Why

Europe needs a true Digital Single Market

everyone.connected

Contents

01

Why Europe Needs a true Digital Single Market

The Single Market today

The Single Market was launched more than thirty years ago with the promise of making the European Union the world's most dynamic, competitive economic bloc – one where goods, services, capital, and people flow freely across national borders. On the back of this promise, Vodafone invested heavily across Member States, with the ambition of becoming a pan-European telecoms operator that would operate seamlessly across the EU.

Yet, three decades on and despite its resounding success in fuelling EU competitiveness in a number of sectors, the ambition of a true single market remains incomplete in the realm of digital communications. Instead of achieving pan-EU scale and global leadership, Europe's telecoms operators, including Vodafone, have continually been required to right-size their businesses, through gradual retreats from a broader EU footprint.

In contrast to countries like the US and China, which have genuine scale operators, the telecommunications market in Europe is characterised by a patchwork of three to four smaller operators per Member State, with no true pan-European operator.

Europe's telecom market still consists of 27 distinct markets with a mere thin veneer of common rules and regulations, which have not allowed cross-border synergies in the production or provisioning of communication services. As a result of this lack of scale, and its negative impact on investments, Europe has been left struggling to retain ground in the digital ecosystem, despite being a leader in connectivity in the late 1990s and early 2000s.

The heart of the problem is that Europe's regulatory environment no longer fits the technological and market realities of the modern communications sector. When the first generation of telecoms rules was designed some two decades ago, connectivity was delivered through traditional physical infrastructure controlled by single national operators. Since then, two key trends have emerged.

First, there has been a trend towards 'virtualisation', with many parts of the traditional physical infrastructure being replaced by software and cloud-based applications. Second, this virtualisation has allowed the communications stack to become 'delayered', meaning that communications services are no longer directly coupled with the networks they run over.

Together, these changes have enabled specialised providers to enter and offer services at different points of the digital communications value chain, and to provide these at scale, in many cases on a cross-border basis. This includes services that are complements to or even replacements for traditional telecommunications services, such as digital communications platforms like WhatsApp, circumventing the historic national boundaries of 'traditional' telecommunication services.

However, it has been predominantly large non-European, companies that have reaped the benefits of these trends. This is because the regulatory framework in the EU has failed to keep pace with technological and market shifts. Notwithstanding the fact that telecom operators have often the same technical ability as tech players to offer services cross-border and independent of physical network locations, the regulation still treats telecom services as tied to the national boundaries. As a result, when technologies have evolved, technology players have been able to exploit these for commercial gain in a manner that European telecom operators, due to nationally oriented regulation, have not.

In particular, the regulatory landscape for the digital communications sector is characterised by:

1. An uneven playing field: regulation is applied inconsistently across the communications ecosystem.
2. An incomplete single market: fragmentation of regulation across Member States.

An uneven playing field: regulation is applied inconsistently across the communications ecosystem

Despite the significant changes in how digital communications services are delivered, regulators have not adequately adapted the rules for new entrants to the digital communications value chain.

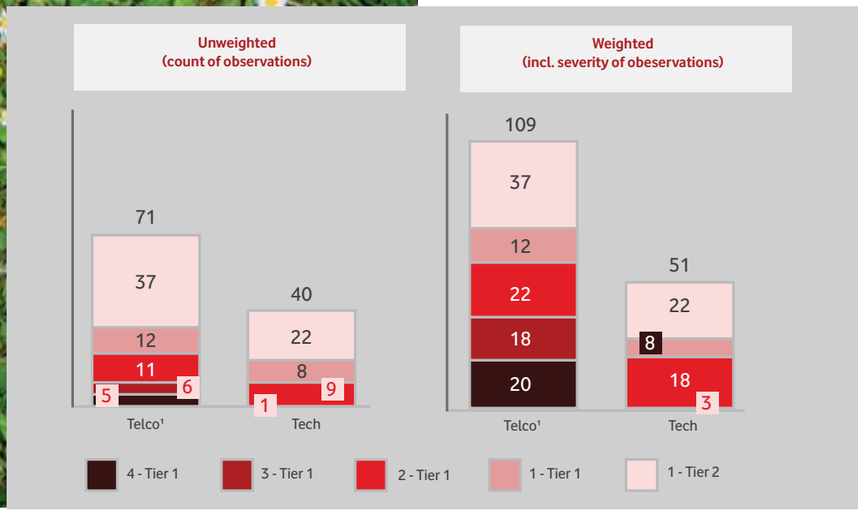
Telecoms regulation – initially developed when telecoms were primarily national monopolies – has tended to focus on liberalisation and facilitating the entry of new players into the sector. This has successfully promoted competition and consumer welfare, with consumers benefitting from more widespread and reliable access, new technologies and faster speeds. However, these rules have accumulated over time without being updated to reflect an increasingly complex digital ecosystem, and many now place a disproportionate burden on network operators.

Europe's integrated telecoms operators face a heavy regulatory burden – both at national and at EU level – stemming from a host of sectoral and general obligations. This includes areas such as security, net neutrality, consumer protection, law enforcement support, numbering and emergency calling. Near-equivalent or substitute services such as online messaging and content delivery are now managed "over the top" by digital platforms that lie beyond the reach of these sector-specific rules.

This fragmentation has created significant competitive distortions. Traditional operators, for example, are forced to allocate significant resource to simply comply with outdated rules. They are subject to considerably more stringent rules when offering equivalent communications services to other forms of digital communication service providers. Ambitious deployment targets in Europe – such as the Digital Decade programme – also increase investment pressures on operators, even as revenues from traditional communications services stagnate.

To size up this problem, Vodafone commissioned research to assess the range of regulatory measures applied across telco and tech firms (see Figure 1).[1] The left-hand side of the chart shows the number of regulatory interventions that are applied to telecoms and tech firms, categorised by severity of interventions. The right-hand side then weights each intervention according to this severity. The review shows that European telcos face regulatory obligations that are twice as onerous as those faced by their tech company competitors.

Figure 1: Relative regulatory burdens on telco and tech companies



An incomplete single market: fragmentation of regulation across Member States

Successive EU frameworks, such as the European Electronic Communications Code, have aimed to harmonise core sectoral regulatory principles. However, harmonisation has largely failed, because the transposition, interpretation and application of the rules continue to differ substantially from one Member State to the next. Even when EU rules exist, European operators are required to comply with 27 (or more) variations of these rules, thereby preventing them from offering truly pan-European services and reaping the full-scale economies and benefits promised by the single market.

For example, operators must modify their services from country to country to meet varied numbering plans,[2] unique know-your-customer (KYC) requirements,[3] differing emergency-calling mandates,[4] and inconsistent data retention rules,[5] to name just a few.

Even in areas where the overarching goals are the same, the administrative path to compliance can diverge substantially, raising costs and complexity for cross border delivery. Rather than seamlessly scaling up at a European level, telecoms providers find themselves replicating infrastructure and processes in each country.

For example, operators need to deploy separate cloud solutions for core networks in each market in which they are operating, increasing the cost of deploying cloud-based networks such as 5G standalone cores in Europe. As Mario Draghi points out:

> "This fragmentation makes the fixed costs of investing in networks relatively more onerous for EU operators than for continent-scale companies in the US or China. Fragmentation also makes it harder to capitalise on new technologies." [6]

Vodafone's experience is emblematic here. Instead of achieving its ambition of becoming a truly pan-European operator, it has been forced to retreat and exit EU markets one by one. Other major operators, which were once the crown jewels of European innovation, industrial prowess and global leadership, have also retreated.

Ultimately, such fragmentation discourages investment in large scale pan-EU deployments and slows Europe's ability to develop truly borderless digital services. Importantly, given that scale is essential for innovation, it undermines European competitiveness in the global race for technological leadership.

European competitiveness is at stake

The current regulatory landscape in the EU both prevents European operators from competing fairly with global platforms at the service layer and limits their ability to scale-up their networks and services. The resulting downwards pressure on financial returns means that operators in Europe are less able to invest effectively in advanced digital communications infrastructure and services. By illustration, telecoms capex per capita sits considerably behind other regions at €109 compared to, for example, the USA's €240 or Japan's €271.71.[7]

The resulting slower roll-out of advanced networks and new technologies has severe repercussions for European competitiveness and start-ups, given the importance of digitalisation for efficiency, productivity and innovation.

First, by falling behind in advanced connectivity, the EU risks falling further behind in all other economic sectors, especially those critical to future growth such as advanced manufacturing, healthcare, AI, and quantum computing. This is particularly true for cutting-edge innovations that rely or build on advanced connectivity networks, such as Virtual Reality and Autonomous Vehicles, which are increasingly led by players based elsewhere, particularly in the US and China.[8]

Second, the lack of a Digital Single Market prevents European technology firms, including telecommunications operators, from scaling easily. As Draghi points out, "Fragmentation of the Single Market hinders innovative companies that reach the growth stage from scaling up in the EU, which in turn reduces demand for financing".[9]

The numbers are striking: only 6% of total global funding for AI start-ups goes to EU companies, compared to 61% for US companies and 17% for Chinese companies. EU companies attract only 5% of global private funding for quantum computing, compared with a 50% share attracted by US companies.[10]

Innovation is therefore occurring and scaling elsewhere, before being sold back to Europe. The EU has become a net technology importer, rather than a pioneer. This poses a challenge to Europe achieving its digital sovereignty goals.

There is a growing consensus that the status quo is unsustainable. The European Commission's White Paper on 'How to master Europe's digital infrastructure needs?', the Letta Report, and the Draghi Report have all called for bold, future-looking reform to reignite Europe's digital leadership and create a genuine Digital Single Market.

Their recommendations share a clear direction. First, harmonise how Europe implements sectoral rules combined with further measures to enable scale,[11] And second, drive competitiveness by simplifying the rule book and ensuring a more level regulatory playing field where equivalent services face equivalent obligations. Only this type of action will enable truly pan-European development and delivery of the next generation of digital communications networks and services.

Vodafone welcomes these ideas. Truly reimagining Europe's digital regulatory framework will require strong political will, targeted legislative changes and thoughtful stakeholder collaboration. They are not easy fixes. Policy makers must balance national priorities and security concerns with the benefits of a cohesive single market.

There are also obstacles to practical implementation and risks which must be overcome.

Yet the urgency of the challenge is clear. In an era where global digital players can rapidly scale across continents, failing to move swiftly leaves Europe at a distinct disadvantage. The EU must therefore seize the opportunity to build on the momentum stemming from the recent discourse on European competitiveness and present a bold package of reforms to deliver a true Digital Single Market.

Policy makers must recognise this new technological reality and design a framework from this starting point, rather than continuing to make slow, piecemeal evolutions to outdated rules.

Reimagining change: a bold vision for a digital single market

To support this thinking, Vodafone has brought together a collection of expert perspectives to spark debate and catalyse meaningful reform. These contributions challenge policy makers to ask what an ideal, future-proof regulatory framework could look like if designed from scratch today, reflecting the delayering and virtualisation of networks, the emergence of new digital players, and the critical need for investment and innovation in Europe's communications infrastructure. Policy makers must recognise this new technological reality and design a framework from this starting point, rather than continuing to make slow, piecemeal evolutions to outdated rules.

Such a framework should be based on three core interlocking principles:

- **Simplification:** Regulations must be made fit for purpose in the modern digital ecosystem and ensure an effective rebalancing of the sector. The new framework should have as an overriding objective to create an environment that drives investment and innovation, and is focussed on achieving regulatory certainty and commercial outcomes, whilst reducing the significant compliance costs created by complex, overly prescriptive, disproportionate and duplicative regulations.

- **Same Service, Same Rules:** Equivalent services must be governed by equivalent rules to avoid competitive distortions. This can be achieved through a combination of limiting existing tech exemptions from regulation and/or streamlining legacy regulations. This should result in an integrated and proportionate regulatory framework for all providers of digital communication services.

- **Single Market:** A service provider in one market should be able to effectively deploy networks and provide services on a pan-EU basis, creating opportunities to scale. This will require the maximum harmonisation of digital sector rules, with national divergence only occurring if clearly and objectively justified.

The following expert contributions examine certain aspects of the regulatory framework, with the aim of providing inspiration and challenging policy makers and industry leaders to think creatively about how Europe can collectively achieve this vision of a more harmonised and proportionate regulatory framework.

Structure of this report

The subsequent chapters present six Vision Papers. Each Paper explores specific dimensions of the various challenges and proposes novel solutions and ideas. Drawing on robust academic research, industry insights, and learnings from other sectors, the Vision Papers cover topics such as new legislative frameworks for digital infrastructure and mechanisms to move beyond the outdated telecoms/technology divide.

In Chapter 2, Assembly Research proposes the foundational elements of a new Digital Communications Act, underpinned by the principles of fairness, symmetry, harmonisation, and proportionality. This paper explores how a single, overarching framework – when applied consistently – could replace the existing patchwork of telecom- and tech-specific laws.

In Chapter 3, Dr. Matthias Bauer and Dyuti Pandya of ECIPE explore the concept of 'passporting' for telecoms – drawing on the case study of the financial services sector – so that an operator authorised in one Member State can extend its services across borders without re-authorisation or duplication of regulatory burdens.

In Chapter 4, academic Professor Alexandre de Streel envisions a European System of Digital Regulators, drawing on models like the Single Supervisory Mechanism in banking. The paper explores how more centralised oversight, by, for example, a single European Digital Authority, could resolve persistent cross-border bottlenecks, leading to less fragmented enforcement of sectoral rules.

In Chapter 5, academics Dr. Wolfgang Briglauer and Professor Antonio Manganelli assess the ongoing debate around net neutrality, showing how the prescriptive interpretation of the Open Internet Regulation rules may fail to reflect new market realities. The paper recommends recalibrating net neutrality policies to balance open access with the need for investment in advanced network technologies, and calls for a re-examination of how large platforms' market power affects genuine 'openness'.

In Chapter 6, academic Arnault Barichella presents a case study on cybersecurity to illustrate how fragmented national approaches create 'weak links' in a 'multispeed Europe' that undermine the collective security of Europe's digital infrastructure. The paper proposes more harmonised EU-level standards and processes to safeguard networks.

In Chapter 7, Neil Brown of decoded.legal, examines lawful interception and law enforcement obligations, highlighting how disjointed national requirements complicate the operation of centralised telecoms infrastructures and hamper operators' ability to provide EU-wide services efficiently. The paper outlines potential frameworks for centralisation that preserve each Member State's legitimate law enforcement needs while still allowing pan-EU service architectures.

The contributions provided are the author's own, and reflect each of their independent perspectives. As such, inclusion in this report does not amount to a direct endorsement of the proposals set out in each paper either by Vodafone or by the other contributors.

Conclusion

The Single Market began with a bold vision of a unified European economic powerhouse, yet decades later, the potential of Europe's digital communications sector remains stymied by persistent fragmentation. The result is an uneven playing field, a burdened telecoms sector forced to maintain patchwork systems across Member States, and an increasingly obvious mismatch between legacy rules and today's converged digital environment.

Vodafone believes that realising a true Digital Single Market demands more than incremental revisions to the existing rule-book. We need a comprehensive re-think of Europe's regulatory architecture – replacing fragmented regulatory instruments with a proportionate, streamlined, and future-proof framework.

The upcoming EU legislative initiatives, such as the proposal for a Digital Networks Act, offer an opportunity to modernise digital communications regulation. By confronting these issues openly and ambitiously, European policy makers can unlock a new era of growth, connectivity, and competitiveness. Our hope is that the insights offered here will help EU legislators to move swiftlytowards a genuinely integrated, modernised regulatory framework – one that delivers on the original promise of Europe's Single Market and secures the region's leadership in the digital age.

Footnotes

1. Vodafone calls for A Framework for Responsible Use of Networks. See full report, page 27.
2. Accountability for defining the numbering plan remains with the national regulatory authorities. Depending on the Member State, the way numbers may be assigned and used differs dramatically.
3. In many Member States providers are obliged to collect data about their subscribers, and the rules vary from Member State to Member State on what must be collected.
4. The technical requirements of how emergency calls must be routed are different in each market, as are the rules on what and how caller information is provided to the emergency authorities.
5. Data retention and disclosure requirements are implemented domestically and there are no overarching international requirements.
6. The future of European competitiveness by Mario Draghi Draghi Report
7. The State of Digital Communications 2024 | Connect Europe
8. This is considered in detail in Vodafone's report on Responsible Use of Networks, accessible: Vodafone calls for A Framework for Responsible Use of Networks.
9. The future of European competitiveness by Mario Draghi
10. The future of European competitiveness by Mario Draghi
11. In particular, competition policy in the EU has historically focused on short-term consumer welfare through lower prices and high retail competition, often at the expense of ensuring sustainable returns for operators. Regulators have, however, started to consider the impact of greater investment for competition in the longer term. For example, the merger of Vodafone and Three in the UK recognises that both consumers and wider society benefit from transformative long-term network investments.
12. For example, there is no clear scientific reason as to why EMF limits should differ from one EU member state to another.

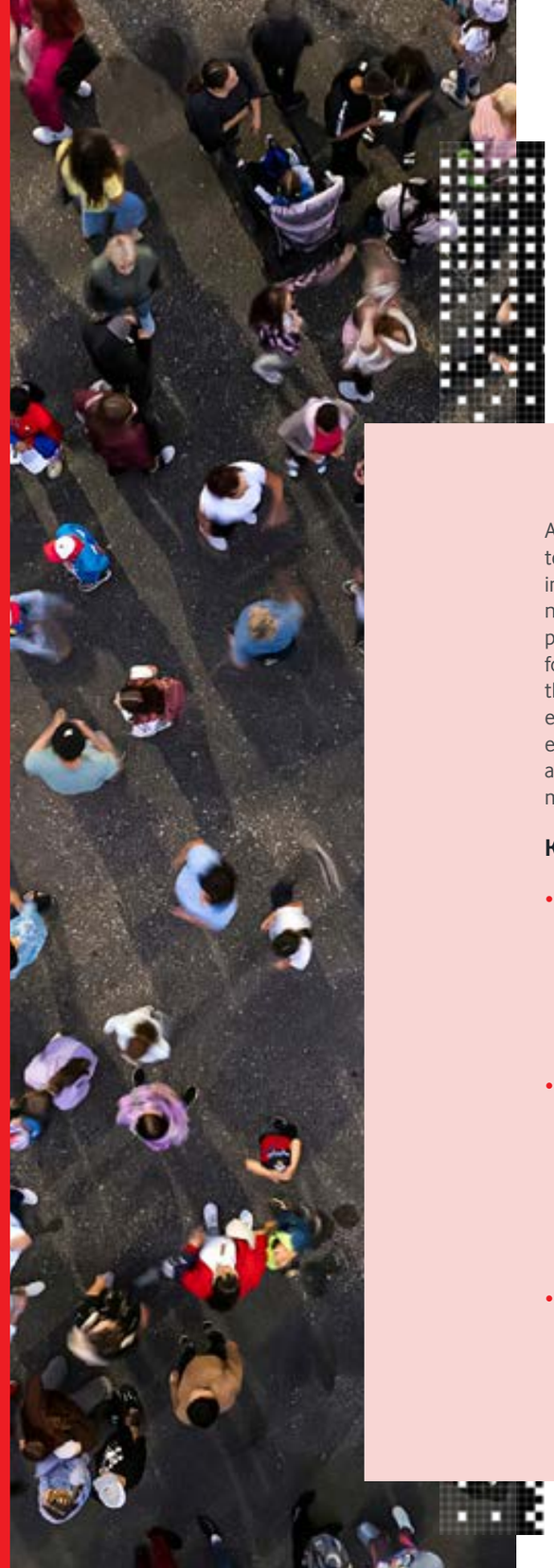
02

The building blocks of a new Digital Communications Act: Fairness, symmetry, harmonisation and proportionality

Assembly Research

Industry analysts Assembly Research provide independent custom and subscription-based information, analysis and opinion on regulatory, policy and legislative developments that affect communications markets and the wider digital economy.
For more information visit assemblyresearch.co.uk.

A unique opportunity to analyse the entire ecosystem, streamline rules for everyone while ensuring regulation applies only where it is appropriate, and drive harmonisation towards a true Digital Single Market.



Amid a mounting regulatory burden on both the telecoms and tech sectors, rather than further incremental changes to the rules, we consider that a new, singular Digital Communications Act (DCA) offers a potential third way for EU regulation. With a broader focus than solely the underlying network infrastructure, the DCA represents a unique opportunity to analyse the entire ecosystem, streamline rules for everyone while ensuring regulation applies only where it is appropriate, and drive harmonisation towards a true digital single market.

Key messages

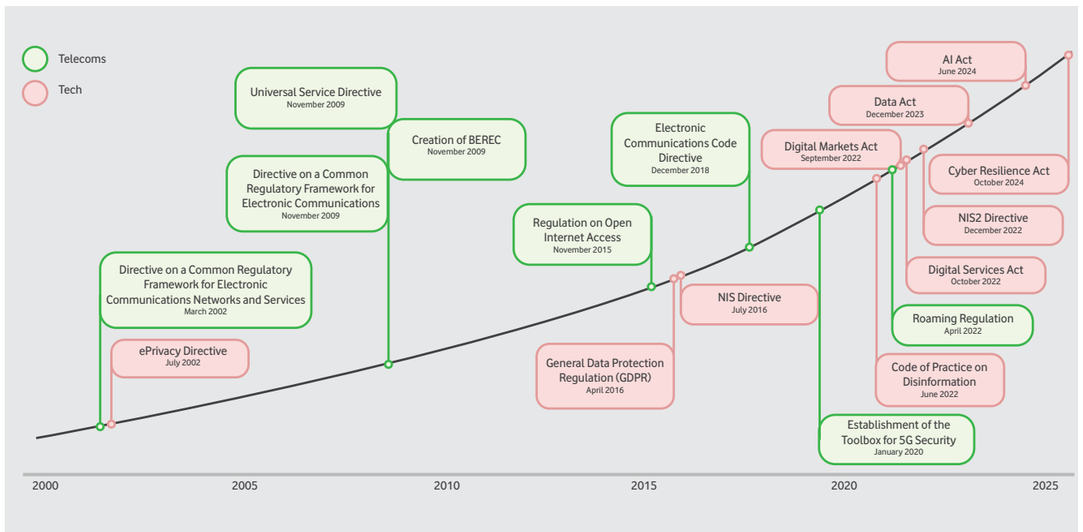
- Since the early 2000s, the EU has built up a portfolio of regulation that oversees the digital communications landscape. While the burden facing telecoms operators has largely increased incrementally, the tech sector has been hit by a wave of new legislation designed from the ground up.
- Amid an EU-wide push for economic growth, competitiveness and investment, there is now a need to course correct by rationalising the rulebook and tackling a series of unintended consequences that have been caused by the existing framework. An overarching DCA would offer the opportunity to start anew.
- This regulatory reset would require a different approach from the EC, establishing a comprehensive yet streamlined regime that would be underpinned by four core principles: fairness, symmetry, harmonisation and proportionality.

Two decades of an increasing regulatory burden

The last two decades have seen remarkable changes in communications markets and in terms of the players that compete within them. In parallel, there has been a revolution in services, technologies, consumers' patterns and levels of usage, and demands on networks, as well as shifts in the roles and responsibilities of regulators. During this period, the EU's regulatory framework for telecoms has helped open up competition in the sector and driven significant investment into telecoms infrastructure while promoting choice and low prices for consumers.

However, periodic reviews of the rules have only led to incremental changes to the regulation of Europe's telecoms sector, which have tended to expand and/or extend the requirements imposed on operators. As noted by Mario Draghi, in parallel to regulation at the EU level, there has also been a costly growth in obligations on the industry as Member States have introduced regulation unilaterally. In more recent years, there has been a proliferation of legislation affecting the broader digital economy. Beginning with the General Data Protection Regulation (GDPR) in 2016, the EU has set about tackling specific issues that have emerged across the online space, including harmful or illegal activities, or threats to competition in markets dominated by certain large platforms – see Figure 1.

Figure 1
Mapping the regulatory burden



The current regime must be re-evaluated to reduce imbalance, fragmentation and complexity

Today's diverse digital ecosystem is unrecognisable from the one on which the original telecoms framework was based. Even where regulation has been scaled back or modernised, typically to try to track changing market dynamics, many legacy obligations remain in place. As highlighted in Enrico Letta's report, this has created a clear regulatory imbalance between different providers of functionally similar services. Further, certain regulation has been agreed upon by EU institutions and introduced at the bloc level but applied and enforced in a fragmented manner nationally, thereby making harmonisation between Member States challenging, if not impossible. Well-intended initiatives such as the Broadband Cost Reduction Directive (BCRD) 2014 provide a case in point for the piecemeal approach operators have had to contend with.

In addition, several distinct pieces of legislation, including the Digital Services Act (DSA), Digital Markets Act (DMA) and AI Act, have been designed from scratch to address particular issues affecting the wider internet value chain. These ground-up initiatives indicate a relatively closer alignment between regulation and the market challenges in need of addressing, and take a more principles-based and proportionate approach to the problem than the range of regulation that exists in the telecoms sector. Nevertheless, these new instruments have still been implemented in a piecemeal way. Now, both tech firms and telecoms operators are impacted by the weight of, and apparent overlaps and complexities in, the application of digital sector rules.

Taken together, the full and fragmented suite of regulation is hampering industry's growth prospects and negatively impacting the region more broadly, in particular by stifling the realisation of a genuine digital single market. Such examples suggest that if the policy development process for the digital communications ecosystem was to begin afresh today, there should be a movement away from slow, ad hoc tweaks that fail each time to catch up sufficiently with market developments and from the drip feed of individual legislation drafted in silo.

A recast regulatory framework grounded in four principles

Rather than additional incremental reviews of Europe's telecoms regulatory framework or the introduction of further standalone laws, the creation of a new Digital Communications Act (DCA) may present a third way. This would require the EC to adopt a markedly different approach to the one that it has employed to date, but there is scope to establish a holistic regime that more accurately reflects – and can better keep pace with – the ongoing technological evolution. A modern, forward-looking framework established through the new act could be underpinned by the following four core principles.

1. Fairness

The principle of fairness means providing the platform for effective and sustainable competition among a variety of players within markets that are open and free from barriers to entry. While it is crucial to promote the long-term interests of consumers, the DCA would be balanced and alive to the needs of industry, ensuring firms are not handicapped but enabled to thrive, including in new markets or service areas

An example of fairness in practice

In telecoms, there has been a fixation on low prices (more so than price relative to usage or quality of service, for example) as a barometer of good regulation, while some operators' returns and other financial health metrics have declined considerably. Fairness would mean acknowledging this trend, prevailing market conditions and operators' valuable role in the economy, and supporting their efforts and capacity to invest, innovate and compete. Within a DCA, this principle could take the form of provisions requiring regulators to pay mind to the need for sustainable investment in the sector and the ability to earn a return on that (even drawing from the EC's Gigabit Recommendation), and to set out in their subsequent implementation of the rules how those provisions have been given due consideration. This would not mean compromising outcomes for consumers but would recognise that telecoms services are often undervalued and that promoting investment can yield positive outcomes for end users in terms of network coverage and performance, which may not necessarily correlate with an increase in prices.

2. Symmetry

This principle would champion greater parity over the current disequilibrium when it comes to providers of similar services, particularly where those appear equivalent from an end user perspective. The act would leverage the existing digital landscape as its starting point, while being mindful of how it could develop (and converge further) going forward.

An example of symmetry in practice

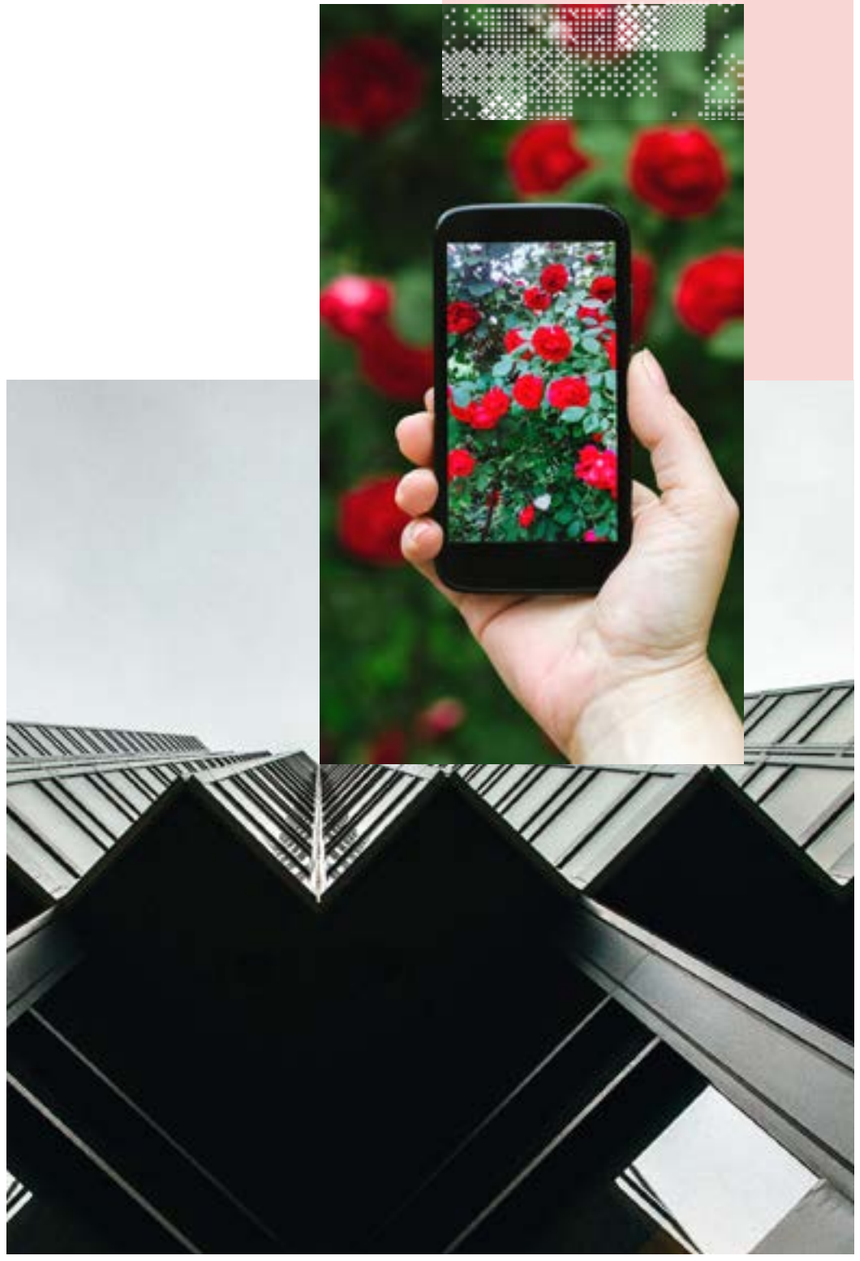
Here, symmetry would mean leaving behind the binary delineation between the telecoms and tech sectors in respect of near-identical communications services, with a view to delivering an appropriate levelling of the playing field. This move is not necessarily intended to add to the regulatory burden on tech firms, but instead to limit exemptions and asymmetries where reasonable to do so, and create an integrated, horizontal regime that offers certainty and predictability to all players. This principle could be reflected in a DCA by adjusting definitions currently used following transposition of the European Electronic Communications Code (EECC), which have resulted in telecoms operators being subject to a raft of sector-specific obligations. This would ensure the act encompasses all aspects of the ecosystem, rather than just focused on a collection of telecoms networks and services and regulating specifically for them.

3. Harmonisation

The principle of harmonisation means striving for greater consistency across borders, ensuring regulators move (at least somewhat) in lockstep in their oversight of the digital communications market. While the DCA would involve a degree of in-built flexibility to account for specific characteristics of national markets, this should not risk complexity. Simplification of, and uniformity in, the rules should be paramount.

An example of harmonisation in practice

Nuances in Member States' approach to regulation has resulted in different requirements for operators offering the same services in different countries. Harmonisation would involve addressing the scope for material divergence from the EU framework, reducing the risk of confusion and conflict, supporting the development for a scaled, pan-European market. This principle could be put into practice through the appropriate choice of legal instrument for a DCA – i.e. a regulation over directive – and stricter responses from the EC to any divergence from the framework at the national level. By following a harmonised approach, updated definitions of digital communications services (discussed above) would then be applied uniformly across Member States. As noted by Letta, the European AI Office implementing the AI Act and the network of Digital Services Coordinators for the DSA could also be a useful point of reference for how to put the DCA into effect, which could involve enhancing the role of BEREC (and its members) or establishing a new authority to act as the central coordinating agency.



4. Proportionality

This principle would involve developing an overarching regulatory framework for digital communications that at the same time does not over-reach. Proportionality means not maintaining outdated regulation designed to fit a bygone era, but taking into account major changes in the market and being aware of expected future realities.

An example of proportionality in practice

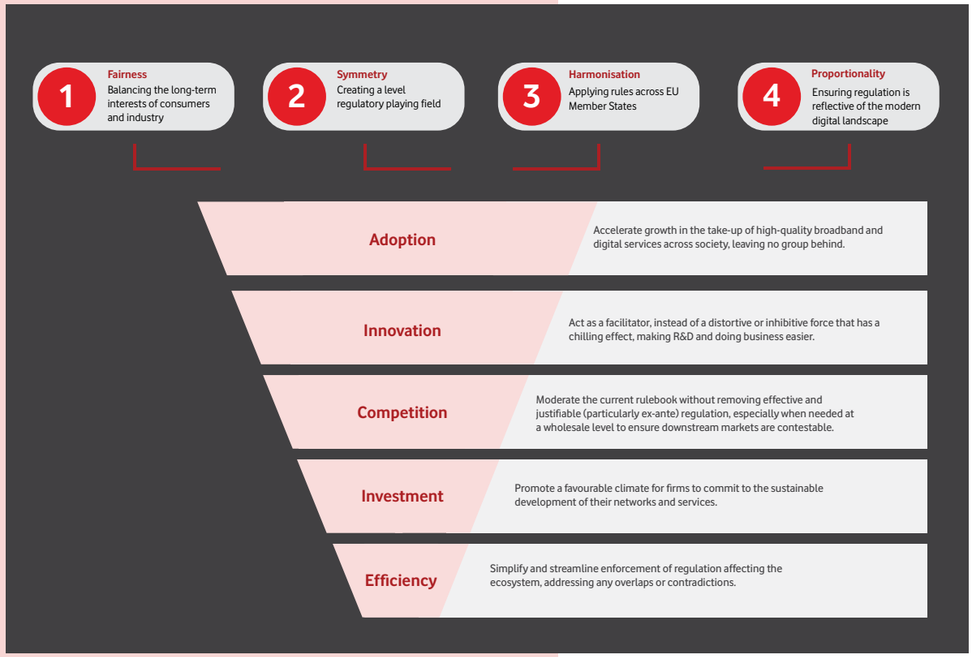
Rules such as the ePrivacy Directive and Open Internet Regulation were adopted many years ago and have been preserved in the EU despite the issues they were intended to fix no longer existing. Meanwhile, the negative outcomes foreseen for the US after the repeal of the Open Internet Order have never materialised. Recognising that both telecoms and tech firms are heavily regulated, proportionality would mean only regulating where it makes sense. While looking to develop a DCA, this principle could be brought to bear through a transition away from formal net neutrality rules to an industry code of practice, thereby more accurately accounting for market and technological developments, and facilitating opportunities for operator innovation in services that could be monetised and benefit end users, but might otherwise be considered incompatible with a free and open internet. Applying this principle, would also mean learning from the different approaches to net neutrality from key international comparators, including the UK where Ofcom has reviewed (somewhat) the rules to ensure the regulatory framework is up to date.

The principles would be geared towards the realisation of five key outcomes

These foundational principles should not sit in isolation but instead would be explicitly linked to five key outcomes the DCA would seek to achieve. Within the new framework, these outcomes should therefore provide guidance and be visibly accounted for as policymakers across the EU carry out their regulatory duties, including analysis within consultations and decisions on how they are being implemented (see Figure 2).

The outcomes of the DCA would therefore tie in with the EU's wider public policy objectives, principally boosting competitiveness, security and growth, as well as sectoral ambitions, including the targets outlined by the Digital Decade policy programme.

Figure 2



An Act that is overarching, pan-European, has legal backing and is enforced more robustly

An all-encompassing framework starting from scratch today would not look like the aggregation of regulations, directives and recommendations that have been issued successively to date, nor would it be specifically telecoms- or tech-focused in nature. There is room to learn lessons from the EC and regulators' experiences with laws such as the GDPR, the DMA and the AI Act, each of which has been developed and implemented for a specific real-world purpose. However, a new DCA would be both comprehensive and singular, reflecting the innate changes seen and felt by industry, helping to reconcile two prominent elements of the value chain that are often seen to be in opposition. Taking a more systematic and adaptable approach, the DCA would prioritise combining regulation and addressing overlaps and inconsistencies to streamline the regime, ensuring not to repeat mistakes witnessed in telecoms.

Effective enforcement of the DCA would be vital to delivering the regulatory reset the EU needs and supporting progress towards a true single market. To that end, introduction of the new act via a regulation that applies directly in Member States – rather than a directive – would be an important first step in the right direction. The latitude afforded to national regulators to date through the various legal instruments employed has led to a patchwork of rules and a disconnect between countries experiencing many of the same trends and transitions, facilitating disparate outcomes for consumers. This ultimately indicates that more rigorous EU-wide implementation is needed alongside improved coordination processes. Individual regulators would be responsible for complying with and uniformly applying the rules, with the scope for closer oversight from the EC and potentially greater consequences for deviation from the regime. While regulating from a more pan-European standpoint would trigger some pushback, developing a framework from the bottom up must prioritise reducing (if not eliminating) fragmentation around the bloc, while ensuring all players are appropriately captured to address perceived imbalances. Grounded in the principles and outcomes described above, this approach would help deliver a new DCA that is fit for purpose, offers clarity and coherence, and can act as a platform for investment, innovation and competition across the digital communications landscape.

03

Scaling Investment and Innovation: A passporting framework for EU telecommunication

ECIPE

Dr Matthias Bauer – Dr Matthias Bauer is a German economist and Director at the European Centre for International Political Economy (ECIPE). He works on EU and global trade policy with a focus on digital and technology policymaking.

Dyuti Pandya – Dyuti Pandya is an Analyst at the European Centre for International Political Economy (ECIPE), specialising in the intersection of law and technology, including both emerging and traditional technologies.

Boost investment, enhance competitiveness, and accelerate the deployment of critical digital infrastructure like 5G, 6G, and fibre.

Executive Summary

The Country of Origin (CoO) passporting model presents a major opportunity for the EU to modernise and scale its telecommunications sector. Building on the success of passporting in financial services, it could boost investment, enhance competitiveness, and accelerate the deployment of critical digital infrastructure like 5G, 6G, and fibre. By allowing telecommunications services providers to operate seamlessly across borders under a single national authorisation, the CoO model would reduce regulatory fragmentation, lower compliance costs, and create a more predictable business environment – key drivers for attracting long-term investments and fostering innovation.

The CoO passporting in telecommunications services could be strengthened by measures that enhance regulatory coherence and support market integration, such as baseline harmonisation of network security and spectrum management obligations, a role for a new EU digital regulatory authority in compliance and dispute resolution, and robust security frameworks for lawful interception, data retention, and cybersecurity to safeguard critical infrastructure. Looking ahead, the CoO model could serve as a stepping stone toward an EU-wide single rulebook for telecommunications, reducing legal fragmentation and positioning the EU as a global leader in digital connectivity and the diffusion of innovation.

1. Passporting: Concept and Origins

Passporting is a legal mechanism within the European Union (EU) that allows regulated businesses to operate across the EU and the European Economic Area (EEA) without needing separate authorisations in each member state. Once a company is authorised by a regulator in one EU/EEA country, it can "passport" that authorisation to offer its services throughout the Single Market, either through cross-border activities or by establishing branches in other countries. The concept is essentially built on two key principles: home-country control and mutual recognition. A regulated company only needs to notify its home state regulator of its intention to operate in other EU countries. The home regulator then informs the host state regulator, ensuring that the service provider remains primarily subject to the jurisdiction of its home country.

2. Passporting in EU Financial Services

Passporting in financial services stems from the EU's goal of a fully integrated Single Market, with the Single European Act of 1986 paving the way.[1] Key directives like the Second Banking Directive (1989), MiFID I & II (2004, 2014), and Solvency II (2009) established and expanded passporting for EU financial services, promoting regulatory coherence, competition, and market efficiency across the EU. The process typically involves:

1. Authorisation in the Home Country: A financial institution obtains a licence from its national regulator.

2. Notification Procedure: The firm notifies its home regulator of its intention to provide services or establish a branch in another member state.

3. Regulatory Communication: The home regulator informs the host country's regulator, after which the firm can begin operations.

While firms benefit from streamlined access, host states may retain certain supervisory powers, particularly concerning conduct of business rules, anti-money laundering (AML) obligations, and financial stability measures. This balance between access and regulatory primacy ensures that firms can operate seamlessly while key operational risks are effectively managed across borders.

3. Legal and Political Challenges of Passporting

The legal transition towards passporting initially faced considerable political resistance, particularly from Member States concerned about losing national competences. Countries like Germany and France feared losing control over their financial systems,[2] as passporting required them to rely on the regulatory decisions of other national authorities, potentially undermining their ability to enforce domestic rules and protect national interests.

Resistance to passporting also stemmed from broader concerns around regulatory divergence and market dynamics. Countries with stricter financial regulations and consumer protection groups worried about a "race to the bottom,"[3] where institutions might gravitate towards jurisdictions with more lenient oversight, risking financial stability. Smaller markets feared domination by larger financial hubs, particularly London,[4] which could outcompete local firms due to its scale and global reach. Additionally, differences in financial market models - such as the bank-centric systems[5] in Germany versus the capital market-driven model of the UK - raised concerns that harmonised rules could disproportionately benefit certain financial structures. Eurosceptic movements[6] further opposed the regime, viewing it as a step towards deeper EU integration and supranational control, challenging the balance between national autonomy and EU-wide regulatory cohesion.[7]

4. The Positive Impacts of Passporting in EU Financial Services

Despite these concerns, Passporting has become a cornerstone of financial integration in the EU, offering significant benefits by facilitating cross-border operations without the need for multiple national authorisations. This streamlined access has reduced administrative burdens and compliance costs for financial institutions, fostering greater competition, innovation, and efficiency across the Single Market. While passporting did not impose uniform rules, it indirectly encouraged regulatory harmonisation. Member States, aiming to prevent firms from exploiting divergent national compliance standards,[8] had strong incentives to align their regulations more closely. This convergence helped create a more consistent regulatory environment, reducing legal uncertainties for firms and enhancing consumer protection across the EU.

Furthermore, passporting played a crucial role in simplifying the EU's previously fragmented financial regulatory framework. Before its implementation, firms navigated a highly complex system of overlapping EU legislation, national laws, and administrative guidelines. Passporting helped dismantle these barriers, promoting a more economically integrated market.[9] However, recognising the legal uncertainty surrounding the general good exception and systemic risks from uneven supervision, the EU moved towards a single rulebook following the de Larosière Report.[10] For example, the general good exception, which allowed host countries to impose additional national rules for public interest reasons (e.g. consumer protection), created legal uncertainty and inconsistencies in the application of passporting rights. The shift the implementation of the report sought was to harmonise regulatory standards, curb regulatory arbitrage, and enhance financial stability, reinforcing fair competition and deeper integration across the EU. Rather than eliminating passporting, it strengthened and standardised it under binding EU regulations, replacing the fragmented national framework.

5. Application of Passporting in the EU Telecommunication Services Sector

Two distinct models could theoretically underpin a future telecom passporting framework in the EU:

1. **Centralised Authorisation with National Enforcement:** A model where a central EU body, e.g., an EU-level digital regulatory authority, incorporating NRA expertise, but led by independent experts, grants EU-wide authorisation (EU "passports"), while National Regulatory Authorities (NRAs) retain enforcement powers. This approach relies on a high degree of pre-harmonised rules across Member States.

2. **Application of the Country of Origin (CoO) Principle:** A model closer to the financial services passporting regime, where telecom providers operate across the EU based on authorisation from their home Member State. This relies on mutual recognition rather than full regulatory harmonisation.

While both centralised authorisation and the CoO principle are valid pathways for introducing a telecom passporting regime, the CoO model may offer the most immediate benefits. It balances the need for regulatory efficiency, market integration, and national sovereignty – factors that have proven critical in the successful development of passporting in the EU's financial sector.

Supported by complementary measures – such as minimum harmonisation in key areas, an enhanced role for a central digital regulatory authority, and minimum consumer protections (see below) – the CoO model can drive investments to achieve the EU's digital transformation goals.

5.1. Core Features of the Country of Origin (CoO) Passporting Model

The CoO model promotes flexibility, reduces administrative burdens, and accelerates cross-border service provision. Its core features include:

1. **Mutual Recognition of National Authorisations:** Once authorised in their home country, providers can deliver telecommunication services across the EU without seeking additional authorisations from host countries. This mirrors the financial services model, where institutions operate under the oversight of their home regulator.

2. **Regulatory Autonomy with Consistent Outcomes**: While Member States retain regulatory autonomy, they commit to mutual recognition of each other's rules, provided that minimum EU-wide standards are met, in line with the minimum requirements set out in the European Electronic Communications Code (EECC), or any new framework regulation created for the sector upon review of the existing rules.[11]

3. **Inclusion of Network-Independent Services:** The Country of Origin (CoO) model is particularly well-suited for network-independent services, which inherently operate across jurisdictions. These include regulated business-to-

business (B2B), Internet of Things (IoT), machine-to-machine (M2M), over-the-top (OTT), and wholesale services. While B2B services are more likely to be network-independent, consumer-facing services often rely on network-based infrastructures, making regulatory considerations more complex. Recognising this distinction ensures that CoO principles are applied where they best support cross-border efficiency and innovation.

4. **Inclusion of Consumer Services:** Expanding passporting to consumer services would enhance scalability, revenues, and investment. However, certain technical requirements remain inherently national, particularly those tied to physical infrastructure and assets (e.g. networks and numbering resources). Addressing these challenges would require regulatory and technical adjustments to ensure seamless cross-border operations. One key example is emergency call handling, where compliance with Article 109 of the EECC necessitates accurate call routing and caller location transmission. Potential solutions include an EU-wide public safety answering point (PSAP) routing database, standardised caller location transmission (e.g., Advanced Mobile Location (AML), Global Navigation Satellite System (GNSS)), interoperability with national emergency infrastructure, and automated language detection to support cross-border accessibility while maintaining public safety.

5.2. Complementary Components to Support the CoO Model

To maximise the effectiveness of the CoO model, several complementary components could enhance regulatory coherence and strengthen Europe's telecommunications market. The CoO framework not only facilitates cross-border scalability but also drives regulatory exchange and cooperation, fostering greater alignment across jurisdictions. Specifically, CoO can gradually drive harmonisation in these key complementary areas – similar to its impact in financial services – ensuring a more integrated, competitive, and well-coordinated European telecom landscape.

1. **Cross-Border Infrastructure Development and Network Access Framework:** To accelerate network deployment and promote fair competition, the CoO model should be supported by a simplified, harmonised framework for both infrastructure authorisation and network access. This includes streamlined rules for spectrum allocation, right-of-way access, and environmental clearances, alongside standardised procedures for obtaining permits with clear approval timelines. Additionally, ensuring non-discriminatory access to essential infrastructure – such as ducts, poles, and towers – and strengthening wholesale access rules will foster greater competition, innovation, and investment in high-capacity networks like 5G, fibre, and edge computing across the EU.

2. **Security and Compliance Frameworks:** A common framework for network security, including rules on lawful interception,[12] data retention,[13] and network security,[14] could ensure that the CoO model does not create regulatory loopholes that could undermine security.

3. **Enhanced Role for an EU- level digital regulatory authority:** While NRAs will retain primary enforcement responsibilities, an EU-level digital regulatory authority, incorporating NRA expertise, but led by independent experts, should play a more prominent role in monitoring compliance, facilitating cross-border cooperation, and ensuring supervisory convergence. Drawing parallels to the European Banking Authority in financial services, enhanced oversight by a central EU body would promote consistent regulatory practices and help resolve potential conflicts between national authorities.

4. **Dispute Resolution Mechanisms:** Effective dispute resolution processes are essential for the smooth functioning of the CoO model. Clear mechanisms should be in place to handle disagreements between telecom operators and National Regulatory Authorities (NRAs), particularly in cross-border contexts. A new central regulatory body could play a formal role in mediating disputes, ensuring that regulatory decisions are applied consistently and fairly throughout the EU, thus reducing legal uncertainty for operators.

6. Potential Impacts of the CoO Passporting Model for EU Telecommunication Services

The Country of Origin passporting model offers a major opportunity for the EU to modernise and scale its telecommunications sector. It provides a pragmatic, efficient way to boost cross-border services, attract investment, and speed up the deployment of critical digital infrastructure. Inspired by the success of passporting in financial services, the CoO model reduces compliance costs, enhances legal certainty, and supports the EU's goal of a fully integrated Digital Single Market.

At its core, the CoO model preserves regulatory autonomy for Member States while ensuring consistent outcomes through adherence to minimum EU-wide standards, as outlined in the EECC or any new framework regulation created for the sector upon review of the existing rules. The CoO model can facilitate cross-border infrastructure deployment, particularly for 5G corridors, fibre networks, and cloud services. By improving investment conditions, profitability, and market access, the model enhances scalability for efficient operators. These operators often benefit from stronger procurement leverage, further lowering costs. A passporting framework would enable telecom and network providers to achieve greater economies of scale and accelerate cost-effective infrastructure deployment.

Looking ahead, the CoO model could serve as a stepping stone toward an EU-wide single rulebook for telecommunications, echoing the evolution seen in the financial services sector. This progression would establish a unified legal framework, reduce regulatory fragmentation, and provide greater legal certainty for operators.

Ultimately, the CoO passporting model is more than just a regulatory tool – it can be a strategic driver of Europe's digital future, enhancing the EU's global competitiveness and supporting its leadership in the next generation of connectivity and digital innovation.

Footnotes

1. ECMI (2020). The EU equivalence regime in financial services: an effective instrument to preserve financial stability after Brexit? Available at https://www.ecmi.eu/publications/policy-briefs/eu-equivalence-regime-financial-services-effective-instrument-preserve. The legal history of the European banking union (1973-2018): how European law drove the integration of the single financial market from its expansion and crisis to the banking union. Available at https://cadmus.eui.eu/handle/1814/65305?show=full;EPRS (2017). Understanding equivalence and the single passport in financial services: Third-country access to the single market. Available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2017)599267.

2. McHugh, F. (1996, March 27). Barriers hold up progress towards single market in financial services. Politico. Available at: https://www.politico.eu/article/barriers-hold-up-progress-towards-single-market-in-financial-services.

3. Hertig, G. (1994). Imperfect mutual recognition for EC financial services. International Review of Law and Economics, 14(2), 177-186.

4. Cassis, Y. (2010). Capitals of capital: the rise and fall of international financial centres 1780-2009. Cambridge University Press.

5. Deeg, R. (2011). Financialisation and models of capitalism: A comparison of the UK and Germany. In Capitalist diversity and diversity within capitalism (pp. 121-149). Routledge.

6. The Turner Review limited the single passport by advocating for branches and subsidiaries to maintain independent liquidity (ring-fencing of liquidity). It called for the suspension of the home country principle, allowing host supervisors to directly intervene in branches, and exerted pressure for branches to be converted into subsidiaries. See: Turner, A. (2009). The Turner Review: a regulatory response to the global banking crisis', Financial Services Authority, at 11-49, referenced from EUI (2019).

7. See, e.g., De Larosière Group (2009). The High-Level Group on Financial Supervision in the EU Report. European Commission. Available at https://ec.europa.eu/economy_finance/publications/pages/publication14527_en.pdf. Posner and Veron (2010). The EU and financial regulation: power without purpose? Available at https://www.tandfonline.com/doi/abs/10.1080/13501761003661950. The EU equivalence regime in financial services: an effective instrument to preserve financial stability after Brexit? Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3567959; EPRS (2017). Understanding equivalence and the single passport in financial services: Third-country access to the single market. Available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2017)599267.

8. Lomnicka, E. (2000). The Home Country Control Principle. European Business Law Review, 11(5).

9. EUI (2019). The legal history of the European banking union (1973-2018): how European law drove the integration of the single financial market from its expansion and crisis to the banking union. Available at https://cadmus.eui.eu/handle/1814/65305?show=full.

10. The de Larosière Report (2009) strengthened the foundation of passporting in financial services by advocating for harmonised supervision and regulatory coherence across the EU. While it did not directly propose changes to passporting, its recommendations – such as the creation of the European Supervisory Authorities (ESAs) – helped ensure consistent oversight of cross-border firms, reducing regulatory arbitrage and enhancing financial stability. These reforms reinforced passporting by improving coordination between home and host country regulators. De Larosière Group (2009). The High-Level Group on Financial Supervision in the EU Report. European Commission. Available at https://ec.europa.eu/economy_finance/publications/pages/publication14527_en.pdf.

11. CERRE (2024). The Future of European Telecommunications: In-depth Analysis. Available at https://cerre.eu/wp-content/uploads/2024/09/CERRE_The-Future-of-European-Telecommunications-In-depth-Analysis_FINAL.pdf.

12. The EECC acknowledges national competence, with very high discretion for Member States as national security remains sovereign, enforced by national law enforcement agencies.

13. The EECC provides no direct regulation post-CJEU rulings. Member States have high discretion, though constrained by EU fundamental rights, enforced by telecom regulators and data protection authorities.

14. The EECC sets minimum security standards (Article 40). Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Member States have moderate discretion to impose stricter national rules, enforced by national regulatory authorities (NRAs) and cybersecurity agencies, supported by EU-level coordination (e.g., ENISA).

04

Towards a European system of digital regulators. Strengthening regulatory cooperation, deepening the single market

Alexandre de Streel: Professor of EU Law at the University of Namur, Visiting Professor College of Europe (Bruges) and SciencesPo Paris; Academic Director at CERRE

A significant opportunity to align the enforcement mechanisms for electronic communications rules with the broader EU digital framework, ultimately streamlining the institutional setup.

The previous European legislature (2019-2024) adopted a comprehensive set of laws to regulate the European digital ecosystem, each with its own enforcement regime, leading to a fragmented institutional framework.[1] The current Commission (2024-2029) has committed to streamlining the EU's digital rulebook and proposing a new Digital Networks Act.[2] Both initiatives present a significant opportunity to align the enforcement mechanisms for electronic communications rules with the broader EU digital framework, ultimately streamlining the institutional setup.

1. The current enforcement regimes of the EU digital rulebook

The EU digital rulebook relies on three main models of enforcement.[3]

The first model is decentralised enforcement based on the 'countries of destination.' In this model, which is the default approach in international law, the regulated company is supervised by the regulator of the Member State where it provides its services. If the company operates in multiple countries, it will be supervised by multiple regulators. This model is used for the regulation of electronic communications networks and services,[4] as well as for network security,[5] consumer protection[6] or competition law.[7] The downside of this model is that, by involving multiple regulators, it can lead to inconsistent enforcement across Member States and increase compliance costs for pan-European companies. To mitigate these risks, coordination networks between national regulators have been established, such as the Body of European Regulators for Electronic Communications (BEREC)[8] or the Consumer Protection Cooperation (CPC) Network.[9]

The second model is decentralised enforcement based on the 'country of origin'. In this model, the regulated company is supervised only by the regulator of the Member State where it is established, but it can provide its services across the entire EU. This model is used for the regulation of digital services,[10] media services[11] or also privacy law.[12] The advantage of this model is that it provides a one-stop regulatory shop and facilitates scaling up across the internal market. The downside, however, is that it only works if there is mutual trust among Member States and if the regulator in the country of origin has both the ability and the incentive to apply EU law effectively for the benefit of all EU citizens. Without this, it may lead to a race to the (regulatory) bottom.

To strengthen these abilities and incentives, networks of national regulators have been established, such as the European Board for Media Services (EBMS)[13] and the European Data Protection Board (EDPB).

The third model is centralised enforcement by an EU institution. In this model, the regulated company is directly supervised by the European Commission or another EU body. This model is used for the regulation of some digital services provided by large tech platforms,[14] as well as partly for regulating AI-based products[15] and competition law.[16] The advantage of this model is similar to the previous one (a one-stop shop), but it comes with fewer downsides, as an EU regulator has more ability and incentive to regulate for the benefit of the entire EU. While the country of origin model under decentralised enforcement has played a crucial role over the last 30 years in integrating national markets and facilitating scale-up in Europe, EU-level enforcement may represent the next step in European integration, particularly when large companies that have already scaled up are regulated at the EU level.

2. The need for change

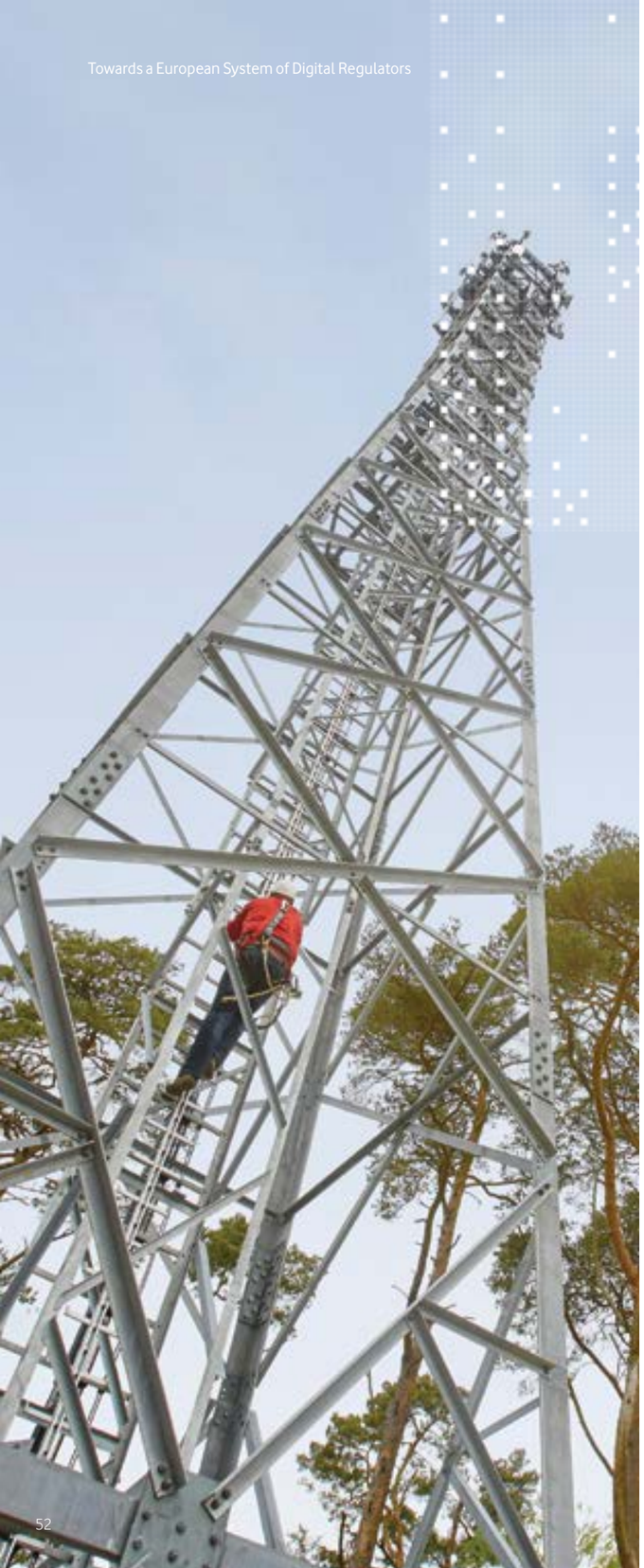
While the enforcement regimes of the various laws in the digital rulebook were developed largely independently, there is now a pressing need to streamline them along three key dimensions to ensure consistent enforcement across the European digital ecosystem: greater regulatory coordination and cooperation, a more integrated internal market, and increased independence.

2.1. Need for more regulatory cooperation

For the effective implementation of the digital rulebook, coordination among the various (national and EU) regulators should be significantly strengthened. This coordination occurs on two levels: first, within the same legal instrument across Member States (for example, coordination among the 27 national telecommunications regulators), and second, across different legal instruments within the digital rulebook (for example, coordination between telecommunications regulators and data protection agencies).

The first type of coordination is organised through the regulatory networks mentioned earlier. However, these networks have different institutional structures and dynamics, and may not yet ensure optimal coordination.[17] For instance, BEREC sometimes fails to achieve true harmonisation in the interpretation and enforcement of the European Electronic Communications Code, often settling for the lowest common denominator among national regulators. Additionally, when BEREC comments on a draft decision by a national regulator, there is a risk of a conflict of interest, as national regulators are also members of BEREC.

The second type of coordination is underdeveloped, both at the national and, even more so, at the EU level.[18] At the national level, some networks of regulators overseeing the digital value chain have begun to emerge, for example, in the Netherlands,[19] France, and Germany. These networks contribute to a shared understanding of



digital ecosystems and foster consistent policy approaches and decisions among different regulators.

At the EU level, the DMA High-Level Group, which consists of five regulatory networks (BEREC, ECN, CPC, EMBS, and EDPB), is the emerging platform for cooperation.[20] However, the functioning of the high-level group is impeded by a lack of transparency and stakeholder involvement.[21] More fundamentally, the scope of this high-level group is limited because, on the one hand, it only deals with policy issue at the general level and cannot handle specific regulatory cases and, on the other hand, it only addresses the DMA and not the other laws in the digital rulebook.

Ideally, a systemic structure should be established that, on one hand, enables and incentivises cross-country and cross-regulatory regime coordination, and on the other hand, ensures hierarchical relationships that allow for the rapid adoption of final decisions in the best interest of the EU as a whole, rather than merely serving the interests of individual Member States.

2.2. Need for more internal market and EU enforcement

The Letta and Draghi Reports recommend strengthening the digital single market to regain European competitiveness and strategic autonomy. This calls for more EU harmonisation of the rules or even the establishment of a '28th' fully harmonised European legal regime that firms could choose to adopt.[22] This also calls for greater harmonisation in the enforcement of the rules. However, the level of centralisation should be assessed given that, as noted by BEREC[23] not every regulatory decision should be centralised at the EU level, and national regulators should continue to play a key role in enforcing the digital rulebook when the benefits of centralisation are outweighed by the costs.[24]

The benefits of EU-level enforcement include: (i) the internalisation of regulatory externalities across Member States, which is particularly important for communications and digital services traded across borders;[25] (ii) cost savings for regulated firms due to the elimination of regulatory duplication (one-stop-shop); (iii) economies of scale and reduced transaction costs for regulators in implementing regulations; and (iv) increased commitment and coherence, as EU authorities tend to be more independent and less susceptible to capture by national firms and governments.

However, EU enforcement also comes with certain costs, including: (i) higher information asymmetry at the EU level compared to the national level; (ii) the loss of the ability for regulatory experimentation and innovation to identify—and potentially converge towards—the most efficient form of regulation,[26] along with, in some cases, lower responsiveness and flexibility at the EU level compared to national procedures; and (iii) the heterogeneity of preferences across Member States, which may not be adequately reflected in a single EU policy.

2.3. Need for more independence

According to the principles of good regulation, regulators should have sufficient powers and resources and be independent not only from the firms they regulate, but also from political influence.[27] While EU law guarantees this dual independence for national regulators, it does not extend the same guarantee to the European Commission.

According to the EU Treaties, the Commission is independent from national governments, but not from the European Parliament.[28] This distinction could become a concern as the Commission takes on a more prominent geopolitical role, particularly as international relations increasingly shift from being based on law to being driven by power dynamics.

Thus, the old debate on the independence of DG Competition and the need to establish a separate EU antitrust agency[29] may come back with a vengeance as the Commission, including other areas of the Commission, takes on more regulatory responsibilities for enforcing the digital rulebook while also becoming more geopolitically engaged. The explicit intrusion of industrial policy goals across a broad range of subject-matter over the past few years has arguably created the perception that the Commission risks prioritising policy choices based on considerations that have less to do with the effectiveness of regulation and more to do with responding to geo-political considerations.

3. Towards a European System of Digital Regulators

One way to streamline the enforcement framework across these three dimensions would be to establish a European System of Digital Regulators, with a two-tier structure:

- An EU tier: the creation of a new EU body, the European Digital Agency (EDA), which would replace and result from a radical transformation of BEREC;
- A national tier: the National Digital Regulators, which could naturally evolve from the telecommunications regulators established under the EECC and the digital services coordinators set up under the DSA.

A possible source of inspiration for this new system could be the Single Supervisory Mechanism (SSM), under which significant banks in the Eurozone are supervised by the European Central Bank (ECB) in close cooperation with national financial supervisors through the establishment of Joint Supervision Teams.[30]

3.1. The division of enforcement powers between the EU and the national level

At the EU level, the establishment of an EU digital regulator has been proposed in the Letta Report of 2024 and was already recommended in the Bangemann Report back in 1994. The Bangemann Report suggested that an EU regulator should deal with 'the regulation of those operations which, because of their Community-wide nature, need to be addressed at the European level, such as licensing, network interconnection when and where necessary, management of scare shared resources (e.g. radio-frequency allocation, subscriber numbering) and advice to Member States' regulatory authority on general issues'.[31]

The Letta Report suggests that an EU regulator should deal with 'the coherence of rules in the Single Market including the rules on net neutrality and roaming and be directly responsible for cross-border services, such as core network services, business networks, and ground and submarine cables connecting more than one country'. [32] The exact and optimum scope of enforcement powers for any new EDA will depend on the substantive rules established in the upcoming Digital Networks Act and, more broadly, in the digital rulebook; but it should be determined by weighing the costs and benefits of EU enforcement outlined above.

In the medium term, with the reform of electronic communications regulation, the EDA could assume direct enforcement powers currently held by the Commission and the existing BEREC structure under the EECC, such as the veto and comments on NRA decisions on market analysis.

Additionally, depending on the final outcomes of the Digital Networks Act, the EDA could gain further powers. One option, inspired by the system of financial supervision, would be to entrust the EDA with regulating significant and pan-EU telecommunications operators, particularly concerning market entry (e.g., authorisation and spectrum assignment) and network access (e.g., identifying bottlenecks to be regulated and implementing EU-wide access remedies). This option could be effectively complemented by the establishment of a '28th' fully harmonised legal regime, mentioned above. In the longer term, the EDA could take over the direct enforcement powers currently exercised by the Commission under all the laws of the digital rulebook (such as the DMA and DSA), as well as the enforcement powers of the various regulatory networks established under the EU digital rulebook.

At the national level, the reformed national digital regulators would retain important roles. On the one hand, the heads of national regulators would participate in key aspects of decision-making carried out by the EDA. On the other hand, national regulators may keep direct enforcement powers in specific cases and they would monitor compliance of the EDA decisions by regulated firms in their respective Member States, handle complaints, and resolve disputes. Additionally, national digital regulators could play a crucial role in merger control, particularly in monitoring behavioural remedies that may be imposed as conditions for merger clearance.[33] This role may become even more significant if, as suggested in the Draghi Report, investment remedies are favoured over merger prohibitions.[34]

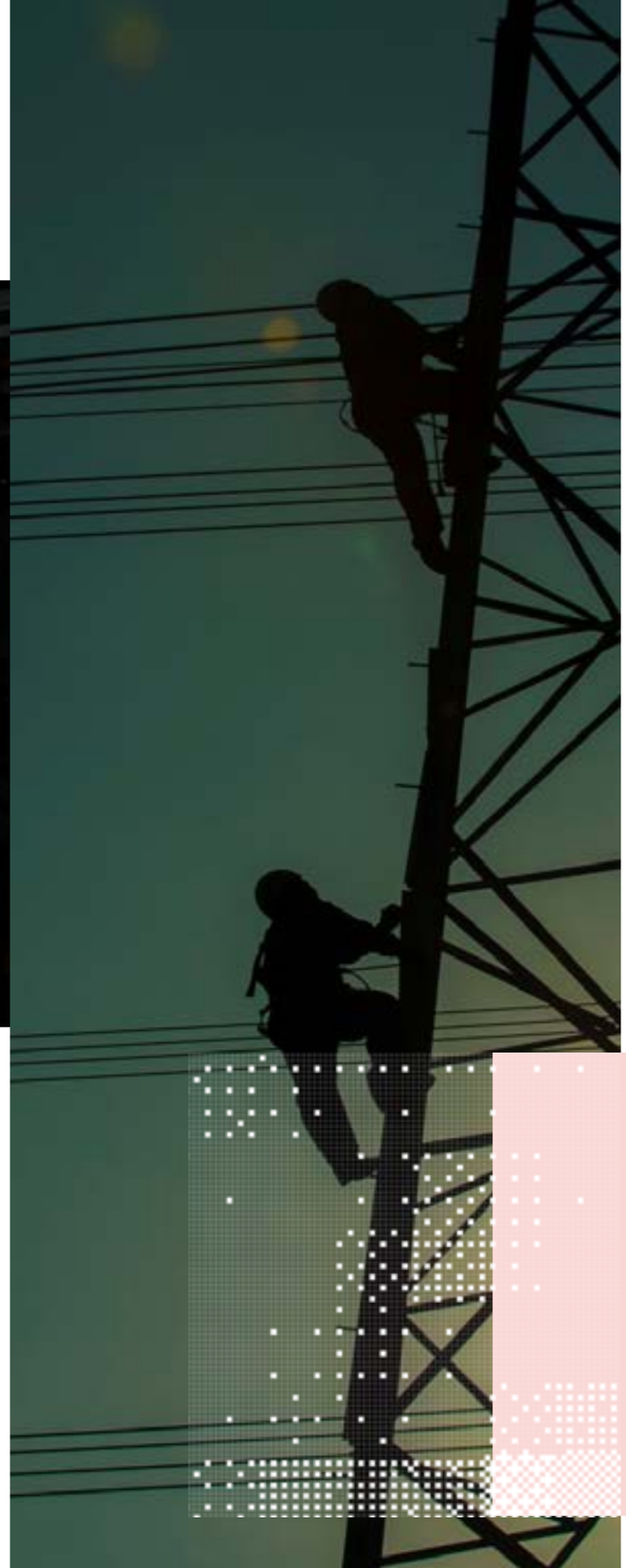
3.2. Institutional structure and legal possibilities

To build on existing institutions rather than starting from scratch, BEREC could be radically transformed into a fully-fledged EU agency and become the EDA. Its structure and governance could draw inspiration from that of the European Central Bank, featuring a small executive board with extensive powers and a management board.[35] The executive board would consist of full-time members appointed by, but independent from, the Member States, with confirmation by the European Parliament. The management board would be made up of the heads of national digital regulators, who would act in their personal capacity, independently of their national authorities. Given the need for "participatory regulation", a stakeholders' committee should also be established with balanced representation from all stakeholders in the EU digital ecosystem, including regulated firms, their competitors, business and end users.

Ideally, the EDA would meet the requirements that EU law generally imposes on national regulators, namely independence, accountability, and transparency. Its decisions would be subject to a Board of Appeal, and those decisions could, in turn, be appealed before the Court of Justice of the EU. The EDA would require the allocation of sufficient human and financial resources, as well as the power to collect information and impose effective sanctions.

The establishment of the EDA is legally possible without changing the EU Treaties, as current case law is more supportive of creating such agencies than when the EU project began in the 1950s, particularly following the Meroni case.[36] In the ESMA Short Selling judgment, the Court of Justice

of the EU confirmed that, based on Article 114 TFEU, the legislature could 'deem it necessary to provide for the establishment of an EU body responsible for contributing to the implementation of a process of harmonisation,[37] especially when specific professional and technical expertise is required. The Court did then set limits: the agency should not make policy decisions, and its rulings should be subject to judicial review. In a more recent judgment concerning the powers of the German energy regulator BNetzA, the Court further clarified the Meroni doctrine and implicitly endorsed the creation of EU agencies with extensive executive powers.[38]



4. Conclusion

The European Commission's 2024-2029 agenda presents a pivotal opportunity to streamline the enforcement mechanisms of the EU's digital rulebook, addressing inconsistencies in the current decentralised enforcement models. The proposed European Digital Agency would enhance regulatory coordination across the digital ecosystem, internal market integration, and independence. This new framework aims to resolve challenges associated with fragmented enforcement, ensuring more cohesive and efficient regulation for cross-border services. By transforming BEREC into the EDA and streamlining the role of national regulators, the EU can foster a more unified and effective regulatory approach to telecommunications and digital infrastructures and services, paving the way for greater EU competitiveness.

Footnotes

1. P. Alexiadis, T. Shortall, A. Guerrero and N. Nikolinakos, Coherence vs Fragmentation - Institutional Challenges to EU Digital Market Regulation" Vol. 24 No.3, September 2023, Business Law International 24(3), 2023, 233-286.

2. See mission letter EVP Virkunnen

3. On those three models, see G. Monti and A. de Streel, Improving institutional design to better supervise digital platforms, CERRE Report, 2022.

4. Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ [2018] L 321/36, hereinafter EECC.

5. Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation 910/2014 and Directive 2018/1972, and repealing Directive 2016/1148 (NIS 2 Directive), OJ [2022] L 333/80.

6. Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ [2005] L 149/22, as amended by Directive 2019/2161; Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ [2011] L 304/64, as amended by Directive 2019/2161.

7. Directive 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, O.J. [2019] L 11/3.

8. Regulation 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of the European Regulators for Electronic Communications, OJ [2018] L 321/1.

9. Regulation 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation 2006/2004, OJ [2017] L 345/1.

10. Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ [2000] L 178/1.

11. Directive 2010/13 of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services (Audiovisual Media Services Directive), OJ [2010] L 95/1, as amended by Directive 2018/1808.

12. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ [2016] L 199/1.

13. Regulation 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13 (European Media Freedom Act), Arts. 8-13.

14. Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), OJ [2022] L 265/1 and Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31, OJ [2022] L 277/1.

15. Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations 300/2008, 167/2013, 168/2013, 2018/858, 2018/1139 and 2019/2144 and Directives 2014/90, 2016/797 and2020/1828 (Artificial Intelligence Act).

16. Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, O.J. [2003] L 1/1, as amended.
17. As already recognised during the previous review of the electronic communications regulatory framework: WIK Consult, Deloitte and IDATE, Regulatory - in particular access - regimes for network investment models in Europe, Study for the European Commission, 2016.

18. The cooperation between the three European Financial Supervision Authorities (European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA)), formalised through the establishment of joint committees, may serve as good practice.

19. https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt

20. https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3904. Previously, the Digital Clearing House, an informal cooperation platforms established at the instigation of the European Data Protection Supervisors, also aims to achieve this cross country and cross regime coordination: https://www.edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en

21. A. de Streel, R. Feasey and G. Monti, DMA@1: Looking Back and Ahead, CERRE report, March 2025.

Footnotes

22. This 28th regime will be proposed by the Commission for start-ups to simplify applicable rules and reduce the cost of failure, including any relevant aspects of corporate law, insolvency, labour and tax law: Communication from the Commission of 29 January 2025, A Competitiveness Compass for the EU, COM(2025)30.

23. BEREC High-Level input on the Commission's White Paper on "How to master Europe's digital infrastructure needs?", BoR (24) 100_2, pp.10-11.

24. A. Alesina, I Angeloni, and L. Schuknecht, 'What does the European Union do?, 123 Public Choice, 2005, 275-319; W. Oates, 'Towards a Second-generation Theory of Fiscal Federalism', 12 International Tax and Public Finance, 2005, 349. Specially for digital markets, see A. de Streel and Ph. Defraigne, Where Should the European Union Intervene to Foster the Internal Market for eCom, Communications & Stratégies 2011, 82, 63-84

25. There is such externality when the regulation (or the absence of regulation) in country A has significant effect on the welfare of the consumers and/or firms in country B and that effect will not be taken into account by the regulator of country A.

26. For a successful example of regulatory experimentation and convergence in broadband regulation, see T. Shortall and M. Cave, Is Symmetric Access Regulation a Policy Choice? Evidence from the Deployment of NGA in Europe, Digiworld Economic Journal 98 (2), 2015, 17-41.

27. R. Baldwin, M. Cave M. and M. Lodge, Understanding Regulation: Theory, Strategy, and Practice, 2nd ed., Oxford University Press, 2012; C. Decker, Modern Economic Regulation: An Introduction to Theory and Practice, 2nd ed, Cambridge University Press, 2023; K. Yeung and S. Ranchordas, An Introduction to Law and Regulation: Text and Materials, 2nd ed, 2024, Cambridge University Press.

28. Article 17 TEU. Incidentally, the previous Justice Commissioner Reynders has acknowledged the potential for a lack of independence of the Commission when he noted that: "... based on Article 8 of the Charter, the enforcer of data protection rules must be ensured by an independent authority. Therefore, the Commission could not have enforcing powers as it has in the DMA as DSA": Speech on "The Future of Data Protection: Effective enforcement in the Digital World", 16 June 2022.

29. C-D. Ehlermann, 'Reflections on a European Cartel Office', Common Market Law Review 32(2), 1995, 471-486.

30. Council Regulation 1024/2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions OJ [2013] L287/63. The SSM illustrates the advantages of centralisation which ensure a level playing field across the Eurozone as well as a holistic and effective regulatory assessment. It also illustrates the many challenges of centralisation. As the system is still in transition, there remain national differences in supervision culture that should be eroded as joint supervisory teams continue to work together. Moreover, sufficient transparency of SSM operation should be ensured to preserve the accountability of the system of supervision

31. Bangemann group, Recommendations of the high-level group on the information society to the Corfu European Council, p.17.

32. E. Letta, Much more than a market: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens, Report to the Council, p. 56.

33. There is administrative precedent for this sort of remedy 'outsourcing' exercise to occur in practice, but its use has been ad hoc and dependent upon the express or implicit conferral of competence to engage in such actions: A classic example is the Decision of the Commission of 2 April 2003 in the Newscorp/Telepiu Case (M.2876), a duopoly-to-monopoly merger between Italy's two satellite pay-TV platforms. In that case, the Commission had effectively outsourced the monitoring of the effectiveness of access remedies to the Italian Media Regulator.

34. M. Draghi, The Future of European Competitiveness, Report to the Commission, Part B, p.299.

35. Art. 129 TFEU and Protocol 4 on the Statutes of the European System of Central Banks and the European Central Banks.

36. Case 9/56 Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community, EU:C:1958:7.

37. Case C-270/12, UK v Parliament and Council (ESMA Short Selling) EU:C:2014:18, para 104.

38. Case C-718/18, Commission v Germany, EU:C:2021:662, paras.131 which summarises the Meroni case-law as follows: 'it is not permissible to delegate to administrative bodies a margin of discretion which may, according to the use which is made of it, make it possible to take political decisions in the true sense, by substituting the choices of the delegator by those of the delegatee, and thus bring about an 'actual transfer of responsibility'. However, a delegation of clearly defined executive powers, the exercise of which can, therefore, be subject to strict review in the light of objective criteria determined by the delegating authority, is permitted'.

05

The future of Open Internet Regulation and net neutrality

Professor Antonio Manganelli, PhD, Professor of competition law and policy, School of Economics and Management, University of Siena.

Dr. Wolfgang Briglauer, Senior Researcher, Research Institute for Regulatory Economics, Vienna University of Economics and Business.

“EU-style NN rules may be restricting ISPs ability to innovate, develop new services and manage their networks, leading to poor consumer outcomes and at the same time creating regulatory market asymmetries vis a vis big tech.”

The net neutrality debate, active for about two decades, has seen recent policy revisions in the EU and UK and diverging approaches in the US.

In the following, we first summarize the most relevant regulatory as well as market and technological developments. This is followed by our assessment of the effectiveness and efficiency of net neutrality regulation. Finally, we provide some policy considerations.

Relevant regulatory developments in the EU, UK & US

EU

Since 2015, the EU has maintained strict net neutrality (NN) rules – referred to as Open Internet Regulation (OIR)[1]. The aim of the Regulation is preventing Internet service providers (ISPs) from exploiting their perceived “gatekeeper” position in local access markets to discriminate against unaffiliated content and application service providers (CAPs). It does so by establishing rules requiring ISPs to carry all Internet traffic without (i) discrimination, (ii) blocking, and (iii) throttling, or prioritization.

The interpretation and application of the rules by national regulatory authorities is supported by the Body of European Regulators for Electronic Communications (BEREC) which issued guidelines for the first time in 2016, revised them in 2020, and again in 2022. These guidelines are not legally binding.

However, the European Court of Justice (ECJ) issued a decision on zero rating in the year 2021, which went against long standing mobile price practices and BEREC’s existing guidance and prohibited most forms of zero-rating[2], including those supporting public-good services like health and education, because those have been considered a form of illicit commercial discrimination. BEREC’s 2022 guidance implemented the ECJ’s 2021 judgments. This shift not only disrupted long-standing practices but also required costly changes by mobile operators.

For 5G technologies, BEREC supports a case-by-case approval process, potentially stifling innovation due to the “innovation by permission” approach.

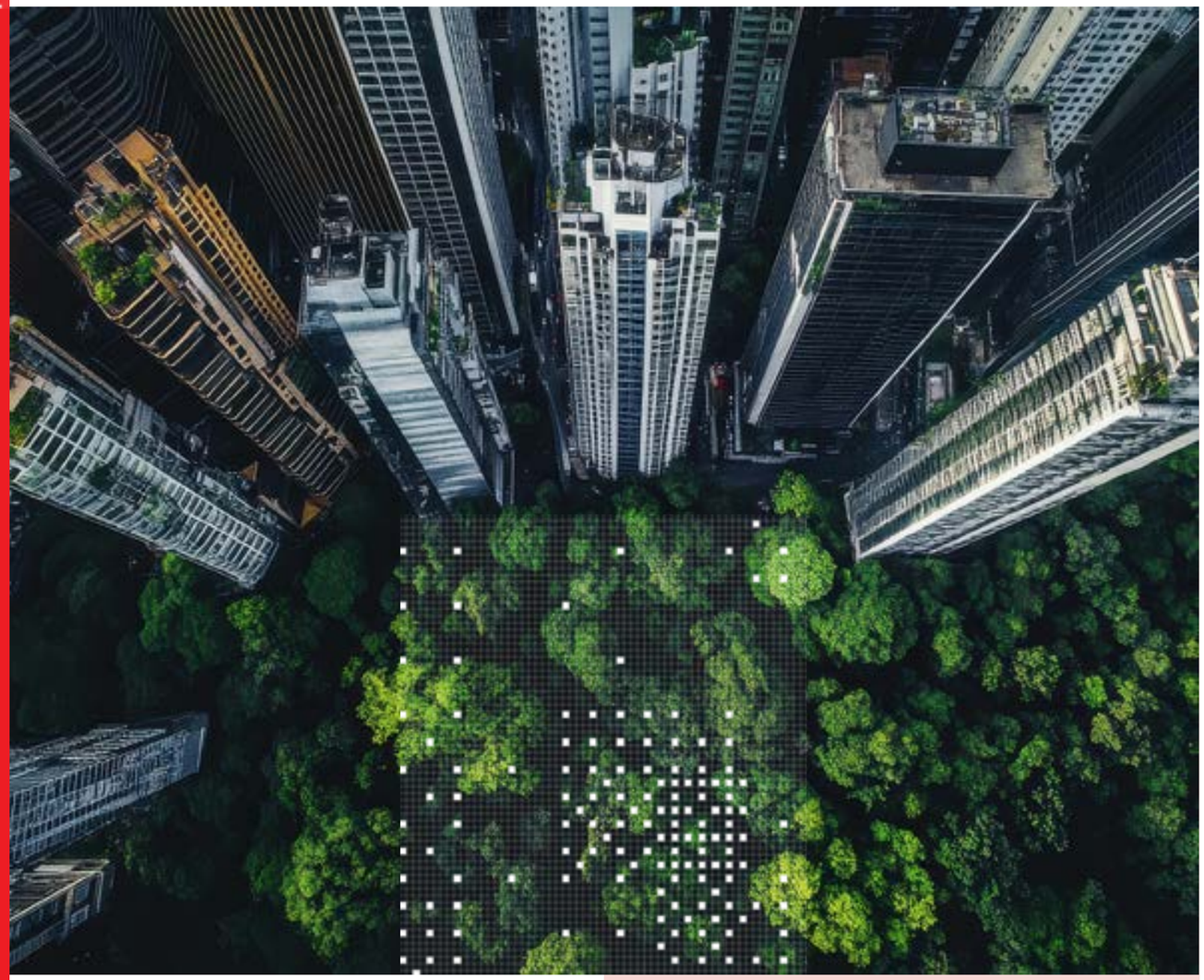
UK

In other jurisdictions, NN rules have been subject to debate and/or revisions to consider the relevant economic trade-offs involved. In the UK, as soon as it was no longer subject to EU legislation, in 2023, Ofcom revised its NN guidelines[3], introducing a more flexible framework.[4] This pragmatic shift marks a departure from strict prescriptive EU-style rules, favoring a more principles-based approach.

US
As for the US, the Federal Communications Commission (FCC) reinstated rules from its 2015 Open Internet Order (that had been withdrawn in 2018)[5]; however, in early January 2025, an US appeals court ruled that the FCC does not have legal authority to introduce net neutrality rules, which de facto means the end of US NN regulation under the Trump presidency.

To summarise, at the basis of Ofcom's review and US's flip-flopping approach stands the fact that the EU-style NN rules, which existed in those markets, may be restricting ISPs ability to innovate, develop new services and manage their networks, leading to poor consumer outcomes and at the same time creating regulatory market asymmetries vis a vis big Tech CAPs.

Furthermore, current NN rules focus only on one specific side of the digital ecosystem, by imposing strict rules to ISPs, while disregarding strong market positions developed by other parties throughout the internet value chain and the existing interdependences among all actors. For example, it is not clear why the core principles of non-discrimination and transparency are relevant only to ISPs; or only in a one-directional manner in the ISP to CAP relationship.



Relevant market and technological developments undercutting OIR assumptions

Significant technological and market changes in the last few years transformed the digital ecosystem and namely the market positions of the largest CAPs both in terms of countervailing power and their ability to influence end-users' internet experience, while NN rules assume that only ISPs have those powers and capabilities.

Market power and competition

As clearly acknowledged by the introduction of the DMA, digital markets and services are highly concentrated, and few large CAPs (i.e., very large online platforms / gate-keepers) have significant and entrenched market power. Moreover, they often provide end-users with "must-have" contents and applications, on one side of the market, and are essential gateways for business-users to reach them, on the other side of the market.

In contrast, in most circumstances (fixed or mobile) ISPs receive strong competitive constraints from other ISPs. Indeed, competition between ISPs for end-users has strongly developed in the telecom sector, not least due to decades of pro-competitive EU access regulation.[6] Consequently, any activity by ISPs blocking or degrading the quality of must-have contents/applications to their subscribers, and even of other contents/applications, would be 'sanctioned' by (empowered) end-users by switching to another ISP.[7]

The combination of these two elements implies that, on one side, ISPs would have no clear economic incentives to manage traffic and deteriorate the end-users' experience and restrict their choice; while, on the other side, an asymmetric negotiation and bargaining power between ISPs and the largest CAPs may have arisen.

Technology evolution

Some technological developments are drastically changing the assumptions underlying the current NN rules in the EU that solely ISPs can affect internet traffic flows and consequently end-users' internet experience. Indeed, there is growing significance to what other players can do in the extended value chain. This is not trivial, particularly considering that most of those players are those very large online platforms/gatekeepers that are considered CAPs under the EU open internet regulation.

In this regard, a big open question originating from the technological development in mobile 5G communications concerns whether other subjects than mobile network operators, e.g., operating system (OS) providers (i.e., mainly Google Android and Apple iOS), could somehow control the different slices of the network.[8] Given the concentration of the consumer market for device OS[9], there is a risk that major OS providers can impose de facto standardisation to the slicing identification mechanism and that as an effect, operators may lose part of the control over which traffic corresponds to each slice, whilst giving the OS control.

In the same fashion, increasingly popular content delivery networks (CDNs)[10] enable to some extent service differentiation by managing traffic via private networks and ensure content is hosted as close to the end-user as possible to guarantee certain quality levels.[11] From a user experience perspective, these and other mechanisms can act as 'technological substitutes' for network management by ISPs, ensuring higher quality of experience perceived by the end-user.[12] This can be seen under an economic perspective as a form of 'paid prioritization' although traffic is not prioritized in the network layer, and thus it is not subject to OIR.[13]

Effectiveness & efficiency assessments of OIR

Effectiveness

These market and technological changes highlight clearly that, on one side, the OIR non-discrimination objectives are not pursued effectively, and, on the other side, that negative pitfalls are affecting the ability of ISPs and users to make the best of technological developments.

Important technological developments, such as the ongoing roll-out of 5G networks, different types of private networks, and CDNs, imply that the actual scope of NN rules, and therefore their effectiveness, is constantly narrowing.[14] In addition, market distortions arise because of wide policy differences between countries and jurisdictions and because regulatory ambiguities embedded in NN rules promote bypass strategies.

Progressive deployments of 5G networks have been bringing increased opportunities to provide different services and innovations strictly interlinked with applications and use-cases that differ significantly in their network requirements. Indeed, 5G mobile broadband is mostly about differentiation of quality of service (QoS) and quality of experience (QoE), especially looking at "network slicing".

In principle, this contrasts with the 'best-effort' and 'equal treatment' approach underlying the NN concept. It is also not supported by an interpretation of OIR that imposes a strong restriction on regulated entities in view of a maximum probability of effectiveness ("precautionary principle"). This current approach inevitably leads to the risk of increased costs for the regulated company, inefficiencies in the market and social costs.[15] Moreover, this kind of regulation is a common feature of a more monopolistic market, as it is aimed to strictly protect end-users who have no alternative market choices but to be subject to a degradation of quality by the only one provider. Yet this approach clearly disregards decades of liberalisation and pro-competitive regulation in the electronic communications market.

Moreover, thinking "out of the (regulatory) box", it is clear that the OIR concepts have been a factor in the disintermediation by digital platforms of telco functionalities. For example, digital platforms such as search engines or social networks, can, *mutatis mutandis*, prioritise contents that pay for a "fast lane", i.e., sponsored contents or (almost) freely moderate contents.[16] Whereas, OIR prohibits to ISPs any commercial discrimination of traffic, even if the end-users ask for it.[17]

Efficiency

Finally, there are efficiency considerations related to investment incentives. Strict NN regulation stands in the way of telecom industry to fully deploy new technologies capabilities, consequently risking inhibiting network expansion and private investment and ultimately negatively affecting the competitiveness of the sector. This is openly contrasting with the recent Commission's white paper[18], which emphasizes that advanced, secure and sustainable digital network infrastructure forms the backbone of a thriving digital economy and society. To achieve this policy objective, the Draghi report[19] suggests, among other things to:

> **"Reduce country-level *ex ante* regulation, which disincentivizes investments and risk-taking, and favour rather ex post competition enforcement in cases of abuse of dominant position or other anticompetitive conducts."**

Coherently, the Letta report[20] specifically calls EU institutions for "a more comprehensive meaningful review of the Open Internet rules... with aim to maintaining the internet open and the user full freedom of choice but at the same time allowing to fully reap the benefits of the upcoming new network technologies". This policy focus on deregulation and incentivising private investment in digital infrastructure is also supported by empirical evidence which points to the negative investment effects of NN regulations on local access ISPs.[21]

Given the proven positive externalities of high-quality broadband networks, any limitations on their deployment will also reduce welfare in the long run.[22]

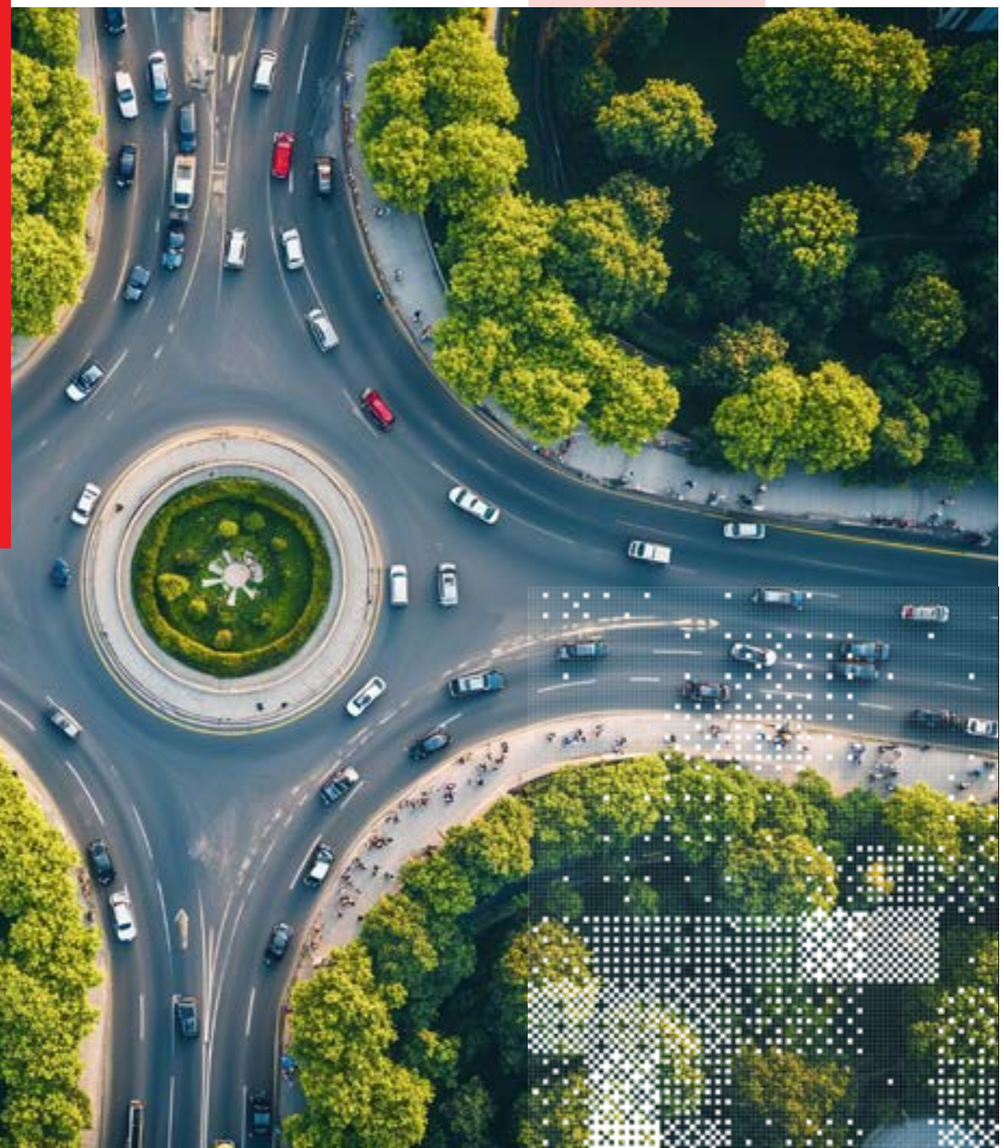
Conversely, so far, there is no empirical evidence supporting the positive effects claimed by NN proponents. Moreover, as historical developments in the EU and the US have shown, NN decisions lead to high costs in terms of implementation, monitoring and enforcement of NN rules, as well as potential market distortions, including market uncertainty due to compliance grey areas and lengthy case-by-case decisions; in addition, EU Open Internet regulation is still interpreted and applied differently across member states, creating fragmentation and hampering the creation of an EU single market and further market distortions.

Taken together with findings from empirical literature, benefits of NN regulation are uncertain if they exist at all, while costs are high. This leads to the conclusion that strict EU-style NN regulation is likely to be inefficient, implying negative welfare effects, even more so when considering the overall regulatory costs. This is an important finding as the burden of proof should be on the side of strong interventionist *ex ante* regulation. The overall regulatory cost of NN, counsel against imposing NN in the absence of evidence demonstrating benefits that could justify incurring those costs.

Conclusions and policy considerations

Current EU-style net neutrality regulation encounters a significant trade-off: either it allows broad exemptions for reasonable traffic management or specialized services, particularly for emerging technologies like 5G, which would render the regulation largely ineffective, or it enforces these exemptions in a highly restrictive and time-consuming case-by-case manner. The latter approach would severely hinder investment and innovation, particularly given the ongoing deployment of 5G and the emergence of future technologies like 6G. This creates particular concern for (European) ISPs, who might otherwise focus on developing and delivering innovative services but instead face uncertainty and compliance challenges within this regulatory framework.

There are, however, alternative approaches that could be adopted.



First-best

In terms of both efficiency and effectiveness, the “first best” policy recommendation based on economic analysis would therefore be to remove obvious over-regulation that impedes investment, such as NN rules, unless proponents can provide strong evidence of ultimate welfare-enhancing effects. Deregulation should not only reduce costs, but also increase network investment by ISPs, in line with EU policy objectives and the related policy initiatives and papers, such as the Draghi and Letta’ reports, and ultimately also resolve the above-mentioned trade-off.

Nevertheless, a balanced assessment must not overlook some of the core objectives of NN rules, i.e., maintaining an open internet and protecting consumer freedom of choice for contents, services, and applications that are not unjustifiably blocked or degraded.[23] So, the main point is to aim for rules which allow to achieve these objectives, by minimising the distortive impact on economic and market dynamics. In other words, NN rules should move away from its “precautionary principle” and embrace a general principle of the EU law: the “proportionality principle”.[24]

Second-best

Under this light, the “second best” policy recommendation based on economic analysis, yet considering the wider public interest objectives, is to provide broadband Internet access services (ISPs/BIAS) more flexibility either in terms of more options for pricing and quality design, subject to established ex-post competition law, combined with the possibility of sanctions in cases of abusive discrimination as well as existing sectoral transparency and end-user protections.

Moreover, a second-best option would need to embrace a systemic perspective, and thus reframe the existing asymmetric approach vis à vis the different actors in the digital ecosystem. This again would imply a softening of the existing over-prescriptive rules on ISPs, to principle-based rules, creating a level playing field across the extended digital ecosystem. This could be designed in different ways, inter alia, by allowing more flexibility and freedom for quality differentiation, as for premium quality services, as well as for zero-rating offers, both as ‘class-based offers’ and ‘content-specific retail offers’, yet only when it is the end-user choosing for such a differentiation (for example by introducing an application-agnostic ‘anchor product’ with a minimum QoS and which all users may choose).

This consumer-empowering approach to NN could strike an effective balance, guaranteeing a freedom of choice, without over-restricting the economic and commercial freedom of companies.

Footnotes

1. Regulation (EU) 2015/2120 laying down measures concerning open internet access.

2. Zero-rating are practices where an ISP does not subtract data usage associated with specific content or a class of content from a customer's data allowance.

3. Ofcom Statement on Net Neutrality Review 2023.

4. Key updates included: (i) eliminating prior approval for new services; (ii) allowing differentiated Internet access tiers; and (iii) permitting zero-rating under certain conditions.

5. The 2014 FCC's Open Internet Order reclassified Broadband Internet Access Services (BIAS) as telecommunications services and Broadband Internet Access providers as "common carrier", thus reintroducing the 2015 EU-style NN regulation, by prohibiting: (i) blocking or throttling lawful content; (ii) paid prioritization; and (iii) practices that unreasonably interfere with user access.

6. Currently access regulations are defined in Art. 69 – 74 EECC.

7. Cave M, Vogelsang I (2015) Net Neutrality: An E.U./U.S. Comparison. Competition Policy International, 11(1), 85–95. Of course, for tackling any possible anticompetitive coordination in this respect there are ex-post competition law instruments in place.

8. BEREC (2024) Report on the entry of large content and application providers into the markets for electronic communications networks and services - BoR (24) 139.

9. As stated in BEREC (2022) Report on the Internet Ecosystem - BoR (22) 167, the mobile OS market in Europe is mainly split between Android (63.6% market share by 2022) and iOS (35.7%).

10. A CDN is a network optimised for the distribution of digital content, which therefore increase the performance of the internet (access) network. In the last few years, the largest CAPs have been investing heavily in their own CDN infrastructure (in-house CDN).

11. See Stocker, V., Smaragdakis, G., Lehr, W.H. & Bauer, S. (2017). The Growing Complexity of Content Delivery Networks: Challenges and Implications for the Internet Ecosystem. Telecommunications Policy, 41(10), 1003-1016. However, on-net CDNs allow to reduce cooperatively capacity costs for ISPs by locating content closer to end-users.

12. See Briglauer W (2024) Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector: Relevant Developments and State of the Empirical Literature, available at https://www.wu.ac.at/fileadmin/wu/d/ri/regulation/Reporte_Studien/Briglauer_NN_paper_final_2024.pdf.

13. Garrett, T., Setenareski, L. E., Peres, L. M., Bona, L. C. E. & Duarte, E. P. (2022). A survey of network neutrality regulations worldwide. Computer Law & Security Review, 44.

14. Briglauer W & Yoo C (2025). Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector: Relevant Developments and State of the Empirical Literature, available at: https://www.wu.ac.at/fileadmin/wu/d/ri/regulation/WPs_und_GAs/Briglauer_Yoo_February_2025.pdf.

15. See, Kramer J, Peitz M (2018) A fresh look at zero-rating, Telecommunications Policy, Volume 42, Issue 7, 501-513; Briglauer W (2024.), op. cit.

16. The newly adopted EU regulation (Digital Markets Act and Digital Services Act) focus on transparency and users' awareness, whereas paid prioritisation and moderation are not excluded, as considered essential part of platforms' business models.

17. It is true that digital platforms are not considered network infrastructures, yet these differences are progressively blurring and need to be assessed against economics effects: on one side, they are using extensively private network infrastructures, and on the other side, traditional infrastructure networks have undergone a path of extensive network functions virtualization.

18. European Commission (2024) White Paper on "How to master EU's digital infrastructure needs", available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14168-White-Paper-How-to-master-Europes-digital-infrastructure-needs?_en

19. Draghi, M. (2024). The future of European competitiveness - Part B "In-depth analysis and recommendations", p. 75

20. Letta, E. (2024) Much More than a Market, p. 59, available at: https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

21. For a recent tabular overview of empirical studies see Briglauer & Yoo (2025), op.cit., p. 20.

22. For a recent and comprehensive survey of the relevant empirical literature see Briglauer, W., Krämer, J. & Palan, N. (2024). Socioeconomic benefits of high-speed broadband availability and service adoption: A survey. Telecommunications Policy 48(7), 102808.

23. EU Parliament, Council and Commission (2023) European Declaration on Digital Rights and Principles for the Digital Decade.

24. See Manganelli, A., (2024) Toward a Ne(x)t Neutrality: a re-thinking of the EU Open Internet Regulation, in MediaLaws, 2024, 3.

06

Addressing fragmentation to create a common EU framework for a true Digital Single Market: a case study of the cybersecurity sector

Arnault Barichella, PhD
Researcher, Twin Climate and Digital Transitions, CEARC – University Paris-Saclay
Associate Researcher, Cybersecurity and Artificial Intelligence – Jacques Delors Institute

“fragmentation in the area of cybersecurity remains a serious challenge for the European Union… there is now a pressing impetus to leap forward in this area with deeper forms of integration”

As the digital revolution has swept across the EU, analogue and mechanical systems have been progressively replaced with digital and computer software. This is partly linked to the effects of globalized competition between companies around the world, which has generated strong incentives for Europe to hasten digitization.[1] This has impacted all vital infrastructure, including transportation, healthcare, communications, the water and food supply, energy, banking and finance, along with governmental entities, the police and the military. The digital revolution has enhanced efficiency in terms of rationalizing the entire supply chain, stimulating the economy by boosting growth, job creation and revenues for businesses.

Despite these benefits, however, the digital revolution is a double-edged sword, leading to considerable new risks in the realm of cybersecurity.[2] Due to the level of interconnection between different sectors, a cyberattack in one sector may rapidly spread to contaminate others with a threat of systemic collapse, potentially bringing society to an abrupt halt. Increasingly sophisticated cyberattacks have risen significantly during the past decade, impacting both private sector firms and public entities alike. Each year, Member States across the EU are targeted by tens, if not hundreds of thousands of cyberattacks, with governmental entities or businesses now confronted with cyber risks on a daily level.[3] For these reasons, the topic of cybersecurity has become a high priority for the EU, with a number of new policy and legislative initiatives being introduced over the last few years.

Overview of the EU's policy and legislative landscape in the field of cybersecurity

EU policies and legislation in the field of cybersecurity find their origins in the 'Programme for Critical Infrastructure Protection' of 2006, along with the Critical Infrastructure Directive of 2008. From the very beginning, however, EU initiatives in this field were limited to establishing loose and general recommendations for Member States. Over the last decade, legislation has become more developed, with the Directive on the Security of Network and Information Systems (NIS) of 2016 creating shared EU standards on cybersecurity in relation to so-called 'operators of essential service', encompassing an array of different types of entities deemed as vital for the effective functioning of European countries.[4] Likewise, processes for the implementation of the NIS Directive were consolidated in 2019 with the EU's Cybersecurity Act, which sought to establish a common market for cybersecurity via the creation of a certification framework covering a broad range of digital services and commodities.[5]

As a follow-up, a proposal for a second and enhanced NIS Directive was set out by the Commission in 2021, with the objective of addressing supply chain security issues, bolstering cyber obligations for private and public entities, strengthening mechanisms for enforcement and supervision, as well as upgrading requirements in terms of cyber incident reporting. NIS2 was adopted in October 2024, expanding the scope of the initial NIS1 Directive by integrating new sectors, which now parallel those sectors dealt with by EU standards for the safety of physical infrastructure. These include: digital infrastructure in general, health, transport, drinking and waste water, energy,[6] finance, banking, as well as outer space, amongst others.

Moreover, it is also worth noting two additional EU legislative initiatives in the area of cybersecurity, recently passed in 2024. Firstly, the Cyber Solidarity Act seeks to enhance the EU's ability to prepare for, detect and react to cyberattacks by creating a European Cybersecurity Alert System composed of operation centres across Member States, along with a new Cybersecurity Emergency Mechanism. Likewise, the Cyber Resilience Act aims to reinforce cybersecurity norms for hardware and software products which incorporate a digital part, making it obligatory for retailers or manufacturers to include cybersecurity-by-design across product lifecycles.

For these reasons, the EU has established itself as an important actor in the realm of cybersecurity over the last decade, with a number of policies and legislative initiatives covering a broad range of different facets in connection to this highly strategic sector.[7] Nevertheless, despite notable progress, the EU's current framework on cybersecurity continues to suffer from a number of inadequacies, failing to fully resolve limitations which go back to the EU's initial policies in this field.

Identification of the main weaknesses in the EU's current legislative framework on cybersecurity

One of the main weaknesses with the EU's current legislative and policy framework in the realm of cybersecurity is that Member States are still afforded an important degree of autonomy in the process of enacting European rules. For example, both the first and second NIS Directives require individual Member States to establish a cybersecurity strategy at the national level. While it is correct that a Cybersecurity Strategy for the EU as a whole was first developed in 2013 and subsequently updated in 2020, this document is purely suggestive in nature, setting out policy recommendations on a general level, while letting countries develop their own detailed national rules. Another salient example is the mode of operation of the EU's Agency for Cybersecurity (formerly known as ENISA).

On the one hand, the Cybersecurity Act of 2019 provided the Agency with more budgetary resources, a permanent mandate, together with additional instruments to support Member States in dealing with cyber threats. On the other hand, the Agency's powers are still very limited, since the bulk of its tasks involve advising countries, collecting and sharing data or information, and fostering collaborative initiatives between Member States. Therefore, and in spite of the latest EU initiatives in this field, the Agency for Cybersecurity continues to lack binding legal tools to ensure effective implementation of EU norms and enhance harmonization across Member States.[8] Furthermore, such a configuration can also be discerned in both NIS Directives, which mandate countries to establish their own 'Computer Security and Incident Response Teams' (CSIRT). Member State CSIRTs are brought together in a European CSIRT network, which works alongside a so-called 'Cooperation Group' encompassing national cybersecurity institutions and the EU Commission.

As with the Agency for Cybersecurity, however, these networks do not possess any binding coercive authority to ensure compliance with European rules and norms in this field. Instead, this is left up to national cyber agencies, which continue to have broad leeway in deciding the degree of competences they want to attribute to their own CSIRTs. Unsurprisingly, this situation has led to the rise of significant divergences across Member States regarding the degree of potency and efficiency for CSIRTs throughout the EU.[9]

The main reason for this state of affairs is that security and defence, including cybersecurity, remain a national prerogative; these competences have not been transferred to the EU. As a result, EU institutions can only act in ways that support and encourage collaboration amongst Member States, but without intruding on national sovereignty. With the rise of Euroscepticism across the Union, national governments are disinclined to delegate further powers to Brussels, especially in such a sensitive field as defence.

Consequently, European countries remain reluctant to disclose confidential information with other Member States, which represents a significant impediment to the creation of a harmonized, common EU framework on cybersecurity, resulting in fragmentation across the continent.

The result is a multispeed Europe, with stark differences between countries in terms of their level of development in the realm of cybersecurity. The broad leeway provided to Member States in the enactment of EU standards has allowed some countries to put in place ambitious cybersecurity frameworks at the national level, whilst others have not. Sizeable Member States like France or Germany, which have at their disposal important financial tools, the requisite IT expertise and extensive infrastructure, have been able to develop world-class national structures for cybersecurity which go beyond EU rules.

For example, France launched its own national cybersecurity agency in 2009 (Agence nationale de la sécurité des systèmes d'information – ANSSI), which has risen to become one of the most rigorous institutions of its kind in the world, with far-reaching competences.[10] The latter are established by strict national standards for cybersecurity, which derive from a 'Military Programming Law' passed in 2013. The law was subsequently updated in 2018, with the latest version passed in July 2023 for a six-year timeframe from 2024-30.

In the field of cybersecurity, the Military Programming Law sets out detailed and obligatory rules for over 200 so-called "operators of vital importance". Likewise, France is one of the only countries in the world to have adopted over the last decade a series of "sectorial decrees", containing in-depth regulations that are customized to the specific features and requirements of particular sectors like nuclear power, electricity, gas, etc.[11]

On the other end of the spectrum however, there are a number of EU Member States which, due to insufficient resources, requisite technical expertise or infrastructure, have not been able to establish sufficiently robust cybersecurity frameworks at the national level. These countries are located mostly in the east or south of the EU (Slovakia, Bulgaria or Greece, for example), which experienced delays in introducing their own national CSIRT and cybersecurity strategies. Other Member States like Croatia, Latvia and Portugal have been slow to enact suitable cybersecurity norms for their critical infrastructure.[12] The end result has been the emergence of a multispeed Europe for cybersecurity, with significant differences in the degree of national cyber protection from one Member State to the other.

This is of course not an isolated situation. Policy domains like monetary policy and the Euro, or border controls involving the Schengen area, have likewise evolved into multispeed paradigms with only some Member States taking part in these initiatives, but not all. However, a multispeed Europe in the realm of cybersecurity is arguably more of a threat than in other policy sectors. Member States in the EU are strongly interconnected due to the legal, economic and technological framework associated with the Single Market. As a result, European countries with inadequate cybersecurity frameworks at the national level are 'weak links', representing vulnerable entry points for malware that may penetrate computer systems and subsequently propagate to other Member States, with the risk of eventually contaminating the whole EU network.[13]

Such a scenario has in fact materialized a number of times, with a series of devastating cyberattacks impacting the EU over the past decade. Prominent examples include the WannaCry virus of 2017, which started out infecting just a few vulnerable Member States, before rapidly spreading to affect practically the entire European computer

system, with the vast majority of EU countries incurring at least some degree of damage from this global cyberattack.[14] Hackers relied on data encryption to ask for the payment of ransoms, which impacted a variety of different sectors ranging from the French automobile manufacturer Renault, Germany's federal railway, the UK's National Health System, Spanish and Portuguese energy or telecom companies, along with Italian academic institutions and laboratories. While determining the exact origin of these types of cyberattacks is always challenging,[15] North Korea has emerged as a prime suspect, with the WannaCry virus costing the EU billions of euros in damages.

However, it should be noted that Russia and the Kremlin's secret services, either directly or indirectly, have been responsible for the majority of cyberattacks that have affected the EU during the last few years.[16] In many ways, especially since the annexation of Crimea in 2014, Moscow has been waging a cyberwar not only against Ukraine, but also against NATO and the EU more generally. Several of the most devastating cyberattacks in history have been launched by Russia against Ukraine, before propagating to neighbouring Member States in Eastern Europe due to inadequate cybersecurity frameworks at the national level, eventually propagating to other Member States and infecting large parts of the EU's computer network.

For instance, the NotPetya malware targeted Ukrainian critical infrastructure in 2017 and affected in total around a third of all computer systems in the country causing massive damage (worth around $10 billion), before spreading to neighbouring EU Member States in eastern Europe which lacked adequate cyber defences.[17] Likewise, in the years leading up to the invasion of Ukraine in 2022, Russia launched significant cyberattacks to disrupt the country.

Throughout the invasion, the Kremlin has engaged in a form of 'hybrid warfare' combining conventional military strikes with cyberattacks against Ukrainian infrastructure, including military and governmental facilities, along with the energy and banking sectors.[18] Once again, propagation to neighbouring Member States like Romania, Hungary or Slovakia has not been uncommon, with many cyberattacks also directly targeting these countries as well as other potential 'weak links' in the EU network.

Policy recommendations

These examples of devastating cyberattacks demonstrate that fragmentation in the area of cybersecurity remains a serious challenge for the European Union. While the EU's latest legislation in the field of cybersecurity (discussed in Part 1) represents an improvement, it clearly does not go far enough to tackle the risk of 'weak links'. For example, although the NIS2 Directive has led to more harmonization in terms of sanctions between countries, Member State authorities are still responsible for developing their own specific rules on cybersecurity at the national level.

Hence, the paradigm of a multispeed Europe and of highly variable cybersecurity standards across the EU continues up to this day, with potentially serious consequences in light of the ongoing War in Ukraine. In response, the last section of this paper will provide policy recommendations to help address fragmentation in the cybersecurity sector, with the goal of contributing towards the creation a true EU Digital Single Market. These policy recommendations will be divided into short term proposals which can be enacted immediately under the EU's current institutional framework, and then medium to long-term policy recommendations, some of which might entail changes in the EU's mode of operation.

Based on current legal mechanisms over the **short term**, it is possible for the EU to go further by enacting new pieces of legislation to reinforce cybersecurity in Europe. For instance and as previously explained, since NIS2 does not go far enough in tackling the issue of weak links, it would be useful for the Commission to consider the possibility of a draft proposal for a third NIS initiative to fill certain gaps with the existing legislation. While it is true that the Commission indicated that the topic would not be reopened in the near future, the highly volatile international context might lead the EU to reconsider this position. Important gaps remain in terms of security of supply chain issues, systems for supervising and enforcing standards, as well as reporting obligations for private and public institutions faced with cybersecurity challenges. The objective of such an NIS3 initiative would not be to over-regulate the economy, but rather to evolve towards smarter, leaner and more targeted forms of regulation that aim to specifically address gaps in key sectors.

In general, Regulations should be privileged over Directives as legislative tools for the EU in the domain of cybersecurity.[19] This would contribute to strengthening EU legislation in this field, since Regulations are immediately binding and directly applicable in their entirety across all 27 Member States. By contrast, Directives provide much more leeway, both from a temporal perspective with a potentially extensive time period for transposition at the national level, and in terms of providing countries with a wide margin for manoeuvre in the enactment of EU norms, which can be adapted to specific national circumstances.

Clearly, Directives open the door to the possibility of differentiated standards for cybersecurity across Member States, leading to fragmentation and a multispeed Europe. They may exacerbate the problem of weak links, which could be mitigated through greater reliance on Regulations as a privileged legislative tool for the EU when it comes to cybersecurity. Thus, it would be useful for the Commission to consider a third NIS legislative proposal under the format of a Regulation instead of a Directive, as was the case recently with the Cyber Resilience and Cyber Solidarity Acts, with smarter and more targeted forms of regulation addressing the specific gaps in key sectors.

Beyond upgrading EU legislation in this area, there are other possibilities over the short term to reinforce the EU's policy framework for cybersecurity. For instance, it would be useful to develop more efficient interconnections between the EU's legislative paradigm in this area and the EU's Common Security and Defence Policy (CSDP). Although the latter is still incipient, this could help to reinforce harmonization of standards and norms on cybersecurity between Member States via enhanced information-sharing, along with more regular exchanges of expertise and best practices.

In addition, another method to enhance harmonization could be to reinforce collaboration and joint exercises on cybersecurity between European nations and the United States, particularly via entities such as NATO. NATO already holds a cybersecurity exercise each year for alliance members called 'Locked Shields', which simulates different types of large scale cyberattacks and how NATO should respond.[20] More regular cyber exercises of this nature could be organized, which would encourage greater harmonization of cyber norms and standards within the Alliance, and between EU Member States.

Lastly, over the short term, the reinforcement of partnerships between governments and the private sector (public-private partnerships) is also critical for addressing previously mentioned cybersecurity gaps with current EU legislation. Across Europe and globally, industry and private firms have a critical role to play concerning the elaboration of norms and best practices in the field of cybersecurity, where they work in partnership with governmental entities. For instance, most EU Member States have established formal partnerships between companies and national governments to bolster cybersecurity, including cybersecurity councils composed of private and public sector representatives. Likewise, the EU launched a 'Contractual Public Private Partnership' (cPPP) in 2016 which brings together the Commission and the 'European Cyber Security Organization' (ECSO - an entity that encompasses private firms and public stakeholders[21]). The cPPP seeks to enhance collaboration between private and public sector entities on cybersecurity via the promotion of common standards.[22] This was reinforced by the 2019 Cybersecurity Act, which developed an EU certification scheme with the aim of enhancing public-private partnerships by creating an internal market for cybersecurity products.

While such initiatives are helpful, collaboration and dialogue between public and private stakeholders on cybersecurity does not go far enough. For instance, the cPPP constitutes a relatively loose, non-binding and under-developed framework when compared to its counterparts in other countries, such as the United States for example.[23] On a more general level, private companies are sometimes hesitant to inform public entities when affected by a cyberattack due to the reputational harm that might ensue. Likewise, dialogue between national frameworks and EU-level initiatives remains inadequate on a number of counts.

Therefore, over the short run, it is essential for the EU to bolster existing private-sector partnerships for cybersecurity such as the cPPP, by making them more rigorous, including in terms of rendering at least some of their shared norms and standards mandatory. Likewise, it might be useful for the EU to consider creating new frameworks that would specialize in certain fields such as

energy or telecommunications. Such new public-private partnerships would need to find ways of encouraging firms to disclose cyberattacks more easily without fear of reputational harm, perhaps by creating a system of anonymous reporting. These new frameworks should also seek to bring in and work more closely with national-level initiatives to ensure better harmonization of standards across the EU.

Over the medium to long run, however, more ambitious policy upgrades are necessary, including a change in the current allocation of competences between the EU and Member States on the issue of cybersecurity. In this regard, the current legal framework, whereby defence remains a national prerogative, will in all likelihood stymie the development of a robust common European cybersecurity policy, failing to resolve the problem of weak links. It is correct that the rise of populist Eurosceptic movements across the continent will make it challenging to convince Member States to transfer additional competences to the EU in the short term. This is especially the case for a policy field like defence, which lies at the core of national sovereignty. Nevertheless, Europe is facing a highly challenging and volatile international context. Russia is making progress on the Eastern front in Ukraine, with Member States in Central and Eastern Europe particularly exposed to Russian expansionism. Likewise, Trump's return to the White House has shaken the very foundations of NATO due to his ambiguous statements on Article 5 whereby an attack on one member constitutes an attack on all, which Russia might seek to exploit in the near future.

Therefore, the need to reinforce and strengthen the EU's defence capabilities, including in the realm of cybersecurity, has arguably never been more urgent, with the continent facing existential risks during the next few years. This dangerous situation might help to convince reluctant Member States and public opinion. For instance, Germany or Scandinavian countries, which have historically been keen to rely on US military deterrence, are becoming more open to the idea that the time is now for the EU to assume responsibility for its own defence.

This would entail deeper forms of integration to reinforce the EU's common security and defence policy, especially in the highly strategic sector of cybersecurity. Certain countries like France have been promoting the idea of a reinforced EU defence policy, with President Macron recently setting out ideas to European partners on how this could be achieved under the Trump administration. Other Member States with prominent military forces, like Poland or Spain, have also been advocating for the reinforcement of a more integrated common EU defence framework.

Rather than duplicate existing frameworks like NATO, the EU must work alongside them, and establish close collaboration with the UK as a former EU member and important military power. Due to the current unpredictability of US policy, collaboration with the UK on cybersecurity and defence issues will be particularly important for the EU, with Prime Minister Starmer clearly reiterating Britain's continued commitment to Europe's defence.

Although this may appear idealistic, it should be noted that Member States have already transferred key national prerogatives to the EU during the last few decades in other essential policy domains. A good example of this is monetary policy, which involves an essential aspect of national sovereignty; and yet, the euro was successfully adopted over twenty years ago and has survived multiple challenges to become one of the world's strongest currencies. While it will be challenging for the EU to advance towards more federalism in the area of defence and cybersecurity, a constellation of factors, both internal and external, are converging in such a way that there is now a pressing impetus to leap forward in this area with deeper forms of integration over the medium to long run.

Bibliography

Barichella A. (forthcoming 2025) Editor-in-Chief. The Palgrave Handbook of Cybersecurity, Technologies and Energy Transitions. Palgrave Macmillan – Palgrave Studies in Energy Trasition series.

Barichella A. (2023). "Cybersecurity and Data Protection in the Power Sector: Challenges, Perspectives and Policy Approaches" in Considine J., Cote S., Cook D. and Wood G. (Editors), A Research Agenda for Energy Politics. Edward Elgar Publishing – Research Agenda series.

Barichella A. (2022a). Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe. Policy Paper n°281 – Jacques Delors Institute.

Barichella A. (2022b). European Cybersecurity and Data Privacy: Threats and Prospects. Policy Brief – Jacques Delors Institute.

Barichella A. (2018). Cybersecurity in the energy sector: a comparative analysis between Europe and the United States. Études de l'Ifri.

Bernabe J. B. and Skarmeta A. (2022), Challenges in Cybersecurity and Privacy - the European Research Landscape, River Publishers.

Blau A. et al. (2019), Cybersecurity: The Insights You Need from Harvard Business Review, Harvard Business Review Press.

Boulet G. et al. (2022), Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives (New Security Challenges), Palgrave Mamillan.

Christou G. (2016), Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (New Security Challenges), Palgrave Macmillan.

Fahey E. (2022), The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity (Modern Studies in European Law), Hart Publishing.

Hassanien, A. E. and M. Elhoseny (eds) (2019), Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments, Basel, Switzerland: Springer.

Karathanasis T. (2024), Cybersecurity and EU Law: Adopting the Network and Information Security Directive, Routledge Research in EU Law – Routledge.

Lindsay J. R., "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack", Journal of Cybersecurity, Volume 1, Issue 1, September 2015.

Porcedda M. G. (2024), Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis, (Hart Studies in Information Law and Regulation) – Hart Publishing.

Footnotes

1. Fahey (2022)
2. Blau et al. (2019), Hassanien and Elhoseny (2019)
3. Barichella (2022b)
4. Christou (2016)
5. Barichella (2023)
6. Regarding cybersecurity in the energy sector, see: Barichella (2025)
7. Porcedda (2024), Karathanasis (2024)
8. Barichella (2022b)
9. Barichella (2018)
10. Barichella (2023)
11. Ibid
12. Barichella (2018)
13. Barichella (2022b)
14. In total, the WannaCry virus ended up infecting computer systems in more than 150 different countries around the world. Ibid.
15. Regarding the difficulties of attribution, see: Lindsay (2015)
16. Barichella (2022a)
17. Ibid
18. Ibid
19. Barichella (2018)
20. Barichella (2022b)
21. ECSO, Mission & Objectives: https://ecs-org.eu/about
22. Barichella (2018)
23. This includes frameworks such as the Cybersecurity Risk Information Sharing Program (CRISP) for example, which works in close cooperation with the US Department of Energy. See: Barichella (2023).

07

Improving lawful interception for law enforcement agencies by supporting cross-border delivery

Neil Brown, decoded.legal

“Lawful interception… remains an inherently national matter. This national nexus poses a significant challenge to the development of a digital single market”

Background

Providing lawful interception has been a condition that national communications licensing authorities can, and do, impose on telecommunications operators[1] from the beginning of the European Union’s general authorisation regime. It remains an inherently national matter.

The methods for implementing lawful interception capabilities are standardised, and publicly available.[2]

Conversely, precise details, such as which telecommunications operators have implemented lawful interception capabilities, and how exactly they have done so, is typically regarded as sensitive, if not secret, information. Knowing this might assist actual or potential interception targets avoid surveillance, or assist threat actors who wish to attack and exploit lawful interception facilities.

Similarly agencies wish to keep secret their targets, both from the targets themselves (since lawful interception is typically a covert capability), and, in some cases, from public authorities in other countries.

The outcome is the expectation, if not a *de jure* requirement, that a telecommunications operator will maintain and operate lawful interception systems in their own country, will keep target lists in-country, and will maintain an in-country team to carry out requirements for lawful interception.

This national nexus poses a significant challenge to the development of a digital single market, and for telecommunications operators which wish to, for example, centralise their core networks, and support teams, even within Europe: even if they are committed to continuing to support lawful interception, the requirement to maintain equipment and staff in-country is a material constraint. It requires operators to spread their staff, and spending, thinly across multiple countries, rather than investing more substantially in, and staffing, a centralised, best-in-class, facility.

It is a constraint which is not faced by providers of over the top communications services, with implications for a level, competitive, playing field.

Enabling Cross-Border Lawful Interception Capabilities

This paper proposes a number of suggestions to aid thinking in how this problem can be unpicked, to enable European telecommunications operators to centralise their systems and people, and help the EU proceed towards a digital single market, while continuing to provide the same (if not improved) lawful interception capabilities, operated centrally, and recognising the security constraints of national law enforcement agencies.

Each of the six proposals individually goes some way towards achieving this goal, but the goal would be most readily achieved if the proposals were considered and implemented collectively.

This paper does not:

- Propose changes to the substantive rules of lawful interception, or the scope of any given Member State's powers (e.g. in terms of cross-border targeting). It is about enabling a telecommunications operator to meet legal obligations in respect of lawful interception on a cross-border basis.

- Comment on the desirability, or not, of lawful interception. This paper will not - indeed, cannot - add anything to what has already been said on those fronts.

- This paper focusses only on 'traditional' lawful interception, and only on law enforcement functions; it does not touch on other capabilities, or national security functions. The centralisation of other law enforcement functions and capabilities would be important to fully ensure effective cross-border capabilities, but is beyond the scope of this paper.

Measures to facilitate centralisation of networks and services

Explicit legal recognition that telecommunications operators can fulfil lawful interception obligations from anywhere within Europe

Annex 1, A4 of Directive (EU) 2018/1972 says that one of the general conditions which may be attached to a general authorisation for electronic communications services (except in respect of number-independent interpersonal communications services) is:

> Enabling of legal interception by competent national authorities in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC.

At present, these obligations are implemented at an inherently national level, with no possibility foreseen for providers to manage requests for lawful intercept in a cross-border manner.

However, a recent paper, "Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement" indicated that:

> The experts agreed that one of the main objectives [of updating lawful intercept rules] would be to create a level playing field between CSPs and other types of electronic communication providers when it comes to enforceable lawful interception obligations.

Other types of 'electronic communication provider', such as providers of 'over the top' communication and platform services already have a greater ability to manage similar law enforcement support requests on a cross-border basis. Law enforcement agencies will typically tolerate cross-border provision of support from these providers, where they are willing to provide this.

Furthermore, the recent development of the eEvidence framework allows authorities in one Member State to request the support of service providers (both traditional telco and over the top communication and platform services) in a third Member State. This framework applies only to obtain certain retained customer data rather than lawful interception of a communication in the course of its transmission, but demonstrates how cross-border Law enforcement agency support may operate in practice.

Whilst this paper is not recommending that the eEvidence framework (which applies to static data, and gives broader jurisdiction to law enforcement authorities over this data) is applied wholesale to 'traditional' law enforcement, the principle that service providers should be able to manage law enforcement requests in a cross-border manner can clearly be extrapolated from this new framework.

Therefore, for there to be a level playing field, telecommunications operator should be empowered to operate in the same cross-border way as providers of over-the-top communications services.

To this end, the starting point of this paper is that there should be express recognition within the European Electronic Communications Code, or another legislative document, that an operator may meet its obligations in respect of lawful interception, in respect of any or all of the Member States in which it provides electronic communications networks or services, from anywhere within the European Union, subject to meeting standardised security requirements.

Those standardised security requirements - of which examples are discussed below - would be designed at a European level, rather than being driven by each national government, and should be capable of practical, cost effective, implementation by telecommunications operators. In other words, the security requirements must not act as a deterrent, or otherwise inhibit, telecommunications operators from centralisation.

Common, Europe-wide, lawful interception capabilities

To enable telecommunications operators to provide lawful interception capabilities centrally, there should be a common, European, standard. Today, there are broad commonalities, but national specificities. A common standard would leave it to each telecommunications operator how to meet that standard, enabling them to take into account differences in national networks (for instance), but it would also permit a telecommunications operator to design one set of lawful interception capabilities, applicable to their networks and services wherever in the Union those are located.

This approach would be beneficial in terms of network upgrades and service changes, with a common standard that each new network or service must meet.

For security reasons discussed below, this may still entail separated, but still centralised, implementations, split along country lines.

Standardisation of capability does not mean that a telecommunications operator must provide lawful interception capability for each Member State. This must still be subject to requirements of necessity and proportionality.

The capability which each telecommunications operator maintains in respect of each Member State would be secret (from other Member States, as well as between operators), operated by vetted telecommunications operator staff (below).

A standardised protocol for the communication of law enforcement assistance orders

Today, an operator which receives requests from law enforcement agencies across the Union may deal with incoming correspondence in different languages, and in different forms, requesting different types of assistance.

This is sub-optimal, bringing with it the risks of misunderstanding or misconstruing requests, and an increase in handling time by telecommunications operators.

In addition to the discussion in respect of the standardisation of capabilities themselves, this paper proposes a mandatory standardised, pan-European, XML schema for the communication of law enforcement assistance obligation. By way of example, see ETSI TS 103 120.[3]

Each European law enforcement authority would transmit to the relevant telecommunications operator its orders using this standardised template.

By adopting a standardised, machine-readable format, an operator could readily and safely extract (automatically or manually) the key information relating to the capability, including the nature of the obliged assistance, factors such as the identity of the target(s), the required time frames, and so on.

Because these would be standardised fields, with standardised metadata identifiers, risks associated with misunderstanding key information about the request due to language or formatting barriers would be greatly reduced.

Ideally, this approach would extend not just to orders relating to lawful interception, but all aspects of law enforcement assistance, and orders of courts and other judicial bodies.

A standardised means of verifying the authenticity and integrity of an order for lawful interception

If a telecommunications operator would, in a centralised team, receive orders to carry out lawful interception, there would need to be simple means by which a telecommunications operator could verify the authenticity of an order to carry out lawful interception, and its integrity.

In other words, a readily available, standardised way for an operator to be confident that:

- the order went through the correct prior independent authorisation;
- the order came from an authorised law enforcement agency, rather than an unauthorised third party using a look-alike email address or a template form of order; or
- that the order was not modified in the course of its transmission or re-transmission to the operator.

This paper proposes that all requests for law enforcement assistance should be digitally signed by the requesting law enforcement authority or the independent authorising body (ideally the latter), in such a way that a telecommunications operator can verify both the authenticity of the order and its integrity, thereby being assured that it is a genuine, authorised order.

Meeting security needs of law enforcement agencies

Mutual recognition of security vetting

As discussed, the provision of lawful interception capability entails processing of sensitive information, including the precise means by which lawful interception is carried out, and the identity of the targets.

Law enforcement agencies quite reasonably seek that the staff of telecommunications operators who are involved routinely in lawful interception matters are vetted, and hold a suitable level of security clearance.

Typically, vetting, and subsequent clearances, are available only to people who are nationals, or long term residents, of the country in question.

This is not consistent with an approach of centralised lawful interception provision, since staff in one or more countries would maintain lawful interception systems, and give effect to lawful interception orders, within the EU but on a cross-border basis.

This paper proposes, as a minimum, mutual recognition of national security vetting. The effect of this would be that someone could be vetted in a Member State and, if they passed vetting, would receive a clearance which would enable them to work on lawful interception capabilities for any country within the EU, not just the country which granted them their clearance.

A directory of telecommunications operator contacts

Today, relationships between law enforcement agencies and telecommunications operators are predominantly national.

Each law enforcement agency will know which telecommunications operators have what capabilities, on which legal entity they need to serve an order, how to serve an order, practically, and with whom they should speak in the event of a problem or question.

This would be more challenging if telecommunications operators moved away from national provision of lawful interception.

This paper proposes a centralised directory for the contact points of telecommunications operators across Europe, accessible (only) to law enforcement agencies and other relevant public authorities.

This directory would enable telecommunications operators to specify a single point of contact, within the European Union, for all requests relating to law enforcement assistance.

All law enforcement authorities would direct requests to - and only to - the contact points set out in this directory.

Technical means to maintain secrecy of targets

More work will be needed to determine how, in a centralised model, secrecy of sensitive targets would be maintained.

In other words, what measures would need to be in place to reassure a law enforcement agency of a Member State that, if it were to task a target for lawful interception by a telecommunications operator in another Member State, that other Member States would not be able to obtain that target information.

This could comprise a combination of legal and technical approaches.

In terms of a legal approach, target information could be given a privileged degree of protection, such that Union law prohibited the disclosure of target information.

From a technical point of view, there may be value in considering separate, virtualised, lawful interception instances, all run centrally by the telecommunications operator. Each Member State which required lawful interception would have its own separate virtual instances, with no sharing of target information between instances.

An added degree of protection may be sought through the storage of target information in encrypted form, using different keys for each Member State, with decryption taking place only within the lawful interception management system.

Impact of Proposals

While each of the proposals would, it itself, have merit, their cumulative implementation would facilitate effective cross-border, potentially improved, lawful interception capability, while supporting the needs of national law enforcement agencies.

A more harmonised approach to lawful interception through the standardisation of requirements, and the ability to manage lawful interception requests cross-border, will make it possible for telecommunications operators to operate networks and services from a centralised core, a key requirement for the deployment of cross-border networks. This will facilitate greater levels of cross-border scale in Europe, bringing the EU closer to a true digital single market.

It will also help level the playing field between traditional telecommunications operators and over the top communications services providers, improving competitive conditions in digital communications.

For law enforcement agencies, if telecommunications operators were able to centralise lawful interception systems and operations, operators would be better placed to invest in best in class technology and processes, and develop a highly expert response team, leading to more consistent and higher levels of service, and more consistent output. Similarly, common standards on transmission of requests should lead to more cost-effective systems for agencies, and a smoother, streamlined, end to end workflow.

Footnotes

1. Strictly, providers of electronic communications networks and electronic communications services. In less legalistic terms, these are the companies operating physical access networks, and providing services using those networks, such as Internet access providers.

2. See, for instance, https://www.etsi.org/committee/1403-li

3. https://www.etsi.org/deliver/etsi_ts/103100_103199/103120/01.18.01_60/ts_103120v011801p.pdf

everyone.connected