ISPA BELGIUM

VISION DOCUMENT

INTERNET SERVICE PROVIDERS ASSOCIATION
Rue de la Loi 38, 1000 Brussels

Introduction

As the Belgian Internet Service Providers Association, ISPA Belgium brings together the Internet industry ecosystem in Belgium, incorporating companies that make the internet work, such as internet service providers (ISPs), web hosting providers, cloud service providers and content providers. Our association ensures that the voice of the Internet community is heard and understood, to enable the creation of digital friendly, future-oriented and coherent policies in Belgium.

ISPA Belgium continues to be active in various sectors of activities and acts as the contact point of the Internet industry in Belgium, aiming to fulfil the economic and social potential of the Internet. Our association's activities are focused, among others, around the topics of the interplay between European and Belgian legislation, data retention, safer internet and cybersecurity, artificial intelligence, privacy and data protection, and sustainability.

Executive summary

1. Stimulating the responsible use of internet and embracing innovation

Belgium faces challenges in digital performance, ranking below the EU average in key indicators. Digital inclusion is hindered by a lack of basic digital skills, particularly impacting vulnerable groups. While commendable initiatives exist, fragmented governance and hesitancy in public authorities to adopt cutting-edge technologies hinder progress. Proposed solutions include integrating digital tools in education, upskilling initiatives, public-private partnerships, and a government leading by example to foster a culture of innovation.

2. Safer internet

Increasing cyber threats and rising computer crime cases underline the need for a coordinated cybersecurity strategy. Fragmented competences contribute to a challenging environment, and the shortage of cyber skills in the workforce poses a significant risk. The Digital Services Act and proposed CSAM Regulation at the EU level could potentially offer positive steps, but a 360-degrees approach is still needed. Proposed solutions involve central political coordination, awareness campaigns, enhancing cyber skills, and incentivizing businesses to invest in cybersecurity. Multi-level collaboration and public-private partnerships are crucial to creating a safer online environment.

3. Regulatory and investment friendly framework

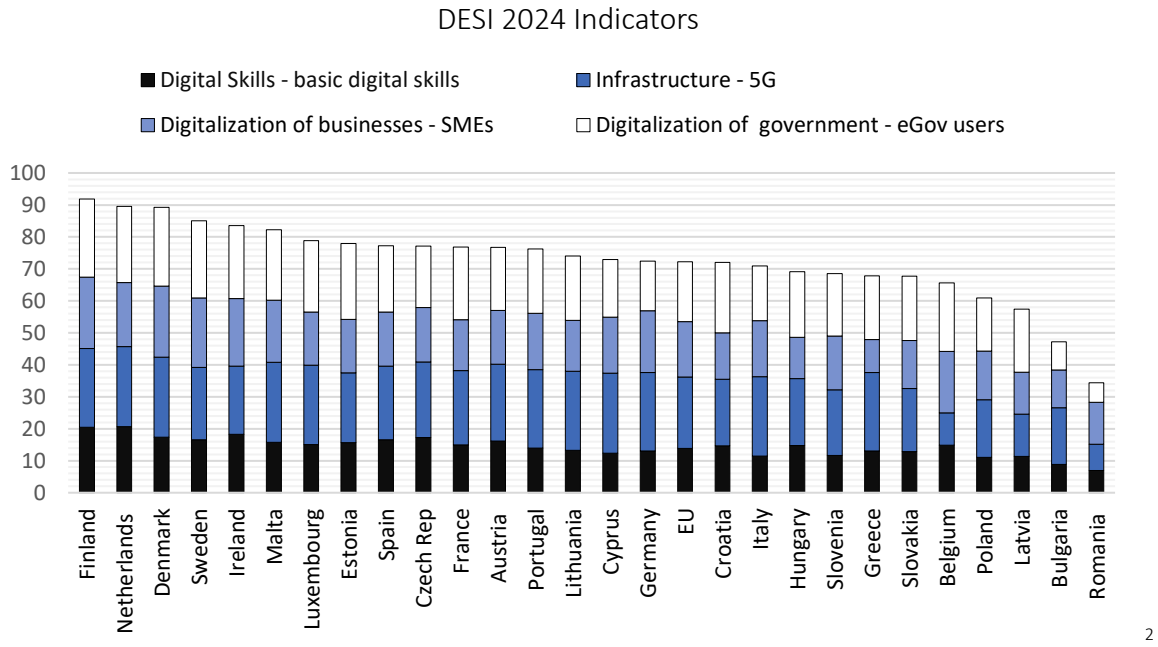
The internet sector calls for a fundamental reassessment of the regulatory framework into a truly investment friendly framework, with legislation that is harmonized between the EU and the member states, but also internally within Belgium (federal, regional and local). The multitude of regulations and directives, combined with national measures, creates a complex environment. To address this, ISPA calls for a period of "stop and think" for regulatory initiatives, to allow for a thorough reassessment of the rules that should lead to simplification. A clear framework aligned with EU standards, harmonization within Belgium, and a more investment friendly fiscal structure are proposed to support the growth of the digital and telecommunications sector. Strengthening awareness of EU policies among stakeholders is essential for effective resource allocation.

1. Stimulating the responsible use of internet and embracing innovation

Context

The Digital Decade Country Report[1], an annual publication by the European Commission, provides a complete assessment of a country's digital performance, based on four indicators: digital skills, digital infrastructure, digital transformation of businesses and digitalization of public services (see figure 1). In the latest edition of this report, Belgium ranks below the EU average on several of these indicators. This sobering reality emphasizes the need for digital growth in our country, both at an individual and societal level. Embracing innovation and making sure everyone can keep up with digital progress, is a crucial step towards sustainable digital growth.

Figure 1: DESI 2024 Indicators



[2]

Source: DESI 2023 dashboard for the Digital Decade

Issue

Digital inclusion means that every individual, regardless of age, gender or socio-economic background can fully participate in the digital society. However, Belgium is lagging behind in terms of digitals skills: only 59% of Belgian citizens has basic digital skills, while hardly 28% of individuals is equipped with above basic digital skills.

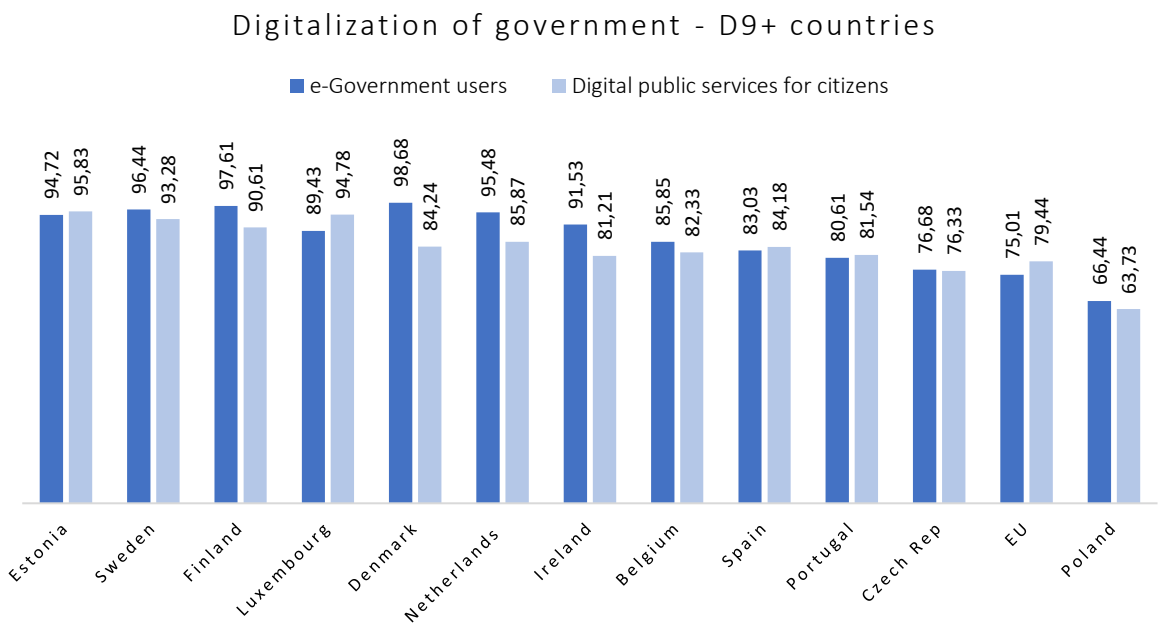
This **gap** prevents people from potential vulnerable groups such as the elderly, people on low-incomes and people with migration backgrounds from fully participating in the digital society as it would limit their access to information, job opportunities and social engagement. This divide reinforces existing social inequalities and leaves a group of Belgian citizens at a disadvantage.

[1] Former name of the index was DESI – link: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports.
[2] DESI 2024 dashboard for the Digital Decade – link: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts.

Several initiatives to improve digital literacy both from public and private players already exist today, such as the BeCentral digital campus[3], DigiSkills Belgium[4], the Digitall coalition[5], the Flemish Digibanks[6], and the UpSkills Wallonia strategy[7]. ISPA supports and applauds these developments, as they can be truly effective in upskilling adults. However, because they are often initiated by different levels of government, our country **would benefit from a coherent strategy** and campaign to make citizens sufficiently aware of the various options.

The **government** also has an important part to play here, as it sets an **example** for its citizens. Belgium, with an impressive 85% engagement in e-Government services, stands as a commendable example of digital progress. However, a discerning examination reveals a hesitancy within public authorities to fully embrace cutting-edge technologies compared to other D9+ nations, as shown in the figure below. This hesitancy to innovate not only hinders efficiency but also creates a gap in setting an example for citizens to follow. Adopting cloud technology and leveraging the opportunities offered by artificial intelligence can help drive the modernization of government services.

Figure 2: Digitalization of government – D9+ countries



Source: DESI 2024 dashboard for the Digital Decade

Proposed solutions

Digital tools in education – Education should play a central role in improving digital skills. While adopting digital tools is not an objective in itself, where benefits are clearly demonstrated, introducing children to these tools early on not only customizes their learning experience but also familiarizes them with digital technology, bridging the digital divide. By integrating digital tools into learning, children can enhance their educational experience, potentially improving reading comprehension for non-native pupils and contributing to a more effective education system overall.

[3] BE CENTRAL – Digital Campus – link: https://www.becentral.org/.
[4] DigiskillsBelgium.be – link: https://digiskillsbelgium.be/.
[5] Digitall – link: https://digitall.be/.
[6] Digibanken Vlaanderen – link: https://digibanken.vlaanderen.be/.
[7] UpSkills Wallonia – link: https://www.digitalwallonia.be/fr/programmes/upskills-wallonia/.

Focus on upskilling initiatives and lifelong learning – ISPA also emphasizes the vital importance of adult-learning initiatives. On the one hand, we ask for a well-structured strategy for the upskilling of potential vulnerable groups. This ensures that these individuals are not excluded in the digitized community while also widening their options on the labor market, considering the pressing shortage of ICT-specialists. That said, whilst it is crucial to give people better tools to navigate through an ever-increasing digital society, alternative options still need to be continuously offered in order to keep working on a balanced and inclusive societal framework. For example, offering online government services is necessary in a modern society, but people should still be offered the option to make an in-person appointment with a public servant.

On the other hand, ISPA supports the efforts that are being taken regarding lifelong learning (e.g. on the Flemish level[8]) since it contributes to ensuring that individuals can adapt to evolving technological landscapes. The sector suggests the implementation of a broad awareness campaign to promote the benefits and availability of lifelong learning.

Public-private partnerships – Collaboration with the private sector will be key to achieving the digital skills goals. Enterprises possess the expertise and the latest technologies to support authorities and educational structures in successfully developing a strong digital skills strategy. The sector urges the legislator to elaborate a well-functioning program for structural partnerships between public and private to enhance digital skills.

Coordinated multi-level collaboration – ISPA supports existing initiatives that are committed to enhancing digital literacy. However, we believe they are not able to reach their full potential in impacting society because of their rather fragmented nature. Hence, we support a constant knowledge exchange between different approaches and the development of a coordinated campaign to reach citizens more effectively.

Performant internet infrastructure – There is a growing demand for digital services. To meet this demand and to ensure the successful digital transformation of both public and private players, a strategic focus on robust internet infrastructure, including the deployment of Gigabit networks, should be prioritized. The sector pleads for measures to accelerate and facilitate the deployment of this infrastructure and increased resources to ensure reliable connectivity, especially in remote areas, to actively include every citizen in the Digital Decade.

A public sector that leads by example – To address the cautious approach in embracing new technologies by the public sector, Belgium can lead by example. By championing a bolder adoption of technological advancements, especially in areas like cloud computing and artificial intelligence, the government can not only modernize public services but also provide citizens and organizations with a compelling example to follow. This goes beyond technological progress; it sets a standard for progressive governance, fostering a culture of innovation and efficiency that resonates with the digital needs of its people. This is why ISPA welcomes and encourages the development of a cloud first policy for the public sector.[9]

---

[8] Vlaanderen – Expertisecentrum Innovatieve Leerwegen – Levenslang Leren – link: https://www.vlaanderen.be/levenslang-leren.

[9] Ministerraad 17 mei 2024: Plan van aanpak voor de opmaak van een transversaal plan voor cloudadoptie bij de federale overheid– link: https://news.belgium.be/nl/plan-van-aanpak-voor-de-opmaak-van-een-transversaal-plan-voor-cloudadoptie-bij-de-federale-overheid.

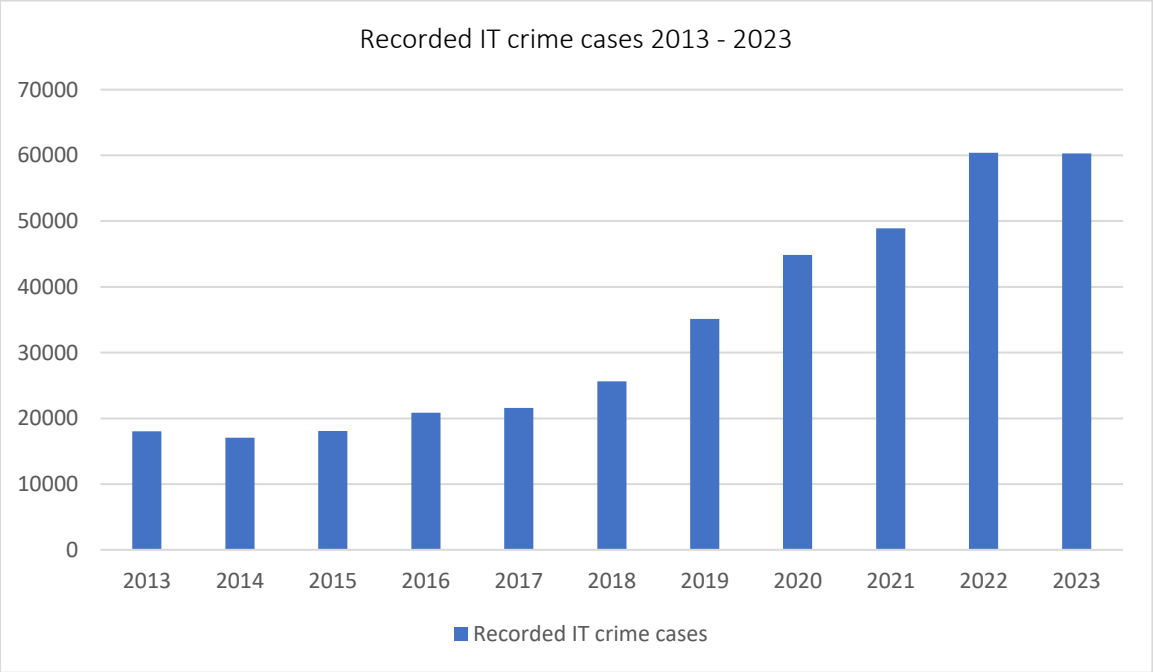
2. Safer internet

Context

The war in Ukraine and ongoing cyber-attacks on Belgian entities have intensified the urgency of cybersecurity measures. Beyond these immediate concerns, addressing illegal online content and ensuring a safe digital space for young individuals are crucial aspects of fostering a secure internet environment. Phishing, internet fraud, cyber-attacks, and the proliferation of illicit online content have shaken the confidence of citizens, businesses, and governments in the internet's safety. This erosion of trust emphasizes the need to collaborate with stakeholders and governments to ensure a secure internet environment that garners users' trust.

In parallel with bolstering cybersecurity efforts, it is vital to address the challenge of illegal online content, particularly content linked to child exploitation. Upholding ethical standards and safeguarding vulnerable internet users are imperative goals. Alongside existing initiatives like age-appropriate content filters, educational programs, and responsible online conduct promotion, adaptable privacy and security policies remain pivotal. These proactive measures foster a safe online environment, preserving the internet's societal and economic value by emphasizing responsible practices within the online ecosystem.

Figure 3: Recorded IT crime cases between 2013 - 2023



Source: Police crime statistics 2013-2023, Federal Police

Issue

A **fragmented division of competences** when it comes to cybersecurity, and digital topics in a broader sense, make it difficult to build an efficiently coordinated cybersecurity, or even internet policy. This makes it all the easier for hackers to have their way in the Belgian digital sphere.

Computer crime has been rising for years, going from 18 074 cases in 2015 to 60 373 cases in 2022, as recorded by the federal police. Whilst that number stagnated in 2023 (60 304), there is clearly an increasing and worrisome trend in terms of internet safety (figure 3).[10]

Another continuous issue is the challenge of addressing **illegal online content** and **misconduct**, encompassing the dissemination of terrorist content, cases of Child Sexual Abuse Material (CSAM), illegal streaming, and incidents of grooming or sextortion. This multifaceted problem poses a significant threat to online safety and privacy, especially for (young) children, necessitating a comprehensive strategy.

Cybersecurity skills are of paramount importance for internet safety as each internet user carries a responsibility in a performant cybersecurity system. In total, only 39% of the Belgians have an above average level of cyber skills, whereas 26% has a basic understanding, leaving 28% with no cyber skills at all (note: 9% does not use the internet).[11] This means a fourth of our country's population is not equipped with the correct knowledge to secure their data and themselves online. These issues align with the broader context of the lack of digital skills in Belgium, as previously mentioned in this document.

Not only citizens, but **businesses** need a good level of understanding about implementing the correct and appropriate cybersecurity practices. For this, they need to become more aware of the importance of it and they need to attract the right people. Following a survey that was conducted by Agoria and Cevora[12], the profile of a **cybersecurity expert** is in high demand in Belgian business, but for many of them it is hard to attract the right profile.

Adding to that, the deadline for compliance with the **NIS 2 Directive**[13] is fast approaching. By 18 October 2024, it is estimated that around 3000 businesses in Belgium will have to implement the correct measures to make themselves compliant with the new set of rules. This deadline is approaching fast and awareness is not yet where it should be.

Proposed solutions

Central political coordination of internet related policy – The issue of decentralized coordination in internet policy at the federal level needs to be tackled. With an ever-increasing complexity in digital, telecom and cybersecurity policy, and an ever-increasing interwovenness of the internet sector, it is crucial that all these aspects are being governed in a centralized way. Ideally, that means having one minister, competent for all these fields of federal competence, that has a mandate to propose broad and horizontal legislation and policies, reaching beyond the traditional division between different portfolios of those federal competences. ISPA believes combining telecommunication, cybersecurity and digitization policies under one minister would be beneficial for achieving a safer internet.

Investment in awareness and cybersecurity – Investing further, not only in programs that elevate the Belgian cybersecurity posture, but also in general awareness on the importance of proper use and safekeeping of the internet, are crucial building blocks in maintaining a safer internet. This not only applies to the public sector, but also to businesses and citizens.

---

[10] Politiële criminaliteitsstatistieken 2013-2022, Federale Politie.
[11] Statbel, digital skills 2021 – Safety.
[12] Cybersecurity-expert nieuwste knelpuntberoep, Agoria, 2023 – link: https://www.agoria.be/nl/standpunten/vlaanderen/cybersecurity-expert-nieuwste-knelpuntberoep.
[13] Directive (EU) 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 (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Enhancing cyber skills – To empower individuals and businesses to navigate the digital landscape safely and responsibly, mitigating online risks effectively. We welcome initiatives and missions of organizations such as Molengeek, BeCode, Digiskills Belgium and others, who actively contribute to improving the digital skills of everyone who wants to. However, as mentioned earlier, our sector calls for a constant exchange between the different existing approaches. A more coherent strategy is needed to offer citizens the needed tools to recognize and deal with cyber risks.

Increase business' awareness – The importance of a good cybersecurity posture in business in Belgium should be made more explicit. Companies should understand better what the potential risks are of not or underinvesting in cybersecurity, be it financial, operational or reputational. The legislator can anticipate to this by pointing out these risks, but also by stimulating this via an incentivizing regulatory framework, with a focus on proactive, rather than reactive measures. For example, the expense made by companies who become victim of a cyber-attack and have to pay ransomware to free their data systems can be considered a deductible professional expense according to the current tax regime. Tax regulation like this is not incentivizing and undermines companies' willingness to invest. Instead of offering a band aid after falling, the goal should be to prevent companies from falling at all.

Attracting cybersecurity experts – To help businesses attract the right cyber profiles, we support the plea of Agoria to add this to the list of bottleneck professions in all regions in Belgium. Despite the high demand of companies, this is not yet the case on neither the list of bottleneck professions of VDAB, nor Le Forem or Actiris.

End-to-end encryption (E2EE) – Protecting E2EE is vital for guaranteeing the privacy and security of user data in online services, establishing a trustworthy internet infrastructure that respects users' private lives and safeguards both personal and professional communications from cyber threats.

Take for example online banking, many mobile banking apps utilize E2EE to ensure secure communication between the user's device and the bank's servers. This encryption safeguards sensitive information such as login credentials, account details, and transaction data from being intercepted or accessed by unauthorized parties. E2EE also protects data that we store on several cloud services, we can conduct online shopping in a safe way and it ensures that sensitive health information is protected in the area of telemedicine or on telehealth platforms. ISPA therefore asks the legislator to not take future initiatives that would undermine, rather than safeguard, E2EE.

Multi-level approach – To effectively tackle the issue of inappropriate online content or behavior, a collaborative and multi-pronged approach is essential. Firstly, recognizing the proactive efforts of our members, who play a vital role in assisting their customers in navigating and addressing these challenges, is crucial.

The implementation of the Digital Services Act (DSA)[14] and ongoing discussions on the proposal for a CSAM Regulation[15] at the EU level are positive steps towards taking measures. At ISPA we believe the **EU** level is best equipped to deal with this cross-border issue.

Use of the D9+ Group – Our sector should acknowledge the importance of the D9+ Ministerial Group and actively encourage the digital ministers of these small and medium-sized countries to align on EU policy initiatives and spearhead the digital transition. Through the D9+ Group, Belgium can take a

[14] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
[15] Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.

leadership role in fostering the Digital Single Market, which is of fundamental importance for Belgium's open economy.

At the **national** level, we advocate for a complementary 360-degree approach, acknowledging the role of various stakeholders, including internet service providers, OTTs, governmental bodies, and NGOs like Child Focus. Notably, Child Focus' commendable work in both informing and preventing online threats, particularly to young individuals, deserves recognition. Their efforts contribute significantly to creating a safer digital environment, and we encourage collaborative initiatives that amplify their impact. Through these combined efforts, we aim to foster a comprehensive and cohesive strategy that addresses the multifaceted challenges posed by illegal online content and misconduct, with a particular focus on protecting the safety and privacy of (young) children. ISPA is open to any dialogue with the involved stakeholders on solutions to make the internet a safer environment.

Transparent and open consultations – During the transposition of the NIS 2 Directive, the Centre for Cybersecurity (CCB) launched a public consultation and collected stakeholder input. As a sector, we support this type of processes and we encourage the legislator to make a habit out of involving stakeholders – who are affected by a specific piece of legislation – in the legislative process. Moreover, we highly encourage to involve the sector as early as possible. More importantly, we ask that these processes are done in a transparent and open way to foster a level-playing-field for any stakeholder who wishes to be involved in the process.

Public-private partnerships – Building strong public-private partnerships between ISPs, OTTs, hosting providers and authorities facilitates information sharing and strengthens the collective response to online fraud. Also, promoting open and transparent multi-stakeholder cooperation fosters a holistic approach to addressing cyber threats, leveraging the expertise and resources of governments, industry, and civil society. The Belgian Anti Phishing Shield (BAPS) is an excellent example of how the direct involvement of ISPs in an initiative of the CCB, is actively contributing to a safer internet.

3. Regulatory and investment friendly framework

Context

The internet sector calls for a fundamental reassessment of the regulatory framework into a truly investment friendly framework, with legislation that is harmonized between the EU and the member states, but also internally within Belgium (federal, regional and local). This calls for a strong awareness of the impact of EU policies in the digital sector, as well as our country's resources being allocated to measures that add value. This way, the digital and telecommunications industry can truly play its role as an innovation stimulating sector.

Issue

A great deal of regulating the internet sector is done at EU level. As shown by the illustration (see Annex 1), the past European mandates have produced a **wide range of initiatives**, among others, in the areas of privacy, data protection, cybersecurity, content moderation, etc. The implementation of these initiatives requires significant company resources, especially considering how fast the sector evolves and how quickly adaptation to new technologies is needed.

However, at times we see national, regional or community measures taken on top of this, often for issues already regulated at EU level. Seeing the vast amount of EU initiatives, this only creates a more **unclear regulatory framework** and threatens the harmonization of the internal market.

Moreover, deviating from the standards set by the EU, especially when implementation also differs between the different regions in Belgium, is only enhancing this fragmentation.

Finally, our country must create a **more investment friendly environment**. Companies are not only disincentivized from making investments because of the above-mentioned fragmented or outdated regulatory framework, but also the current taxation system can pose issues. Several municipalities tax transmission masts or fixed networks and are pushing for a retribution on fiber optic rollout, negatively impacting the investment climate in Belgium and hampering entrepreneurship and innovation.

Proposed solution

Focus on the thorough reassessment of existing regulatory initiatives – Our sector calls for the next EU legislature to focus on implementation and simplification of the existing rules. As shown by the annexed visual, the past two European legislatures have produced a wide range of initiatives for the digital and telecommunications sector. The sector needs the time for current initiatives to be properly reassessed.

Clear framework, with awareness of impact EU policy – A stronger "EU reflex" should exist amongst our policymakers and stakeholders. Having a strong knowledge of what and how measures are being regulated on EU level and what the effect is on the Belgian market, means our country's resources can be invested more adequately and efficiently in complementary measures to those taken on Union level.

Call against gold-plating – To have a stable, complemental regulatory digital framework, it is advised to not deviate from the requirements set by the EU. Extending the powers of directives when transposing them into national law needs to be avoided, in order to create a harmonized digital ecosystem within the Single Market.

Harmonized Belgian framework – Our complex state structure can often be a contributing hindering factor to balanced and coordinated policies. The sector therefore encourages effective coordination between the different regions, especially when implementing European legislation.

Examples:

- Belgium is the second European country to introduce a repairability index,[16] as part of the federal circular economy action plan. As a European repairability index is currently also in the making with the proposal of a directive on common rules promoting the repair of goods,[17] Belgium's early regulation risks deviating from the approach foreseen at EU level and fragmenting the internal market. Recital 2 of the proposed directive even mentions that "differing mandatory national rules in this area (i.e. repair of goods) constitute actual or potential obstacles to the functioning of the internal market, adversely affecting cross-border transactions of economic operators acting on that market".
- The Digital Services Act provides unified rules for a safe and trusted online environment in the Digital Single Market, targeted towards online intermediary services. The regulation of platforms is fully foreseen by the DSA, meaning Belgium should now focus on the necessary alignment between the various competent authorities for the implementation of the DSA, on providing sufficient transparency on the scope of the various competent authorities involved, and finally, in providing our Digital Services Coordinator with the needed tools to perform its task as efficiently as possible. This also includes raising awareness, enabling guidance and

[16] Press release Minister Khattabi 2 June 2023: Belgium becomes the second European country to introduce a reparability index – link: https://khattabi.belgium.be/en/pr-repairindex.
[17] Proposal for a Directive of the European Parliament and of the Council on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394, Directives (EU) 2019/771 and (EU) 2020/1828.

focusing on prevention regarding the DSA, its impact, and the rights and obligations it creates. For example, in protecting children online, our country can allocate a coordinating role to Child Focus.

Investment friendly framework – Finally, in order to strengthen an investment friendly framework, unnecessary fiscal burdens need to be averted. Double taxation and taxation on infrastructure, such as transmission masts and pylons[18] or fixed networks, must be avoided. Moreover, the request of several cities and municipalities for a retribution on fiber optic rollout must be countered.

[18] As part of the Giga Région program of Digital Wallonia, a new Tax on Pylons agreement (3rd edition) was agreed upon between the telecom operators and Wallonia. In the agreement, Wallonia undertakes to maintain the abolition of regional taxes and the recommendation to provinces and communes not to levy taxes on masts, pylons and antennas in exchange for investments in improved regional connectivity. We would like to see such measures on the whole territory, as several Flemish municipalities currently still have taxes on pylons in place. – link: https://www.digitalwallonia.be/fr/publications/giga-region-3eme-accord-top-operateurs/.

Annex 1: overview of recent EU initiatives (non-exhaustive)

	Adopted	Pending	(Potential) new initiatives
Research & Innovation	• Digital Europe Programme Regulation • Horizon Europe Regulation		
Industry Policy	• Regulation on High Performance Computing Joint Undertaking • Invest EU Programme Regulation • Decision establishing the Digital Decade Policy Programme 2030 • European Chips Act • Regulation establishing the Strategic Technologies for Europe Platform (STEP) • Net Zero Industry Act		
Connectivity	• Broadband Cost Reduction Directive • Open Internet Access Regulation • European Electronic Communications Code • Roaming Regulation • Regulation on the Union Secure Connectivity Programme • Gigabit Infrastructure Act		• Digital Networks Act
Data Protection & Privacy	• Regulation on the Free Flow of Non-personal Data • Open Data Directive • Data Governance Act • Interoperable Europe Act • Data Act	• ePrivacy Regulation • European Health Data Space (Regulation) • GDPR Enforcement Regulation	• GreenData4All
Cybersecurity	• Cybersecurity Act • NIS 2 Directive • Regulation establishing the European Cybersecurity Competence Centre	• Cyber Resilience Act • Cyber Solidarity Act	
Enforcement	• Regulation on Addressing the Dissemination of Terrorist Content Online • Temporary CSAM Regulation • E-evidence Regulation	• New CSAM Regulation	
Safety	• eIDAS Regulation • Regulation for a Single Digital Gateway • AI Act	• AI Liability Directive	
E-commerce & Consumer Protection	• E-commerce Directive • Directive on Consumer Rights • Geo-Blocking Regulation • Directive Concerning Contracts for the Supply of Digital Content and Digital Services • DSA & DMA • Regulation on Transparency and Targeting of Political Advertising	• Right to Repair Directive	• Multimodal Digital Mobility Services
Media	• Directive on Information Society Services • Audiovisual Media Services Directive • Copyright Directive • European Media Freedom Act		
Finance	• Payment Services Directive 2 (PSD2) • Digital Operational Resilience Act (DORA)	• Payment Services Directive 3 (PSD3) • Payment Services Regulation (PSR) • Regulation for Digital Euro	

Source: Bruegel factsheet - Overview of EU Legislations in the Digital Sector, 16 November 2023