regarding shared use (e.g. antenna sites).

Co-investment refers to agreements that divide responsibilities for deployment among the partners of the sharing agreement as well as joint ventures to invest in the deployment of networks. Operators can agree on sharing passive network elements (passive sharing), or active network elements (active sharing). Passive sharing includes co-location, site sharing, and mast sharing. Operators may also agree to share active elements in the access networks (e.g. Radio Access Network (RAN) network sharing), backhaul and backbone network.

RAN sharing is especially relevant for the deployment of 5G networks, due to the high densification of base stations. RAN sharing consists of the sharing of active elements of the radio access network. Depending on whether operators share the same spectrum, a distinction can be made between Multi Operator Radio Access Network (MORAN) (no spectrum sharing), and Multi-Operator Core Network (MOCN) (with spectrum sharing), with the possibility of spectrum pooling.

Throughout the OECD, infrastructure sharing agreements are very common and most OECD countries foster infrastructure sharing while safeguarding competition. For example, passive infrastructure sharing is commonly practiced in many OECD countries and RAN sharing agreements continue to increase. In all cases of infrastructure sharing, it is important to keep the public policy goal of fostering competition in markets in mind. Typically, passive infrastructure sharing raises less concerns than active infrastructure sharing. However, especially in rural and remote areas, active infrastructure sharing can also be a viable way to not only ensure that mobile coverage is extended, but also to ensure that different operators can compete with their offers in those areas (OECD, 2021[96]).

In Korea, for example, SK Telecom, KT, and LGU+ signed a sharing agreement in April 2021 to allow shared access to their respective 5G networks in 131 rural and coastal locations (The Korean Bizwire, 2021[97]). Given network densification with the further deployment of 5G and related costs, it is expected that the number of sharing agreements increases across the OECD.

The objectives of regulatory intervention in the field of infrastructure sharing are driven by market efficiency, but also by user and environmental benefits. Many operators consider the sharing of existing passive infrastructure, as well as the coordination of civil works and other co-investment or joint deployment mechanisms, to have a significant impact on the timely and efficient deployment of electronic communications networks (Box 2).

In terms of market performance, the regulatory objective of infrastructure sharing is twofold. On the one hand, it supports economic efficiency in network deployment, which in turn drives network extension and the availability of services to users. On the other hand, it avoids harmful effects on the market such as barriers to entry for new entrants through anti-competitive practices, or disincentives to investment or innovation (OECD, 2014[98]). In the environmental field, the policy objective is to minimise the environmental impact of network infrastructures. Thus, practices such as 'dig once' (joint deployment) help to harmonise network deployment with land-use planning. Likewise, the co-location of sites or masts reduces the environmental footprint of radio networks.

Box 2. Public consultation on the European Union's Broadband Cost Reduction Directive

The European Commission held a public consultation on the review of the Broadband Cost Reduction Directive, which aims to facilitate and incentivise the deployment of high-speed communication networks with physical infrastructure measures. The public consultation was answered by both regulators, operators and other interested stakeholders. According more than two thirds of respondents (77%), access to existing physical infrastructure has a significant impact on the timely and efficient deployment of communication networks.

The respondents considered that the lack of availability of suitable physical infrastructure (76%), the difficulty to agree on terms and conditions of access with owners of physical infrastructure (58%) and the slow or ineffective dispute resolution process (54%), leads to a more costly or lengthy network deployment.

It is also noteworthy the relevance of the coordination of civil works and other co-investment or joint roll-out mechanisms for a majority of the participants of the public consultation (62%). In particular, survey respondents point to the relevance of coordination with the deployment of other communication networks (71%), with transport networks, including railways, roads, ports and airports-(68%), and with electricity networks, including public lightning-(67%).

As a precondition for the implementation of both access to physical infrastructure and the coordination of civil works, the importance of information availability is also highlighted. Most of the respondents indicate that public information has a significant impact on the timely and efficient deployment of networks. Namely, information concerning existing physical infrastructure, 79% of respondents, information about other elements and facilities suitable to install network elements (e.g. street furniture, lighting), 71% of respondents, as well as information related to on-going or planned civil works, 68% or respondents.

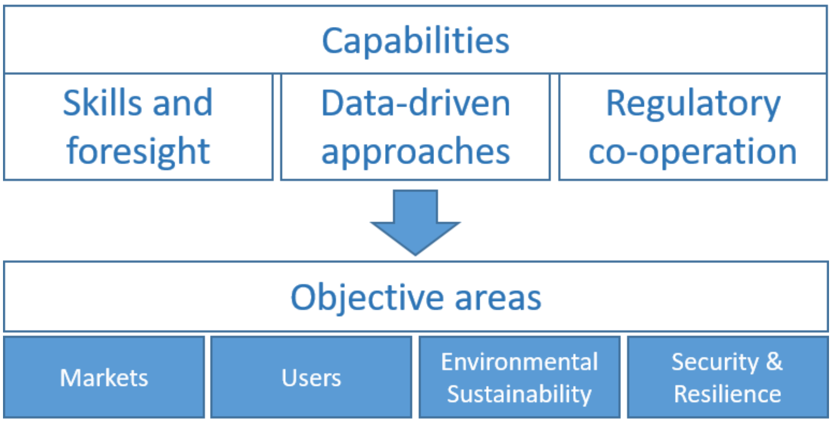
Source: (European Commission, 2021[13])

Analysis of recent regulatory developments reveals a trend towards fine-tuning regulations to keep pace with market developments. Beyond this, it is necessary to add a forward-looking perspective to the regulator's work, to identify market trends, assess the implications, and adapt regulations accordingly. On the other hand, the emergence of new policy objectives related to environmental and security challenges facing our societies, will led to new or significantly expanded roles and mandates for communication regulators. All this will undoubtedly require new capabilities for communication regulators, and the adaptation and improvement of existing regulatory measures, if not the design of new ones.

Capabilities of communication regulators of the future

In the face of technological developments and market transformation, communication regulators need to ensure they have the appropriate capacity and capabilities to respond to current and future challenges, to remain effective and efficient in delivering on policy objectives. Evolutions in the sector, and in particular, the rise of the digital transformation, have seen communication regulators take on new functions or even significantly expanded mandates. In this context, the capacity of a regulator to effectively deliver on its mandate is multidimensional. Communication regulators need to be equipped with the right knowledge and skills to keep pace with market developments and take advantage of new tools for regulating. Apart from keeping pace, regulators will also have to build foresight capacity to identify new innovations and assess their implications. Responding to new mandates or integrating new skills sets may require changes to internal structures. Moreover, regulators need to have the appropriate powers, whether for data collection and publication or for co-ordinating with other authorities, domestically and internationally (Figure 4).

Figure 4. Capabilities of communication regulators of the future



Source: OECD

Realising the full potential of innovation while addressing its risks requires a shift in regulatory policy and governance towards more agile and forward-looking approaches. The *OECD Recommendation for Agile Regulatory Governance to Harness Innovation* (OECD, 2021[99]) recognises that capacity and skills are key enabling factors for agile and innovation-friendly regulatory policy. In particular, regulators will need the capacity to: (i) ensure regulatory management tools such as regulatory assessment cycles are adaptive, iterative, and flexible to ensure regulations are fit for the future; (ii) enable regulatory co-operation and joined up approaches within and across jurisdictions; (iii) develop governance frameworks to enable the development of agile and future-proof regulation (e.g. through enhanced foresight capacity, use of outcome-based regulation); and (iv) adapt regulatory enforcement strategies and activities to promote compliance, for example, by adopting data-driven responsive approaches to identify, assess and manage risks.

Skills for the future

Regulators need to continually update and enhance the skills, knowledge, and capacity of their staff to keep pace with technological developments and changes in the sector, to deliver on evolving mandates, and to take advantage of the possibilities made available by digitalisation and big data on new ways to regulate.

The skills that communication regulators require are expanding, with a strong focus on digital and data skills. While the 'traditional' professions of engineers, economists and lawyers remain central, regulators are looking to reinforce their workforces with a range of additional specialist skills and professions. Regulators throughout the OECD are seeking data scientists and analysts, data architects and data engineers as well as experts on digital security, network security and network architecture, data centres and cloud computing. These specialists are seen as necessary for the delivery of regulatory functions due to developments in the market, e.g. experts on algorithms are needed for the oversight of online platforms to ensure non-discriminatory behaviour. They are also recognised as essential for regulators wanting to exploit digitalisation and big data for better regulatory delivery, for example using AI and machine learning to streamline reporting processes. As well as these highly specialised skills, the growing pervasiveness of digitalisation is spurring some regulators to consider a more general upskilling of their workforces in terms of data literacy. This will be key to supporting the formation of interdisciplinary teams consisting of economists, lawyers, technicians, industrial engineers, data scientists and data analysts, an ambition held by German regulator BNetzA, for example.

In addition to data and digital skills, regulators are seeking to introduce or reinforce other skills either to *keep pace with technological developments and related market evolutions* (e.g. including space-related skills such as space law and satellite filings, geographical survey experts, specialists for the next generation of mobile networks), *to meet new policy objectives* (e.g. skills related to sustainability and the circular economy) or *to ensure effectiveness at engaging with stakeholders* (e.g. public relations specialists).

Skills to carry out foresight exercises will be fundamental to address the “pacing problem”. The *OECD Recommendation for Agile Regulatory Governance to Harness Innovation* underlines the importance of enabling agile and future-proof regulation by developing the institutional capacity to conduct systematic and co-ordinated horizon scanning and scenario analysis, anticipating and monitoring the regulatory implications of high-impact innovations, actively engaging with stakeholders, and fostering continuous learning and adaptation. For example, in the energy sector, French regulator CRE created a Foresight Committee in 2017, bringing together energy industry stakeholders to consider the implications of the energy transition and digital revolutions (Commission de Régulation de l'Énergie, 2021[100]). The Colombian regulator, CRC, established an Innovation and Foresight unit, as well as a Data Analytics Intelligence unit, to meet the evolving challenges in relation to data and innovation.

Following a recommendation by the federal Broadcasting and Telecommunications Legislative Review Panel, the Canadian regulator, the CRTC, has recently invested in strengthening its research capacities, with the goal of developing strategic foresight on the sectors it regulates. The activities, which include establishing new industry data collection systems and conducting end-to-end survey operations and analytics for the communication sector, are led by a new division with a renewed focus on research and market intelligence (Government of Canada, 2022[101]).

At the same time, regulators may face constraints in meeting their skills needs. Regulators may operate within administrative constraints with regard to headcount or competitiveness of salaries due to general public administration rules and frameworks (OECD, 2020[102]). Communication regulators are often competing with the regulated sector for skilled professionals. In some cases, this may justify a deviation from the public sector norm and a need for certain autonomy to adjust salary scales (OECD, 2017[25]). The OECD Survey on the Resourcing Arrangements of Economic Regulators (OECD, 2022[103]) found that regulators that need to follow government remuneration on average face more difficulties to recruit and more frequently report salaries below those in the regulated sector. In the communications sector, regulator salaries tend to compare least favourably, with 67% of communications regulators reporting that their salaries are below those in the sector (OECD, 2022[103]). Importantly, the ability of regulators to attract and retain talent depends not just on the comparison of salaries with regulated entities, but also on the wider benefits to public sector employment (quality of workplace, non-monetary benefits, job stability, etc.). Care should also be taken, given the confidential nature of the regulators’ work, to avoid that bringing in new personnel with skills acquired in the regulated sector gives rise to potential conflicts of interests, to avoid undue influence in the regulator’s work (OECD, 2017[25]).

In addition to new recruitment, training and continued professional development also play an important role in ensuring that staff have relevant and up to date skills. Communication regulators are implementing a range of initiatives in this regard, including: bespoke development initiatives, coaching, peer-to-peer learning, communities of practice or professional networks, technical and professional training, and options to pursue formal education. For example, Brazil’s communication regulator Anatel established the Center for Advanced Studies in Telecommunications (*Centro de Altos Estudos em Telecomunicações*, Ceatel), responsible for defining the institutional policy for training and development of staff, organising training events and encouraging research on the communication sector, among other things (ANATEL, 2018[104]). To support staff members to expand their skills, 89% of communications regulators in the OECD Survey on the Resourcing Arrangements (OECD, 2022[103]) provide financial support to their technical staff to obtain external qualifications, such as academic qualifications, professional qualifications or external training courses. This share is higher than for regulators in the energy, transport and water sectors in the survey.

Some regulators expect to meet their skills needs by contracting specialised companies to help them develop more data-driven regulatory processes. Regulators cited the need to strike a balance between in-house resources and outsourcing. If carefully designed, outsourcing arrangements could be used to supplement or build up in-house skills. For example, in Australia, the ACMA is anticipating that its digital and ICT workforce will be supplemented with IT industry partners to uplift its capability but also to provide job rotation opportunities for staff to develop new skills. In Lithuania, the communication regulator joined an initiative by the government called the "GovTech Lab", aimed to bring in external skills to innovate public sector processes by involving start-ups and innovative tech companies to develop digital solutions.

Bringing in new skills may require significant change in terms of the governance of regulatory and operational decision-making, resourcing and internal structure. For example, as mandates evolve or institutions converge, regulators' decision-making bodies may need to adapt to include a diversity of skills and experience that is tailored to the functions of the regulator, in order to facilitate robust decision making. The enabling legislation should identify the skills set and experience relevant to the regulatory functions that need to be represented on the governing body (OECD, 2014[105]). Case studies of regulators that have successfully undergone organisational transformation point to the role of change management strategies to ensure that the organisational culture can adapt to and support these changes (OECD, 2020[102]).

When regulators consider their future skills and staff, sufficient attention should also be given to ensure the diversity and inclusiveness of the organisation, which has the potential to boost performance and innovation (Nolan-Flecha, 2019[106]). A 2021 OECD survey found that while regulators on average employ roughly equal shares of male and female staff, women constitute only 43% of senior management (OECD, 2022[103]). Diversity is one of the principles that guides recruitment at Canada's CRTC, alongside openness, transparency and merit. CRTC's recruitment strategies seek to attract qualified candidates who reflect Canada's diversity in terms of linguistic capacity[21], regional representation, and diversity[22] (Government of Canada, 2021[107]).

Data-driven regulatory approaches

Data and analytics, machine learning and the automation of processes are widespread in the private sector and are increasingly used by regulators. Several factors drive the development and adoption of digital technologies by regulatory agencies, such as business climate reforms, efficiency-based incentives and leadership (OECD, forthcoming[108]). Harnessing digital tools to improve enforcement is one of the principles laid down in the OECD *Recommendation for Agile Regulatory Governance to Harness Innovation* (OECD, 2021[99]). Digital tools can enable economic regulators to monitor communication markets more closely and in real time, significantly improving supervision, inspection, and enforcement activities. Data-driven regulation can also help reduce information asymmetries between the regulated entity and consumers. Additionally, the use of data could enhance the opportunities for more outcome-based regulations.

Digital tools and big data can enable the automation of regulatory processes. Automated data collection can ensure the availability of real-time information on market performance and compliance, which could make regulatory processes more efficient by reducing regulatory burdens and improving compliance. Systems that combine big data with digital tools can automatically process data to guide regulatory activities. For example, Costa Rica's communications regulator SUTEL is exploring a new spectrum monitoring system that uses big data and automation to recommend specific actions.

Regulators highlight the importance of data to increase publicly available information on the sector, which can support the functioning of markets by empowering consumers with accurate and up-to-date knowledge. An increase in available data on the regulated sector can be used as so-called "soft law" tools or “sunshine regulations”, tools which rely less on traditional powers of regulators but rather aim to improve performance through the availability of information (Université Paris Dauphine-PSL, 2021[109]). These tools are premised on the idea that regulators can strengthen accountability, transparency and the effectiveness of regulatory systems by making more data and information publicly available. A report by seven French regulatory bodies highlights that such approaches might be a powerful tool to reduce information asymmetries and improve transparency for consumers (OECD/KDI, 2021[110]).

For example, to empower consumers to make informed decisions, France’s communication regulator (Arcep), publishes maps with a detailed comparison of communication network coverage and quality (OECD, 2020[102]). Similarly, Canada publishes a National Broadband Internet Service Availability Map indicating retail broadband services and wholesale backbone infrastructure in Canada. The data used to create the map includes two key components that collectively describe Internet service availability in Canada: availability of retail broadband services by technology, speed and provider; and availability of wholesale high-capacity transport services within each community. Users can zoom in to view available Internet connectivity options by 250 metre road segments, or view area information about their community, including different technology types available, Internet service providers operating in the area, and publicly funded connectivity projects improving service (Government of Canada, 2022[111]). These initiatives to provide transparency and empower consumers with information may also generate positive incentives for operators to increase the quality of their services. Digital tools also hold the potential to help meet objectives regarding market developments, Users, or Environmental sustainability and market development.

Digitalisation and big data could also bring opportunities to enhance the benefits of outcome-based regulation. The OECD *Recommendation for Agile Regulatory Governance to Harness Innovation* recommends “developing more outcome-focused regulatory approaches to enable innovation to thrive by harnessing the opportunities offered by digital technologies and big data” (OECD, 2021[99]). Outcome-based models theoretically allow regulated entities to choose the most efficient way of achieving a regulatory goal, while lowering compliance costs (OECD, 2021[8]), and offer benefits such as increased flexibility and scope for innovation and more direct incentives to increase performance.

The use of digital technologies and big data can support the regulator in developing, monitoring and enforcing outcome-focused regulations, in particular by enabling remote and real-time monitoring of compliance and market developments. In the communication sector, there could be advantages of shifting to outcome-based regulation in some areas. This could warrant a shift towards a regulatory framework that targets more precisely the achievement of specific outcomes through a system of incentives and obligations and relies less on the control of market entry.

The ability of regulators to use data-driven tools as part of their toolkit depends on the existence of appropriate powers for them to collect information and to share such information publicly. Changes in legislation may be required to adjust the legal powers assigned to regulators to enable them to respond to developments in the communication sector, such as the blurring of traditional market definitions (OECD, 2020[102]), and to put in place innovative regulatory approaches. For example, in France, through Order 2021-650, Arcep was granted additional powers to collect information not only on companies operating in the communication sector, but also those operating in closely related sectors, such as digital content providers (Légifrance, 2021[112]). Similarly, in a context where regulatory approaches are increasingly data-driven, the ability of regulators to carry out new functions – such as those related to environmental sustainability – may depend on the legal power and ability to collect relevant data.

To unlock the potential of data-driven regulation, some regulators are making efforts to develop internal data governance structures. The deployment of necessary digital infrastructure can support efficient and secure generation, collection, storage, management, sharing and dissemination of data. In Australia, ACMA works to improve the discoverability, usability and safety of data by building an enterprise level data analytics platform, as a means to improve its analytical capability. The increasing use of data will make it important for regulators to develop standards for the collection and storage of information within the organisation. The interoperability of data could also benefit from international standards to ensure harmonised approaches for data usage.

Overall, data-driven regulatory approaches can form part of the approaches used by communication regulators to ensure agile regulatory governance that stimulates innovation while upholding protection to citizens and society. Where the speed, breath and uncertainty of innovation is high, additional instruments such as sandboxes can be used to enable controlled experimentation and stimulate innovation (OECD, 2021[113]).

Regulatory co-operation

Regulatory co-operation is a key element of regulatory quality (OECD, 2012[9]) and will be an increasingly important capacity for communication regulators, both at the domestic, cross-sectoral level and internationally. The blurring of traditional market boundaries includes the entry of communication operators into other sectors, such as the payment services market, and greater interaction with providers in other sectors, such as power and transport networks, and vice versa. It will be increasingly important for regulators to share their experiences and lessons, co-ordinate regulatory approaches to prevent regulatory arbitrage or avoidance, ensure role clarity and co-operate on emerging issues, such as new challenges in evaluating the competitive landscape in different markets and mechanisms that ensure a continued promotion of competition and protection of consumers in individual sectors as well as broader digital ecosystems.

Domestic regulatory co-operation

There is a wide diversity in approaches to co-operation between regulatory authorities at the domestic level. Some regulators rely on informal co-ordination through ad hoc meetings, workshops or conferences. Others draw on more formal co-operation mechanisms such as memoranda of understanding (MoU) to facilitate information sharing and exchange of best practices.

The impetus for regulatory co-operation can come from different sources. If the legislative framework allows, it can be at the initiative of the regulator. In many jurisdictions, co-ordination is defined in specific legislation, such as requiring formal opinions from one regulator on another agency's draft decisions. At other times, the government may give instructions for regulatory co-operation. In Sweden, for example, more formal co-ordination between regulators is the result of government instructions that several authorities shall share the responsibility in a certain field. The effectiveness of such arrangements will depend on the capacity of regulators to identify opportunities and forge effective working relationships (OECD, 2014[24]). Furthermore, as stated in the *OECD Best Practice Principles on the Governance of Regulators*, there needs to be clear authority for co-ordination to remove uncertainty about the legality of any arrangements, and legislation should explicitly empower regulators to co-operate with other bodies in pursuit of the regulator's objectives (OECD, 2014[24]).

This capacity and legal clarity for co-ordination will likely become even more important going forward, as many communication regulators foresee the need for increased co-ordination, in particular in fields such as the "Internet economy" and digital platforms. Digitalisation engages a number of regulatory regimes, including communications, broadcasting, privacy and data, digital security, content, financial services, consumer protection and competition (OECD, forthcoming[114]). This, alongside the scale and global nature of many digital firms, makes the need for increased and more permanent forms of co-operation between regulators responsible for these regimes even greater. In recent years, some countries have seen a move towards more formalised co-operation structures between cross-sectoral regulators in the digital space.

One example is the United Kingdom's Digital Regulation Cooperation Forum (DRCF), formed in 2020, that brings together Ofcom, the Competition and Markets Authority (CMA), the Information Commissioner's

Office (ICO) and the Financial Conduct Authority (FCA). In the Netherlands, the Digital Regulation Co-operation Platform comprises the Authority for Consumers and Markets (ACM), the Data Protection Authority (AP), the Authority for the Financial Markets (AFM), and the Media Authority (CvdM). Arcep and Arcom set up a joint division on digital technology markets and new regulations set up in France in March 2020. In Mexico, the communication regulator (Instituto Federal de Telecomunicaciones, IFT) signed a Memorandum of Understanding with the Data Protection Authority and established a technical spectrum committee with stakeholders. These structures could go beyond just information sharing and might include sharing of expertise and resources, reporting on results and mutual support to enforcement procedures. In some cases, this might require legislative changes, in particular when data is shared beyond members for the purposes of investigative work or joint analysis. The emergence of these structures is an indication that existing forms of regulatory co-operation may not always be sufficient to address the complexity of the issues raised by the digital economy.

Importantly, co-operation at the domestic level tends to take place not just between regulatory bodies, but also vis-à-vis other public bodies. Regulatory bodies are not islands, but rather they are part of the policy making processes and are particularly engaged in policy implementation (OECD, 2017[25]). Given the knowledge and foresight capacity of regulators regarding developments in the regulated sector, their input could support the quality of policy making. Ninety-three percent of communication regulators included in the *2018 Indicators on the Governance of Sector Regulators* make recommendations or issue opinions on policy proposals by the executive, and in many cases the opinion is made public (OECD, 2021[8]). A report from the Body of European Regulators for Electronic Communications (BEREC) on lessons learned from the COVID-19 crisis also highlights the importance of co-operation among stakeholders in supporting an efficient crisis response to increase resilience (BEREC, 2021[115]).

International regulatory co-operation

Given the transboundary nature of online platforms, many communications regulators anticipate that international regulatory co-operation (IRC) and co-ordination will intensify. As affirmed in the OECD Best Practice Principles for International Regulatory Co-operation, “IRC encompasses a multiplicity of approaches, which are united by their focus on enhancing the interoperability of laws, regulations and regulatory frameworks. This includes a range of ‘softer’ activities beyond the development of rules, such as exchanging information and participating in international fora, which form the building blocks of rulemaking and regulatory co-operation” (OECD, 2021[116]). Indeed, many regulators across OECD countries participate in international networks, such as BEREC for European communications regulators and Regulatel for Latin American communications regulators. Importantly, IRC is not limited to the design phase of the regulatory governance cycle, but includes the downstream side of implementation, enforcement, and ex post management of regulation. Indeed, the upcoming European Union Digital Services Act includes provisions to promote co-operation between regulatory bodies responsible for the enforcement of the regulation.

To be effective, IRC requires an enabling governance structure with clearly defined roles and responsibilities and whole-of-government approach, giving strategic leadership as well as co-ordination across government on parallel co-operation initiatives. Unilaterally, regulators can start by leveraging traditional regulatory management tools (e.g. regulatory impact assessments, stakeholder engagement, *ex post* evaluations etc.) with an additional international “lens”, to learn from foreign peers early on in their consideration of regulatory or non-regulatory alternatives, to measure unintended international impacts on innovation or trade or to consult foreign stakeholders. The (OECD, 2021[116]) could be instructive for regulators needing to navigate this complexity.

Conclusion

The communication sector is undergoing high-paced developments driven by the digital transformation of our economies and societies. Communication regulators are at the heart of this transformation, but also must constantly develop to embrace opportunities laying ahead. Addressing the challenges posed by the digital transformation requires coherent regulatory approaches. Adequate regulatory frameworks are indispensable to keep pace with technology and market developments.

To respond to the challenges of future communication regulation, countries need to adapt these frameworks. While there is no one-size-fits-all approach, the report presents different options to adjust to an ever-evolving environment, ranging from the accommodation and expansion of mandates to elevated levels of regulatory co-operation. Adapting existing regulations to foster the deployment of the next evolution of broadband networks will become increasingly relevant. Finally, communication regulators of the future will need commensurate capabilities to deliver upon their mandate, in a context where market evolution and a rapidly advancing digital transformation are reshaping functions and expectations.

Annex

Table A.1. Converged regulators: Communication and broadcasting

Country	Communication regulator	Converged broadcasting and communication regulator?
Australia	Australian Communications and Media Authority (ACMA)	Yes
Austria	Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)	No
Belgium	Belgian Institute for Postal Services and Telecommunications (BIPT)	No*
Canada	Canadian Radio-television and Telecommunications Commission (CRTC)	Yes
Chile	Subsecretaría de Telecomunicaciones (Subtel)	No
Colombia	Communications Regulation Commission (CRC)	Yes
Costa Rica	Superintendencia de Telecomunicaciones (SUTEL)	No
Czech Republic	Czech Telecommunication Office (CTU)	No**
Denmark	Danish Business Authority (DBA)	No
Estonia	Consumer Protection and Technical Regulatory	Yes
Finland	Finnish Transport and Communications Agency (Traficom)	Yes
France	Autorité de régulation des communications électroniques et des postes (ARCEP)	No
Germany	Bundesnetzagentur (BNetzA)	No
Greece	Hellenic Telecommunications and Post Commission (EETT)	No
Hungary	National Media and Infocommunications Authority (NMHH)	Yes
Iceland	Electronic Communications Office of Iceland (ECOI)	No
Ireland	Commission for Communications Regulation (ComReg)	No
Israel	Ministry of Communications (MOC)	No
Italy	Autoritá per le garanzie nelle comunicazioni (AGCOM)	Yes
Japan	Ministry of Internal Affairs and Communications (MIC)	Yes
Korea	Ministry of Science and ICT(MSIT); Korea Communications Commission (KCC)	Yes
Latvia	The Public Utilities Commission of Latvia (SPRK)	No
Lithuania	Communications Regulatory Authority of the Republic of Lithuania (RRT)	No
Luxembourg	Institut luxembourgeois de régulation (ILR)	No
Mexico	Instituto Federal de Telecomunicaciones (IFT)	Yes
Netherlands	Autoriteit Consument & Markt (ACM)	No
New Zealand	Commerce Commission	No
Norway	Norwegian Communications Authority (Nkom)	No
Poland	Office of Electronic Communications (UKE)	No
Portugal	Autoridade Nacional de Comunicações (ANACOM)	No
Slovak Republic	Telecommunications Regulatory Authority	No
Slovenia	Agency for Communications Networks and Services of the Republic of Slovenia (AKOS)	Yes
Spain	Comisión Nacional de Mercados y de la Competencia (CNMC)	Yes
Sweden	The Swedish Post and Telecom Authority (PTS)	No
Switzerland	Office fédéral de la communication (OFCOM); Federal Communications Commission (ComCom)	Yes
Türkiye	Information and Communication Technologies Authority (BTK)	No
United Kingdom	Office of Communications (Ofcom)	Yes
United States	Federal Communications Commission (FCC)	Yes

Notes: *Belgium: In Belgium, the Communities are competent for the technical aspects and the contents of the audio-visual media services. However, in the bilingual Brussels-Capital Region, some activities of the media sector cannot be exclusively linked to one of the two Communities (the Flemish Community and the French Community): in that case, the Federal State is competent for these activities.
**Czech Republic: Spectrum management for all sectors are responsibility of CTU.
Sources: OECD elaboration based on responses to regulatory questionnaires and OECD (2017[117]), supplemented with national sources.

Table A.2. Mandate of communication regulators in OECD countries

Country	Digital security	Privacy	Online platforms	OTT services	Issues related to cloud computing	Issues related to end-user devices	Issues in the area of the IoT and AI	Issues related to the digital aspects of transportation	Issues related to health	Issues related to the sustainability of networks?
Austria	Partially	Partially	No	Yes	No	No	Partially	No	No	Partially
Belgium	Partially	Partially	No	Partially	No	Yes	Partially	No	No	No
Canada	Partially	Partially	No	Partially	No	Partially	No	No	No	Partially
Chile	Partially	Partially	Partially	Partially	Partially	Partially	Partially	Partially	Partially	Partially
Colombia	No	No	No	No	No	Yes	No	No	No	No
Costa Rica	Partially	Partially	No	Partially	No	Yes	Partially	Partially	Partially	No
Czech Republic	Partially	Partially	No	Partially	No	No	No	No	No	No
Estonia						Yes				Yes
Finland	Yes	Yes	Partially	Partially	Partially	Partially	Partially	Yes	No	Yes
France	No	No	No	Partially	No	No	No	No	No	Partially
Germany	Partially	Partially	Partially	Partially	No	Yes	Partially	Partially	No	Partially
Greece	No	No		No	No	Partially	No	No	No	No
Hungary	Partially	Partially	No	Partially	Partially	Partially	Partially	Partially	Partially	Partially
Iceland	Yes	Partially	No	No	Partially	Yes	Partially	Partially	No	Partially
Ireland	No	Partially	No	Partially	No	No	Partially	No	No	No
Israel	Partially	No	No	No	No	Yes	Partially	Partially	No	No
Japan	Yes	Yes	Partially	Yes	Partially	Yes	Partially	No	No	Yes
Korea	Yes	No	Partially	Partially	Yes	Yes	Yes	Partially	Partially	Yes
Latvia	No	No	No	No	No	No	No	No	No	Partially
Lithuania	Partially	No	No		No	Yes	Partially	No	No	No
Mexico	Partially	No	Partially	Partially	No	Yes	Partially	No	No	Partially
New Zealand	Partially	Partially	No	No	No	No	Yes	No	Partially	Yes
Norway	Partially	Partially	Partially	Partially	Partially	Partially	Partially	Partially	Partially	Partially
Poland	Yes	Yes	Yes	Yes	No	Yes	No	No	No	Partially
Portugal	No	No	No		No		No	No	No	No
Slovak Republic	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes
Slovenia	Partially	Partially	Yes	Yes	No	Partially	Partially	No	No	No
Spain	No	No	Partially	Partially	No	No	No	No	No	No
Sweden	Partially	Partially	Partially	Partially	No	Partially	Partially	No	No	
Switzerland	Partially	Partially	Partially	Yes	No	Yes	Partially	No	No	No
Türkiye	Yes	Yes		No		Partially	Partially		No	Yes
United Kingdom	Yes	No	Yes	Yes	Partially	Partially	Partially	No	No	No
Brazil	Partially	Partially	Partially	Partially	Partially	Yes	Partially	No	No	No
Singapore	Partially	Yes	Partially	Yes	No	Yes	Partially	No	Partially	Yes

Note: OECD countries, Brazil, and Singapore responded to the question "Does your national regulatory authority, with responsibility for communication/telecommunication/broadcasting services have the mandate for the following areas: Digital security, Privacy, Platforms, OTT services, Issues related to cloud computing, Issues related to end-user devices, Issues in the area of the IoT and AI, Issues related to the digital aspects of transportation, Issues related to health, Issues related to the sustainability of networks or ICTs more general?" As to the complexities of the remits of converged regulators as well as to the specific circumstances of each country, the response to this question and how to interpret the terms "yes", "partially", and "no" has been up to the discretion of the respondents to the survey. The table does not contain countries that did not respond to these questions.
Source: OECD elaboration based on the responses to the "*OECD Communication Infrastructures and Services Policy Questionnaire on Upcoming Reports*".

References

ACCC (2021), *News Media and Digital Platforms Mandatory Bargaining Code*, https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code. [35]

ANATEL (2018), *Resolution No. 691, of February 22, 2018 [Resolução nº 691, de 22 de fevereiro de 2018]*, https://informacoes.anatel.gov.br/legislacao/resolucoes/2018/978-resolucao-691#art2 (accessed on 25 April 2022). [104]

Arcep (2022), *Evaluation de l'impact environnemental du numerique en France et analyse prospective*, https://www.arcep.fr/uploads/tx_gspublication/etude-numerique-environnement-ademe-arcep-note-synthese_janv2022.pdf (accessed on 5 May 2022). [21]

Arcep (2022), *The Environment: 5G and networks' environmental footprint: Arcep engages in new work to inform the debate and identify levers of action*, https://en.arcep.fr/news/press-releases/view/n/the-environment-140122.html (accessed on 31 January 2022). [70]

Arcep (2019), *Réseaux du futur: L'empreinte carbone du numérique*, https://www.arcep.fr/uploads/tx_gspublication/reseaux-du-futur-empreinte-carbone-numerique-juillet2019.pdf (accessed on 6 August 2021). [69]

Arcep (2018), *Devices, the weak link in achieving an Open Internet*, https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf (accessed on 5 May 2022). [15]

Australian Government. Department of Home Affairs (2022), *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*. [87]

Australian Government. Department of Home Affairs (2021), *Protecting Critical Infrastructure and Systems of National Significance. Security Legislation Amendment (Critical Infrastructure) Bill 2020*. [86]

Autorité de la concurrence, AMF, Arcep, ART, CNIL, CRE, CSA, HADOPI (2020), *Accord de Paris et urgence climatique: enjeux de régulation*, https://www.arcep.fr/fileadmin/user_upload/publications/cooperation-AAI/publication_AAI-API_Accord_de_Paris_052020.pdf (accessed on 5 May 2022). [22]

BEREC (2021), *BEREC recommends clarifying the scope of the Digital Markets Act in relation to number-independent interpersonal communication services (NI-ICS)*, https://berec.europa.eu/eng/document_register/subject_matter/berec/press_releases/9967-berec-recommends-clarifying-the-scope-of-the-digital-markets-act-in-relation-to-number-independent-interpersonal-communication-services-ni-ics (accessed on 14 March 2022). [125]

BEREC (2021), *BEREC Report on COVID-19 crisis – lessons learned regarding communications networks and services for a resilient society*, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/10135-berec-report-on-covid-19-crisis-lessons-learned-regarding-communication-networks-and-services-for-a-resilient-society (accessed on 25 April 2022). [115]

BEREC (2021), *Report on the ex ante regulation of digital gatekeepers*, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/10043-berec-report-on-the-ex-ante-regulation-of-digital-gatekeepers (accessed on 5 May 2022). [16]

BEREC (2019), *BEREC Common position on infrastructure sharing*, https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/common_approaches_positions/8605-berec-common-position-on-infrastructure-sharing (accessed on 15 March 2022). [90]

BEREC (2018), *BEREC Report on the application of the Common Position on geographic aspects of market analysis*, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8308-berec-report-on-the-application-of-the-common-position-on-geographic-aspects-of-market-analysis (accessed on 15 March 2022). [92]

Bernat, L. (2021), “Enhancing the digital security of critical activities”, *Going Digital Toolkit Note, No. 17*, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf. [77]

BIPT (2019), *Strategic Plan 2020-2022*, https://www.bipt.be/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/425348345ee55f90ca0b2b6870780e8730b3fc5d/Strategic_plan_2020-2022.pdf (accessed on 10 January 2022). [72]

Bundesministerium der Justiz (2021), *Telecommunications Telemedia Data Protection Act of June 23, 2021 (BGBl. I p. 1982)*, https://www.gesetze-im-internet.de/ttdsg/ (accessed on 24 February 2022). [54]

Bundesnetzagentur (2022), *Datensicherheit [Data security]*, https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Unternehmenspflichten/Datenschutz/Datenschutzverletzungenmelden/start.html (accessed on March 2022). [81]

Bundesnetzagentur (2022), *Digitalisierung*, https://www.bundesnetzagentur.de/DE/Sachgebiete/Digitalisierung/start.html (accessed on 22 February 2022). [5]

Bundesnetzagentur (2022), *Elektronische Vertrauensdienste [Electronic Trust Services]*, https://www.elektronische-vertrauensdienste.de/cln_122/EVD/DE/Home/start.html (accessed on 14 March 2022). [80]

Bundesnetzagentur (2022), *Katalog von Sicherheitsanforderungen [Catalogue of security requirements]*, https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Sicherheitsanforderungen-node.html (accessed on 14 March 2022). [82]

Bundesnetzagentur (2022), *Privacy, Data protection in the telecommunications sector*, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Unternehmenspflichten/Datenschutz/start.html (accessed on 24 February 2022). [55]

Bundesnetzgentur (2022), *Publikationen zu Digitalisierung und Daten*, https://www.bundesnetzagentur.de/DE/Sachgebiete/Digitalisierung/Grundsatzpapier/grundsatzpapier-node.html (accessed on 13 January 2022). [31]

Cave, M. (2014), "The ladder of investment in Europe, in retrospect and prospect", *elecommunications Policy*, Vol. 38/8–9, pp. 674-683, https://doi.org/10.1016/j.telpol.2014.04.012. [89]

Cave, M. (2006), "Encouraging infrastructure competition via the ladder of investment", *Telecommunications Policy*, Vol. 30/3–4, pp. 223-237, https://doi.org/10.1016/j.telpol.2005.09.001. [88]

CISA (2022), *Critical Infrastructure Sectors*, Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors (accessed on 27 February 2022). [75]

CNMC (2021), *Plan de Actuación 2021-2022*, https://www.cnmc.es/consultas-publicas/cnmc/plan-actuacion-2021-2022 (accessed on 9 February 2022). [32]

Commission de Régulation de l'Énergie (2021), *Foresight Committee*, https://www.cre.fr/en/Energetic-transition-and-technologic-innovation/foresight-committee (accessed on 5 May 2022). [100]

ComReg (2021), *Electronic Communications Strategy Statement*, https://www.comreg.ie/media/2021/12/ComReg-ECS-Strategy-Statement-English-Dec-7-Final-Web.pdf (accessed on 8 February 2022). [67]

ComReg (2021), *Electronic Communications Strategy Statement 2021-2023*, https://www.comreg.ie/publication/electronic-communications-strategy-statement-2021-2023 (accessed on 13 March 2022). [68]

Congress of Mexico (2014), *LEY FEDERAL DE COMPETENCIA ECONÓMICA*, [Federal Economic Competition Law], https://www.diputados.gob.mx/LeyesBiblio/pdf/LFCE_200521.pdf. [38]

Council of the European Union (2021), *Interinstitutional File: 2020/0359(COD): Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 - General Approach*, https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf (accessed on 13 March 2022). [124]

CSA (2022), *Our Organisation*, https://www.csa.gov.sg/Who-We-Are/Our-Organisation (accessed on 14 March 2022). [84]

data-infrastructure.eu (2022), *GAIA X*, https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (accessed on 22 February 2022). [119]

DCMS (2022), *Open consultation: Telecoms security: proposal for new regulations and code of practice*, https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/telecoms-security-proposal-for-new-regulations-and-code-of-practice (accessed on 14 March 2022). [79]

DCRF (2021), *Digital Regulation Cooperation Forum—written evidence (DRG0019), House of Lords Communications and Digital Committee inquiry into Digital Regulation*, https://committees.parliament.uk/writtenevidence/40479/pdf/ (accessed on 5 January 2022). [46]

DIGI (2021), *Australian Code of Practice on Disinformation and Misinformation*, https://digi.org.au/wp-content/uploads/2021/10/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-WORD-UPDATED-OCTOBER-11-2021.pdf. [65]

EUR-Lex (2021), *Amendments adopted by the European Parliament on 15 December 2021 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 20*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=EP%3AP9_TA%282021%290499 (accessed on 5 May 2022). [127]

EUR-Lex (2002), *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (accessed on 24 February 2022). [53]

European Commission (2022), *ePrivacy Regulation | Shaping Europe's digital future*, https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation (accessed on 10 March 2022). [121]

European Commission (2021), *Broadband Cost Reduction Directive: summary report of the consultation for its review*, https://digital-strategy.ec.europa.eu/en/broadband-cost-reduction-directive-summary-report-consultation-its-review (accessed on 5 May 2022). [13]

European Commission (2020), *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final*. [42]

European Commission (2020), *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN (accessed on 5 May 2022). [17]

European Commission (2020), *The Digital Services Act: ensuring a safe and accountable online environment*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en (accessed on 24 February 2022). [62]

European Commission (2018), "Directive (EU) 2018/1972 of the European Parliament and of the Council of December 2018 establishing the European Communications Code", *Official Journal of the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972 (accessed on 14 March 2022). [36]

European Commission (2017), *Proposal for a Regulation on Privacy and Electronic Communications*, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications (accessed on 24 February 2022). [58]

European Commission (2016), *Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148& (accessed on 13 March 2022). [122]

European Commission (2014), "Directive 2014/61/EU of the European Parliament and of the Council of May 15 2014 on measures to reduce the cost of deploying high-speed electronic communications networks", *Official Journal of the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0061&from=pl (accessed on 14 March 2022). [126]

European Parliament (2022), *Legislative train schedule: Review of the Directive on security of network and information systems*, https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive (accessed on 13 March 2022). [123]

Fastweb (2022), *Il futuro è 5G*, https://www.fastweb.it/corporate/futuro-piu-connesso/la-nostra-rete/5g/ (accessed on 3 March 2022). [95]

FCC (2022), *About the FCC: Federal Communications Commission*, https://www.fcc.gov/about-fcc/what-we-do (accessed on 5 2022 May). [12]

Godlovitch, I. et al. (2019), *Prospective competition and deregulation An analysis of European approaches to regulating full fibre for BT With contributions from*, WIK-Consult. [93]

Government of Canada (2022), *Canadian Radio-television and Telecommunications Commission: gneral Plans and Reports*, https://crtc.gc.ca/eng/publications1.htm (accessed on 5 May 2022). [101]

Government of Canada (2022), *Government introduces a bill to ensure fair compensation for news media and the sustainability of local news*, https://www.canada.ca/en/canadian-heritage/news/2022/04/government-introduces-a-bill-to-ensure-fair-compensation-for-news-media-and-the-sustainability-of-local-news.html. [41]

Government of Canada (2022), *Government of Canada announces expert advisory group on online safety*, https://www.canada.ca/en/canadian-heritage/news/2022/03/government-of-canada-announces-expert-advisory-group-on-online-safety0.html (accessed on 5 May 2022). [48]

Government of Canada (2022), *Government of Canada Introduces Legislation to Support the Next Generation of Canadian Artists and Creators*, https://www.canada.ca/en/canadian-heritage/news/2022/02/government-of-canada-introduces-legislation-to-support-the-next-generation-of-canadian-artists-and-creators.html. [40]

Government of Canada (2022), *National Broadband Internet Service Availability Map*, https://www.ic.gc.ca/app/sitt/bbmap/hm.html?lang=eng\ (accessed on 4 May 2022). [111]

Government of Canada (2021), *Governor in Council appointments*, https://www.canada.ca/en/privy-council/topics/appointments/governor-council.html (accessed on 6 May 2022). [107]

Government of Canada (2020), *Broadcasting and Telecommunications Legislative Review*, https://www.ic.gc.ca/eic/site/110.nsf/eng/home (accessed on 11 January 2022). [47]

Government of Canada (1993), *Telecommunications Act*, https://laws-lois.justice.gc.ca/eng/acts/t-3.4/page-1.html (accessed on 14 March 2022). [14]

Government of Ireland (2021), *Climate Action and Low Carbon Development (Amendment) Bill 2021*, https://www.gov.ie/en/publication/984d2-climate-action-and-low-carbon-development-amendment-bill-2020/ (accessed on 8 February 2022). [71]

Government of Japan (1984), *Telecommunications Business Act (Act No. 86 of 1984) [Amendment of Act No. 75 of 2021]*, https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_2.pdf (accessed on 5 May 2022). [19]

House of Lords, select committee on communications (2019), *Regulating a digital world, 2nd report of session 2017-19*, https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf (accessed on 5 January 2022). [45]

IFT (2021), *Plataformas Digitales OTT*, https://www.ift.org.mx/sites/default/files/contenidogeneral/competencia-economica/plataformasdigitalesott.pdf (accessed on 4 August 2022). [39]

IMDA (2021), *https://www.imda.gov.sg/regulations-and-licensing-listing/infocomm-media-cyber-security*, https://www.imda.gov.sg/regulations-and-licensing-listing/infocomm-media-cyber-security (accessed on 14 March 2022). [83]

Korea Communications Commission (2018), *Telecommunications Business Act. Partial Amendment*, https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=TELECOMMUNICATIONS+BUSINESS+ACT&x=35&y=17#AJAX (accessed on 29 July 2022). [18]

Légifrance (2021), *Ordonnance n° 2021-650 du 26 mai 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et relative aux mesures d'adaptation des ...*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043534846 (accessed on 22 February 2022). [112]

Ministry of Economy and Finance of Korea (2020), *Government releases an English Booklet of the New Deal*, https://english.moef.go.kr/pc/selectTbPressCenterDtl.do?boardCd=N0001&seq=4948. [66]

Ministry of Internal Affairs and Communications (2022), *Study Group on Governance of Cybersecurity and Data in Telecommunications Business*, https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000237.html (accessed on 28 February 2022). [59]

Ministry of Internal Affairs and Communications (2021), *Release of Interim Report from Study Group on Platform Services and Result of Appeal for Opinions*, https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000128.html (accessed on 25 February 2022). [63]

Ministry of Internal Affairs and Communications - Japan (2021), *2021 White Paper on Information and Communications in Japan*, https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/whitepaper/2021/pdf/contents.pdf (accessed on 5 May 2022). [23]

Ministry of Internal Affairs and Communications, Japan (2021), *Information and Communications in Japan 2021. Chapter 5. ICT Policy Directions.*, https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/whitepaper/2021/index.html (accessed on 5 May 2022). [20]

Ministry of Internal Affairs and Communications, Personal Information Protection Commission (2022), *Guidelines for Protection of Personal Information in Telecommunications Business (PPC and MIC Public Notice No. 4 of March 31, 2022)*, https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html (accessed on 26 April 2022). [52]

MinTIC (2019), *Presidente Duque sancionó la Ley de Modernización del sector TIC*, https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/101905:Presidente-Duque-sanciono-la-Ley-de-Modernizacion-del-sector-TIC (accessed on 11 February 2022). [27]

NMHH (2022), *Our tasks*, https://english.nmhh.hu/the-nmhh (accessed on 13 January 2022). [28]

Nolan-Flecha, N. (2019), “Next generation diversity and inclusion policies in the public service: Ensuring public services reflect the societies they serve”, *OECD Working Papers on Public Governance*, No. 34, OECD Publishing, Paris, https://doi.org/10.1787/51691451-en. [106]

OECD (2022), “Broadband networks of the future”, *OECD Digital Economy Papers*, No. 327, OECD Publishing, Paris, https://doi.org/10.1787/755e2d0c-en. [3]

OECD (2022), *Equipping Agile and Autonomous Regulators*, The Governance of Regulators, OECD Publishing, Paris, https://doi.org/10.1787/7dcb34c8-en. [103]

OECD (2022), *E-waste generated, kilograms per inhabitant*, https://goingdigital.oecd.org/indicator/53 (accessed on 9 March 2022). [120]

OECD (2021), “Bridging connectivity divides”, *OECD Digital Economy Papers*, No. 315, OECD Publishing, Paris, https://doi.org/10.1787/e38f5db7-en. [96]

OECD (2021), *Broadband Policy and Technology Developments*, https://www.oecd-ilibrary.org/docserver/e273ff77-en.pdf?expires=1645439318&id=id&accname=ocid84004878&checksum=2CB8BFFBCBDCFC503BB5C477DF9B0984 (accessed on 21 February 2022). [6]

OECD (2021), *Competition issues concerning news media and digital platforms*, https://www.oecd.org/daf/competition/competition-issues-in-news-media-and-digital-platforms.htm. [44]

OECD (2021), “Emerging trends in communication market competition”, *OECD Digital Economy Papers*, No. 316, OECD Publishing, Paris, https://doi.org/10.1787/4ad9d924-en. [2]

OECD (2021), *International Regulatory Co-operation*, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, https://doi.org/10.1787/5b28b589-en. [116]

OECD (2021), *Interoperability of privacy and data protection frameworks“, Going Digital Toolkit Note, No. 21*, https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf. [57]

OECD (2021), *OECD Recommendation on Agile Regulatory Goverance to Harness Innovation*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464 (accessed on 4 October 2022). [99]

OECD (2021), *OECD Regulatory Policy Outlook 2021*, OECD Publishing, Paris, https://doi.org/10.1787/38b0fdb1-en. [8]

OECD (2021), *Practical Guidance on Agile Regulatory Governance to Harness Innovation*, https://legalinstruments.oecd.org/public/doc/669/51f6da97-c198-4c93-922f-1a5d80beae86.pdf (accessed on 5 May 2022). [113]

OECD (2021), *Recommendation of the Council on Broadband Connectivity, OECD/LEGAL/0322*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0322 (accessed on 4 January 2022). [10]

OECD (2020), "Current approaches to terrorist and violent extremist content among the global top 50 online content-sharing services"*, OECD Digital Economy Papers*, No. 296, OECD Publishing, Paris, https://doi.org/10.1787/68058b95-en. [61]

OECD (2020), "OECD bundled communication price baskets"*, OECD Digital Economy Papers*, No. 300, OECD Publishing, Paris, https://doi.org/10.1787/64e4c18a-en. [26]

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [30]

OECD (2020), *OECD Telecommunication and Broadcasting Review of Brazil 2020*, OECD Publishing, Paris, https://doi.org/10.1787/30ab8568-en. [29]

OECD (2020), "Protecting children online: An overview of recent developments in legal frameworks and policies"*, OECD Digital Economy Papers*, No. 295, OECD Publishing, Paris, https://doi.org/10.1787/9e0e49a9-en. [60]

OECD (2020), *Shaping the Future of Regulators: The Impact of Emerging Technologies on Economic Regulators*, The Governance of Regulators, OECD Publishing, Paris, https://doi.org/10.1787/db481aa3-en. [102]

OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, https://doi.org/10.1787/53e5f593-en. [43]

OECD (2019), "The effects of zero rating"*, OECD Digital Economy Papers*, No. 285, OECD Publishing, Paris, https://doi.org/10.1787/6eefc666-en. [34]

OECD (2019), "The operators and their future: The state of play and emerging business models"*, OECD Digital Economy Papers*, No. 287, OECD Publishing, Paris, https://doi.org/10.1787/60c93aa7-en. [1]

OECD (2019), "The road to 5G networks: Experience to date and future developments"*, OECD Digital Economy Papers*, No. 284, OECD Publishing, Paris, https://doi.org/10.1787/2f880843-en. [94]

OECD (2017), *Creating a Culture of Independence: Practical Guidance against Undue Influence*, The Governance of Regulators, OECD Publishing, Paris, https://doi.org/10.1787/9789264274198-en. [25]

OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, https://doi.org/10.1787/9789264276284-en. [117]

OECD (2014), *Connected Televisions: Convergence and Emerging Business Models*, https://one.oecd.org/document/DSTI/ICCP/CISP(2013)2/FINAL/en/pdf (accessed on 11 January 2022). [33]

OECD (2014), “Decision making and governing body structure for independent regulators”, in *The Governance of Regulators*, OECD Publishing, Paris, https://doi.org/10.1787/9789264209015-8-en. [105]

OECD (2014), *The Governance of Regulators*, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, https://doi.org/10.1787/9789264209015-en. [24]

OECD (2014), “Wireless Market Structures and Network Sharing”*, OECD Digital Economy Papers*, No. 243, OECD Publishing, Paris, https://doi.org/10.1787/5jxt46dzl9r2-en. [98]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [49]

OECD (2012), *Recommendation of the Council on Regulatory Policy and Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264209022-en. [9]

OECD (2002), *Regulatory Policies in OECD Countries: From Interventionism to Regulatory Governance*, OECD Reviews of Regulatory Reform, OECD Publishing, Paris, https://doi.org/10.1787/9789264177437-en. [7]

OECD (2000), “Telecommunications Regulations: Institutional structures and responsibilities”*, OECD Digital Economy Papers*, No. 48, OECD Publishing, Paris, https://doi.org/10.1787/236438205724. [128]

OECD (1995), *Recommendation of the Council on Improving the Quality of Government Regulation*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0278 (accessed on 18 February 2022). [118]

OECD (forthcoming), *Developments in Spectrum Management for Communication Services*, https://one.oecd.org/document/DSTI/CDEP/CISP(2022)1/REV2/en/pdf. [11]

OECD (forthcoming), *Digitalising Regulatory Delivery Using Emerging Technologies*. [108]

OECD (forthcoming), *Enhancing the security of communication infrastructure*. [76]

OECD (forthcoming), *Implementation of the 2007 OECD Council Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy: Draft Monitoring Report*. [50]

OECD (forthcoming), *Summary Record: OECD Experts’ Meeting on Institutions and Regulatory Governance of Digital Platforms*. [114]

OECD/KDI (2021), *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*, OECD Publishing, Paris, https://doi.org/10.1787/8fa190b5-en. [110]

Ofcom (2021), *Promoting competition and investment in fibre networks: Wholesale Fixed Telecoms Market Review 2021-26 Volume 2: Market analysis*. [91]

Ofcom (2021), “Technology Futures Spotlight on the technologies shaping communications for the future”, https://www.ofcom.org.uk/__data/assets/pdf_file/0011/211115/report-emerging-technologies.pdf (accessed on 10 March 2022). [64]

Office of the Deputy Prime Minister for Investments and Informatisation of Slovakia (2019), *2030 Digital Transformation: Strategy for Slovakia*, https://www.mirri.gov.sk/wp-content/uploads/2019/10/SDT-English-Version-FINAL.pdf (accessed on 15 February 2022). [4]

OPCC (2014), *CASL memorandum of understanding*, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/canadas-anti-spam-legislation/mou_casl_2014/ (accessed on 24 February 2022). [56]

Parliament of Australia (2021), *Security Legislation Amendment (Critical Infrastructure) Bill 2021*, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6657 (accessed on 14 March 2022). [85]

RTR (2021), *Bundesverwaltungsgericht: Kommunikationsplattformen-Gesetz steht mit EU-Recht im Einklang*, https://www.rtr.at/medien/aktuelles/publikationen/Newsletter/RTR_Medien_04_2021/ErkenntnisseBVwGKoplG.de.html (accessed on 10 January 2022). [37]

Swiss Federal Council (1997), *Telecommunications Act (TCA) [784.10] [Status as of 1 July 2021]*, https://www.fedlex.admin.ch/eli/cc/1997/2187_2187_2187/en (accessed on 24 February 2022). [51]

The Korean Bizwire (2021), *S. Korean Telcos to Share 5G Networks in Remote Areas | Be Korea-savvy*, http://koreabizwire.com/s-korean-telcos-to-share-5g-networks-in-remote-areas/187457 (accessed on 11 August 2021). [97]

UK Parliament (2021), *Telecommunications (Security) Act 2021*, https://bills.parliament.uk/bills/2806 (accessed on 14 March 2022). [78]

UKRN (2022), *UK Regulators Network*, https://www.ukrn.org.uk/ (accessed on 7 January 2022). [73]

UKRN (2021), *UKRN annual report and multi-year workplan*, https://www.ukrn.org.uk/wp-content/uploads/2021/03/UKRN-workplan-and-annual-review-2021-for-publication-.pdf (accessed on 7 January 2022). [74]

Université Paris Dauphine-PSL (2021), *Sunshine Regulation: Implemented Practices and Observable Impacts - Conference report*, https://chairgovreg.fondation-dauphine.fr/sites/chairgovreg.fondation-dauphine.fr/files/attachments/synthese_Sunshine%20Regulation.pdf (accessed on 22 February 2022). [109]

End notes

[1] Although there is no accepted international definition of regulation, the term "regulation" is used broadly in this document to include the full range of legal instruments by which governing institutions, at all levels of government, impose obligations or constraints on private sector behaviour. Constitutions, parliamentary laws, subordinate legislation, decrees, orders, norms, licenses, plans, codes and even some forms of administrative guidance can all be considered as "regulation" (OECD, 1995[118]). The "communication regulator" refers to the body that is tasked with the supervision of communication regulations (see also (OECD, 2000[128])). The term "regulators" refers to "national regulators" but may under certain circumstances also apply to supra-national regulators.

[2] While network operators still represent the major source of financing for broadband deployment, there is no longer one configuration for a "network operator". What is referred to as a network operator in fact may involve a variety of business models. The different operators can be roughly categorised into four types : (i) traditional - vertically integrated - mobile and fixed broadband providers; (ii) vertically integrated cable operators; (iii) wholesale - vertically separated - operators (e.g. municipality networks providing access to dark fibre); (iv) and - terminal - equipment and online service providers.

[3] With Gaia-X, representatives from business, science and politics on an international level aim to create a next generation data infrastructure proposal which is based on an open, transparent and secure digital ecosystem (data-infrastructure.eu, 2022[119]).

[4] Other policy instruments that may be used to this purpose, such as support programmes for operators or end-users or digital literacy programmes, fall outside the scope of regulation.

[5] Currently under approval (amendments adopted by the European Parliament on 15 December 2021 in (EUR-Lex, 2021[127])).

[6] E-waste refers to all items of electrical and electronic equipment that have been discarded as waste without the intent of re-use. It includes cooling and freezing equipment, screens and monitors, lamps, large equipment (e.g. washing machines and solar panels), small equipment (e.g. vacuum cleaners, microwaves and electronic toys), and small IT and telecommunications equipment (e.g. mobile phones, personal computers and printers) (OECD, 2022[120]).

[7] NIICS are defined in the EECC as one of the Interpersonal Communication Services (ICS) that allow interpersonal communication among a limited number of persons. The definition of ICS excludes communications between and with machines, as well as communication services provided as an ancillary service. BEREC is furthermore of the opinion that ICS (including NIICS) fall outside the definition of online platforms. Typically, NI-ICS do not allow publishing information to an unlimited group of recipients (BEREC, 2021[125]).

[8] "Communication services" as used in the OECD terminology is largely equivalent to what the European Commission defines as "electronic communication service".

[9] An exchange rate of 1.254 CAD/USD for the year 2021 from OECD.stat has been used.

[10] "The proposal for a regulation for ePrivacy rules for all electronic communications includes: Simpler rules on cookies: the cookie provision, which has resulted in an overload of consent requests for internet users,

will be streamlined. The new rule will be more user-friendly as browser settings will provide an easy way to accept or refuse tracking cookies and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies that improve internet experience, such as cookies to remember shopping-cart history or to count the number of website visitors" (European Commission, 2022[121]).

[11] Signatories to The Australian Code of Practice on Disinformation and Misinformation are committed to tackling the harms caused from digital content propagated by users of digital platforms that threatens democratic political and policymaking processes and public goods, such as citizens' health.

[12] The study identifies two scenarios based on identical traffic growth: a 4G-only network and a network that combines 4G and a 5G deployment. Initially, 5G will generate an increase in energy consumption – for a length of time that depends on different 5G rollout scenarios. After which 5G deployment will enable total energy savings of up to ten times 2020 consumption levels by 2028, compared to a scenario of 4G-only network densification, as well as a corresponding decrease of greenhouse gas (GHG) emissions of up to eight times 2020 GHG emissions. In less densely populated areas, however, where traffic density is lower, virtually non-existent gains will not be seen until 2025 at the earliest, and by 2028 at the latest.

[13] This was an Amendment to the Irish Climate Action and Low Carbon Development Act 2015.

[14] An exchange rate of 1.454 AUS/USD for the year 2020 from OECD.stat has been used.

[15] For more discussion on these challenges and how they are impacting communication infrastructure, please see the report on, "Enhancing the security of communication infrastructure" [DSTI/CDEP/CISP/SDE(2021)3/REV1].

[16] The Telecommunications (Security) act received Royal Assent on 17 November 2021 (UK Parliament, 2021[78]).

[17] Currently, EU members are subject to Directive 2016/1148 (NIS directive), however revisions to the Directive are currently being discussed (NIS 2 Directive) (European Commission, 2016[122]; European Parliament, 2022[123]). The original NIS directive applies to "operators of essential services and digital service providers", however operators providing "public communication networks or publicly available electronic communication services" are excluded from the scope, because they are subject to specific security obligations in the European Electronic Communications Code (EECC) (European Commission, 2016[122]). However, among the proposed revisions of the NIS 2 is to bring these operators also under the scope of the Directive, and repeal the related security provisions in the EECC (Council of the European Union, 2021[124]).

[18] Fixed communication markets in the Hull Area are regulated separately from the rest of the United Kingdom. This is because KCOM, rather than BT, is the incumbent communication provider, and is the owner of the only ubiquitous fixed network in the Hull Area. The Hull Area therefore has very different competitive conditions from the rest of the UK.

[19] An exchange rate of 0.845 EUR/USD for the year 2021 from OECD.stat has been used

[20] Directive 2014/61/EU of the European Parliament and of the Council of 15 may 2014 on measures to reduce the cost of deploying high-speed electronic communications networks (European Commission, 2014[126]).

[21] The Government considers bilingual (English and French) proficiency as part of its assessment of candidates.

[22] Women, Indigenous peoples, persons with disabilities, and members of visible minority and ethnic/cultural groups.