ISPA BELGIË

VISIEDOCUMENT

JULI 2024

INTERNET SERVICE PROVIDERS ASSOCIATION
Wetstraat 38, 1000 Brussel

Inleiding

Als de Belgische associatie van internetdienstenleveranciers brengt ISPA België het ecosysteem van de internetindustrie in België samen, met bedrijven die het internet laten werken zoals internet service providers (ISP's), webhosting providers, cloud service providers en content providers. Onze vereniging zorgt ervoor dat de stem van de internetgemeenschap gehoord en begrepen wordt, zodat een digitaal vriendelijk, toekomstgericht en coherent beleid in België kan worden ontwikkeld.

ISPA België is actief in verschillende sectoren van activiteiten en fungeert als aanspreekpunt voor de internetindustrie in België, met als doel het economisch en sociaal potentieel van het internet optimaal te benutten. De activiteiten van onze vereniging zijn gefocust op thema's zoals de wisselwerking tussen Europese en Belgische wetgeving, dataretentie, veiliger internet en cyberbeveiliging, artificiële intelligentie, privacy, gegevensbescherming, en duurzaamheid.

Algemene samenvatting

1. Bevorderen van verantwoord gebruik van het internet en omarmen van innovatie

België staat voor uitdagingen op het gebied van digitale prestaties, gezien het onder het EU-gemiddelde scoort voor belangrijke indicatoren. Digitale inclusie wordt belemmerd door een gebrek aan digitale basisvaardigheden, wat vooral kwetsbare groepen treft. Hoewel er lovenswaardige initiatieven bestaan, belemmeren een gefragmenteerd bestuur en aarzeling bij de overheid om vooruitstrevende technologieën toe te passen de vooruitgang. Oplossingen hiervoor zijn onder andere de integratie van digitale hulpmiddelen in het onderwijs, bijscholingsinitiatieven, publiek-private partnerschappen en een overheid die het goede voorbeeld geeft wat het bevorderen van een innovatiecultuur betreft.

2. Veiliger internet

Toenemende cyberdreigingen en toenemende gevallen van computercriminaliteit onderstrepen de noodzaak van een gecoördineerde strategie voor cyberbeveiliging. Gefragmenteerde bevoegdheden dragen bij aan een uitdagende omgeving en het tekort aan cybervaardigheden bij de beroepsbevolking vormt een aanzienlijk risico. De Digital Services Act en de voorgestelde CSAM-verordening op EU-niveau kunnen potentieel stappen zijn in de goede richting, maar er is nog steeds een 360-gradenaanpak nodig. Voorgestelde oplossingen omvatten centrale politieke coördinatie, bewustmakingscampagnes, het verbeteren van cybervaardigheden en het stimuleren van bedrijven om te investeren in cyberbeveiliging. Samenwerking op meerdere niveaus en publiek-private partnerschappen zijn cruciaal voor het creëren van een veiligere online omgeving.

3. Regelgevend en investeringsvriendelijk kader

De internetsector vraagt een fundamentele herbeoordeling van het regelgevend kader tot een echt investeringsvriendelijk kader, met wetgeving die geharmoniseerd is tussen de EU en de lidstaten, maar ook intern binnen België (federaal, regionaal en lokaal). De veelheid aan verordeningen en richtlijnen, gecombineerd met nationale maatregelen, creëert een complexe omgeving. Om dit aan te pakken roept ISPA op tot een periode van "stop and think" voor regelgevende initiatieven, om een grondige herbeoordeling van de regels mogelijk te maken, wat moet leiden tot vereenvoudiging. Een duidelijk kader dat is afgestemd op de EU-normen, harmonisatie binnen België en een meer investeringsvriendelijke fiscale structuur worden voorgesteld om de groei van de digitale en telecommunicatiesector te ondersteunen. Voor een doeltreffende toewijzing van middelen is het essentieel dat stakeholders zich beter bewust zijn van het EU-beleid.

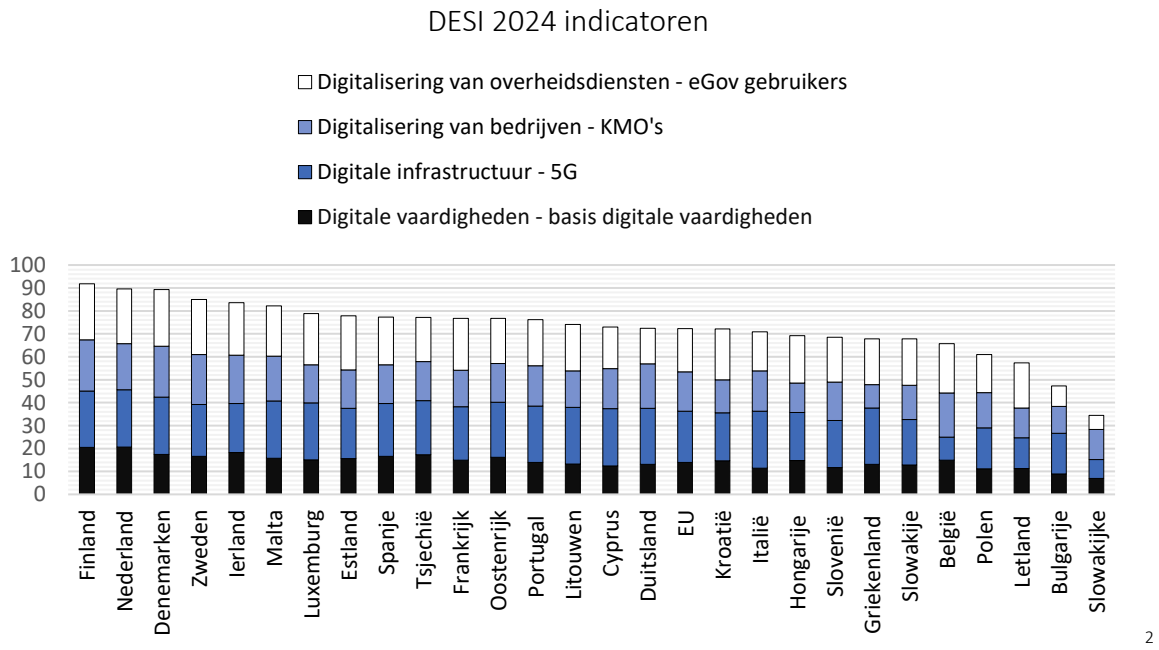
1. Bevorderen van verantwoord gebruik van internet en omarmen van innovatie

Context

Het Digital Decade Country Report[1], een jaarlijkse publicatie van de Europese Commissie, geeft een volledige beoordeling van de digitale prestaties van een land op basis van vier indicatoren: digitale vaardigheden, digitale infrastructuur, digitale transformatie van bedrijven en digitalisering van overheidsdiensten (zie figuur 1).

In de laatste editie van dit rapport scoort België op verschillende van deze indicatoren onder het EU-gemiddelde. Deze ontnuchterende realiteit benadrukt de nood aan digitale groei in ons land, zowel op individueel als op maatschappelijk niveau. Innovatie omarmen en ervoor zorgen dat iedereen de digitale vooruitgang kan bijbenen, is een cruciale stap naar duurzame digitale groei.

Figuur 1: DESI 2024 Indicatoren



[2]

Bron: DESI 2024 dashboard voor de Digital Decade

Probleem

Digitale inclusie betekent dat elk individu, ongeacht leeftijd, geslacht of socio-economische achtergrond, volledig kan deelnemen aan de digitale samenleving. België heeft echter een achterstand op het gebied van digitale vaardigheden: slechts 59% van de Belgische burgers beschikt over digitale basisvaardigheden, terwijl nauwelijks 28% van de burgers over digitale vaardigheden beschikt die hoger zijn dan de basisvaardigheden.

Deze **kloof** verhindert mensen uit potentieel kwetsbare groepen zoals ouderen, mensen met een laag inkomen en mensen met een migratieachtergrond om volledig deel te nemen aan de digitale samenleving, aangezien het hun toegang tot informatie, kansen op werk en sociale betrokkenheid zou

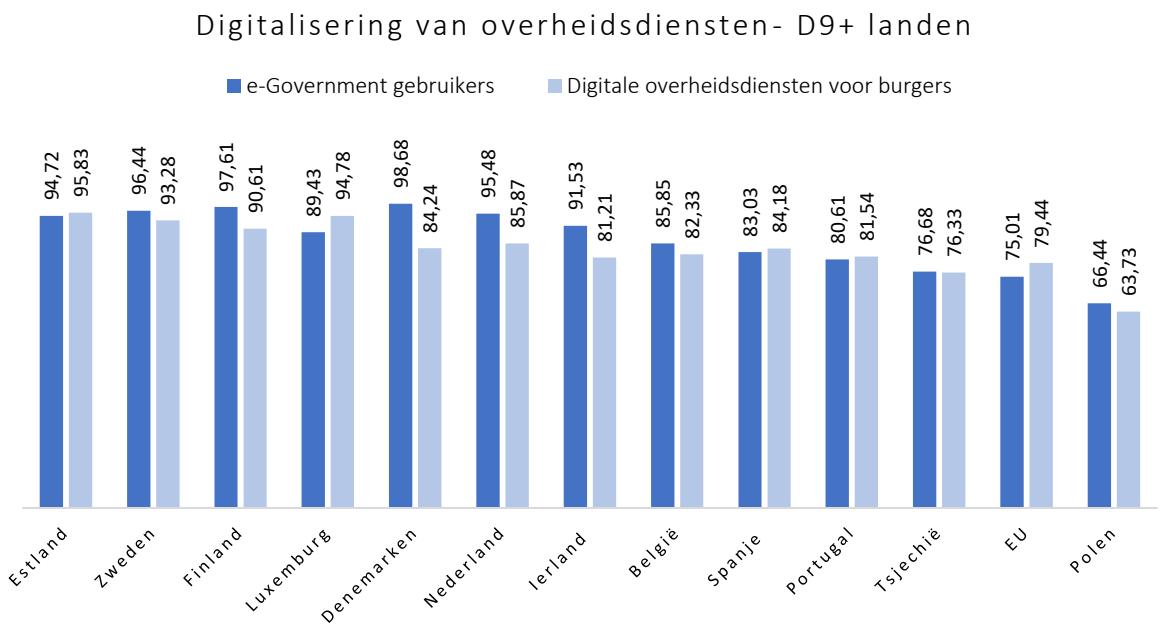
[1] De vorige naam van deze index was DESI – link: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports .
[2] DESI 2024 dashboard voor de Digital Decade – link: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts.

kunnen beperken. Deze kloof versterkt bestaande sociale ongelijkheden en plaatst een groep Belgische burgers in een nadelige positie.

Vandaag bestaan er al verschillende initiatieven om de digitale geletterdheid te verbeteren, zowel van publieke als van private spelers, zoals de digitale campus BeCentral[3], DigiSkills Belgium[4], de Digitall coalitie[5], de Vlaamse Digibanken[6], en de UpSkills Wallonia strategie[7]. ISPA steunt en juicht deze initiatieven toe, aangezien ze zeer effectief kunnen zijn in het bijscholen van volwassenen. Ze worden echter vaak door verschillende overheidsniveaus geïnitieerd, dus ons land zou **baat hebben bij een coherente strategie** en campagne om burgers voldoende bewust te maken van de verschillende opties.

De **overheid** heeft hier ook een belangrijke rol te spelen, aangezien zij het goede **voorbeeld** dient te geven aan haar burgers. België, met een indrukwekkend 85% gebruik van e-overheidsdiensten, is een noemenswaardig voorbeeld van digitale vooruitgang. Een kritische blik onthult echter een aarzeling binnen de overheid om volledig gebruik te maken van geavanceerde technologieën in vergelijking met andere D9+ landen, zoals blijkt uit onderstaande figuur. Deze aarzeling om te innoveren belemmert niet alleen de efficiëntie, maar zorgt er ook voor dat burgers niet het goede voorbeeld kunnen geven. Het gebruik van cloud-technologie en het benutten van de mogelijkheden van artificiële intelligentie kunnen de modernisering van overheidsdiensten stimuleren.

Figure 2: Digitalisering van overheidsdiensten – D9+ landen



Bron: DESI 2024 dashboard voor de Digital Decade

Voorgestelde oplossingen

Digitale hulpmiddelen in het onderwijs – Onderwijs moet een centrale rol spelen bij het verbeteren van digitale vaardigheden. Hoewel het gebruik van digitale hulpmiddelen geen doel op zich is, zorgt de vroege introductie van deze hulpmiddelen bij kinderen er niet alleen voor dat hun leerervaring wordt

[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/.

aangepast, maar maakt hen ook vertrouwd met digitale technologie, waardoor de digitale kloof wordt dichtgereden. Door digitale hulpmiddelen in het leren te integreren, kunnen kinderen hun onderwijservaring verbeteren, kunnen de leesvaardigheden van anderstalige leerlingen vooruitgaan en kan worden bijgedragen aan een effectiever onderwijssysteem in het algemeen.

Focus op bijscholingsinitiatieven en levenslang leren – ISPA benadrukt ook het vitale belang van initiatieven op het gebied van volwasseneneducatie. Aan de ene kant vragen we voor een goed gestructureerde strategie voor de bijscholing van potentieel kwetsbare groepen. Dit zorgt ervoor dat deze individuen niet uitgesloten worden in de gedigitaliseerde gemeenschap, terwijl het ook hun opties op de arbeidsmarkt vergroot, gezien het nijpende tekort aan ICT-specialisten. Hoewel het van cruciaal belang is om mensen betere hulpmiddelen te geven om te navigeren in een steeds groter wordende digitale samenleving, moeten er nog steeds alternatieve opties worden aangeboden om te blijven werken aan een evenwichtig en inclusief maatschappelijk kader. Het aanbieden van online overheidsdiensten is bijvoorbeeld noodzakelijk in een moderne samenleving, maar mensen moeten nog steeds de mogelijkheid hebben om een persoonlijke afspraak te maken met een ambtenaar.

Aan de andere kant steunt ISPA de inspanningen die worden geleverd op het vlak van levenslang leren (bv. op Vlaams niveau[8]) omdat het ertoe bijdraagt dat individuen zich kunnen aanpassen aan evoluerende technologische landschappen. De sector stelt voor om een brede sensibiliseringscampagne op te zetten om de voordelen en de beschikbaarheid van levenslang leren te promoten.

Publiek-private partnerschappen – Samenwerking met de private sector is essentieel om de doelstellingen op het gebied van digitale vaardigheden te halen. Bedrijven beschikken over de expertise en de nieuwste technologieën om overheden en onderwijsstructuren te ondersteunen bij het succesvol ontwikkelen van een sterke strategie voor digitale vaardigheden. De sector dringt er bij de wetgever op aan om een goed werkend programma uit te werken voor structurele partnerschappen tussen de publieke en private sector om de digitale vaardigheden te verbeteren.

Gecoördineerde samenwerking op meerdere niveaus – ISPA steunt bestaande initiatieven die zich inzetten om digitale geletterdheid te verbeteren. Wij geloven echter dat die initiatieven erin slagen om hun volledige potentieel te bereiken in het beïnvloeden van de samenleving vanwege hun gefragmenteerde aard. Daarom ondersteunen wij een constante kennisuitwisseling tussen verschillende benaderingen en de ontwikkeling van een gecoördineerde campagne om burgers effectiever te bereiken.

Performante internetinfrastructuur – Er is een groeiende vraag naar digitale diensten. Om aan deze vraag te voldoen en de succesvolle digitale transformatie van zowel publieke als private spelers te garanderen, moet een strategische focus op robuuste internetinfrastructuur, inclusief de uitrol van Gigabitnetwerken, prioriteit krijgen. De sector pleit voor maatregelen om de uitrol van deze infrastructuur te versnellen en te vergemakkelijken, en voor meer middelen om betrouwbare connectiviteit te garanderen, vooral in afgelegen gebieden, zodat elke burger actief kan deelnemen aan het Digitale Decennium.

Een publieke sector die het goede voorbeeld geeft – Om de voorzichtige aanpak van nieuwe technologieën door de publieke sector aan te pakken, kan België het goede voorbeeld geven. Door te pleiten voor een doortastender gebruik van technologische vooruitgang, vooral op gebieden zoals cloud computing en artificiële intelligentie, kan de overheid niet alleen overheidsdiensten moderniseren,

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

maar ook burgers en organisaties een overtuigend voorbeeld geven om te volgen. Dit gaat verder dan technologische vooruitgang; het stelt een norm voor vooruitstrevend bestuur en bevordert een cultuur van innovatie en efficiëntie die aansluit bij de digitale behoeften van de bevolking. Daarom verwelkomt en stimuleert ISPA de ontwikkeling van een cloud-first-beleid voor de publieke sector. [9]

2. Veiliger internet

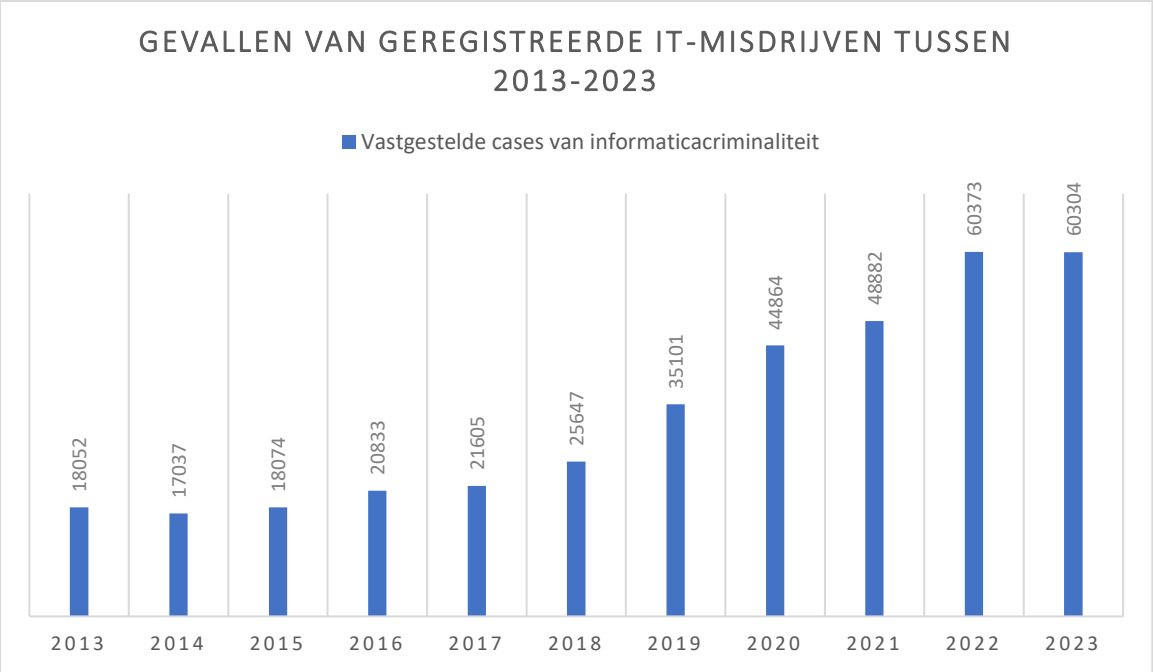
Context

De oorlog in Oekraïne en de aanhoudende cyberaanvallen op Belgische entiteiten hebben de urgentie van cyberbeveiligingsmaatregelen nog verhoogd. Naast deze onmiddellijke zorgen zijn het aanpakken van illegale online inhoud en het zorgen voor een veilige digitale ruimte voor jongeren cruciale aspecten van het bevorderen van een veilige internetomgeving. Phishing, internetfraude, cyberaanvallen en de verspreiding van illegale online inhoud hebben het vertrouwen van burgers, bedrijven en overheden in de veiligheid van het internet aangetast. Deze erosie van vertrouwen benadrukt de noodzaak om samen te werken met belanghebbenden en overheden om te zorgen voor een veilige internetomgeving die het vertrouwen van gebruikers wint.

Naast het versterken van de inspanningen op het gebied van cyberveiligheid is het van vitaal belang om het probleem van illegale online inhoud aan te pakken, met name inhoud die verband houdt met de uitbuiting van kinderen. Het handhaven van ethische normen en het beschermen van kwetsbare internetgebruikers zijn dwingende doelstellingen. Naast bestaande initiatieven zoals leeftijdsgebonden inhoudfilters, educatieve programma's en bevordering van verantwoordelijk online gedrag, blijft een aanpasbaar privacy- en beveiligingsbeleid van cruciaal belang. Deze proactieve maatregelen bevorderen een veilige online omgeving en behouden de maatschappelijke en economische waarde van het internet door de nadruk te leggen op verantwoordelijke praktijken binnen het online ecosysteem.

[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.

Figuur 3: Gevallen van geregistreerde IT-misdrijven tussen 2013-2023



Bron: Politie criminaliteitsstatistieken 2013-2023, Federale Politie

Probleem

Een **versnipperde verdeling van bevoegdheden** op het vlak van cyberbeveiliging en digitale thema's in bredere zin maken het moeilijk om een efficiënt gecoördineerd cyberbeveiliging- of zelfs internetbeleid uit te bouwen. Dit maakt het des te gemakkelijker voor hackers om hun gang te gaan in de Belgische digitale sfeer.

Computercriminaliteit stijgt al jaren, van 18 074 gevallen in 2015 tot 60 373 in 2022, zoals geregistreerd door de federale politie. Hoewel dat aantal in 2023 stagneerde (60 304), is er duidelijk sprake van een toenemende en zorgwekkende trend op het gebied van internetveiligheid (figuur 3).[10]

Een ander voortdurend probleem is de uitdaging om **illegale online inhoud** en **wangedrag** aan te pakken, waaronder de verspreiding van terroristische inhoud, gevallen van seksueel misbruik van kinderen, illegale streaming en incidenten van grooming of sextortion. Dit veelzijdige probleem vormt een aanzienlijke bedreiging voor de online veiligheid en privacy, met name voor (jonge) kinderen.

Cyberbeveiligingsvaardigheden zijn van het grootste belang voor internetveiligheid omdat elke internetgebruiker een verantwoordelijkheid draagt in een goed functionerend cyberbeveiligingssysteem. In totaal heeft slechts 39% van de Belgen een bovengemiddeld niveau van cybervaardigheden, terwijl 26% een basiskennis heeft en 28% helemaal geen cybervaardigheden heeft (opmerking: 9% maakt geen gebruik van het internet). [11] Dit betekent dat een vierde van de bevolking van ons land niet is uitgerust met de juiste kennis om hun gegevens en zichzelf online te beveiligen. Deze problemen passen in de bredere context van het gebrek aan digitale vaardigheden in België, zoals eerder vermeld in dit document.

[10] Politiële criminaliteitsstatistieken 2013-2022, Federale Politie.
[11] Statbel, digital skills 2021 – Safety.

Niet alleen burgers, maar ook **bedrijven** hebben een goed begrip nodig van het implementeren van de juiste en gepaste cyberbeveiligingspraktijken. Hiervoor moeten ze zich meer bewust worden van het belang ervan en de juiste mensen aantrekken. Uit een onderzoek van Agoria en Cevora[12] blijkt dat er veel vraag is naar het profiel van een **cyberbeveiligingsexpert** in Belgische bedrijven, maar dat het voor veel van hen moeilijk is om het juiste profiel aan te trekken.

Daar komt nog bij dat de deadline voor naleving van de **NIS 2-richtlijn**[13] snel nadert. Naar schatting zullen tegen 18 oktober 2024 ongeveer 3000 bedrijven in België de juiste maatregelen moeten nemen om te voldoen aan de nieuwe regels. Deze deadline nadert snel en het bewustzijn is nog niet waar het zou moeten zijn.

Voorgestelde oplossingen

Centrale politieke coördinatie van intern gerelateerd beleid – Het probleem van de gedecentraliseerde coördinatie van het internetbeleid op federaal niveau moet worden aangepakt. Met een steeds toenemende complexiteit in het digitale, telecom- en cyberbeveiligingsbeleid, en een steeds grotere verwevenheid van de internetsector, is het cruciaal dat al deze aspecten op een gecentraliseerde manier worden geregeld. Idealiter betekent dit dat er één minister is, bevoegd voor al deze federale bevoegdheidsdomeinen. Deze minister heeft dan een mandaat om brede en horizontale wetgeving en beleidslijnen voor te stellen, die verder reiken dan de traditionele verdeling tussen verschillende portefeuilles van die federale bevoegdheden. ISPA gelooft dat het combineren van het telecommunicatie-, cyberbeveiliging- en digitaliseringsbeleid onder één minister gunstig zou zijn voor het realiseren van een veiliger internet.

Investeren in bewustzijn en cyberveiligheid – Verder investeren, niet alleen in programma's die de Belgische cyberveiligheidspositie verhogen, maar ook in algemeen bewustzijn over het belang van correct gebruik en veilig gebruik van het internet, zijn cruciale bouwstenen voor het behoud van een veiliger internet. Dit geldt niet alleen voor de publieke sector, maar ook voor bedrijven en burgers.

Het verbeteren van cybervaardigheden – Om individuen en bedrijven in staat te stellen veilig en verantwoordelijk door het digitale landschap te navigeren en online risico's effectief te beperken. We verwelkomen initiatieven en missies van organisaties zoals Molengeek, BeCode, Digiskills België en anderen, die actief bijdragen aan het verbeteren van de digitale vaardigheden van iedereen die dat wil. Zoals eerder vermeld, vraagt onze sector echter om een constante uitwisseling tussen de verschillende bestaande benaderingen. Er is een meer coherente strategie nodig om burgers de nodige tools aan te bieden om cyberrisico's te herkennen en ermee om te gaan.

Het bewustzijn van bedrijven verhogen – Het belang van een goede cyberbeveiligingshouding in bedrijven in België moet explicieter worden gemaakt. Bedrijven moeten beter begrijpen wat de potentiële risico's zijn van niet of te weinig investeren in cyberbeveiliging, of het nu gaat om financiële, operationele of reputatierisico's. De wetgever kan hierop anticiperen door op deze risico's te wijzen, maar ook door dit te stimuleren via een activerend regelgevend kader, met een focus op proactieve in plaats van reactieve maatregelen. Bijvoorbeeld, de kosten die bedrijven maken als ze slachtoffer worden van een cyberaanval en ransomware moeten betalen om hun datasystemen te bevrijden, kunnen volgens het huidige belastingregime worden beschouwd als een aftrekbare beroepskost. Een dergelijke belastingregeling is niet stimulerend en ondermijnt de bereidheid van bedrijven om te investeren. In

---

[12] Cybersecurity-expert nieuwste knelpuntberoep, Agoria, 2023 – link: https://www.agoria.be/nl/standpunten/vlaanderen/cybersecurity-expert-nieuwste-knelpuntberoep.

[13] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

plaats van het bieden van een pleister na een val, zou het doel moeten zijn om te voorkomen dat bedrijven überhaupt vallen.

Cybersecurity-experts aantrekken – Om bedrijven te helpen de juiste cyberprofielen aan te trekken, steunen wij het pleidooi van Agoria om dit toe te voegen aan de lijst van knelpuntberoepen in alle regio's in België. Ondanks de grote vraag van bedrijven is dit nog niet het geval op noch de lijst van knelpuntberoepen van VDAB, noch Le Forem of Actiris.

End-to-end encryptie (E2EE) – Het beschermen van E2EE is van vitaal belang om de privacy en veiligheid van gebruikersgegevens in online diensten te garanderen, een betrouwbare internetinfrastructuur op te zetten die het privéleven van gebruikers respecteert en zowel persoonlijke als professionele communicatie beschermt tegen cyberbedreigingen.

Neem bijvoorbeeld online bankieren: veel apps voor mobiel bankieren maken gebruik van E2EE om veilige communicatie te garanderen tussen het apparaat van de gebruiker en de servers van de bank. Deze versleuteling beschermt gevoelige informatie zoals inloggegevens, rekeninggegevens en transactiegegevens tegen onderschepping of toegang door onbevoegden. E2EE beschermt ook gegevens die we opslaan op verschillende clouddiensten, we kunnen op een veilige manier online winkelen en het zorgt ervoor dat gevoelige gezondheidsinformatie beschermd wordt op het gebied van telegeneeskunde of op telegezondheidsplatforms. ISPA vraagt de wetgever daarom om in de toekomst geen initiatieven te nemen die E2EE ondermijnen in plaats van beschermen.

Meerlagige aanpak – Om het probleem van ongepaste online inhoud of gedrag effectief aan te pakken, is een gezamenlijke en meervoudige aanpak essentieel. Ten eerste is het van cruciaal belang om de proactieve inspanningen van onze leden te erkennen, die een essentiële rol spelen in het helpen van hun klanten bij het navigeren door en het aanpakken van deze uitdagingen.

De implementatie van de digitaledienstenverordening (Digital Services Act/DSA)[14] en de lopende discussies over het voorstel voor een CSAM-verordening[15] op EU-niveau zijn positieve stappen in de richting van maatregelen. Bij ISPA geloven we dat het EU-niveau het best uitgerust is om deze grensoverschrijdende kwestie aan te pakken.

Gebruik van de D9+ Groep – Onze sector zou het belang van de D9+ Ministeriële Groep moeten erkennen en de digitale ministers van deze kleine en middelgrote landen actief moeten aanmoedigen om zich aan te sluiten bij EU-beleidsinitiatieven en een voortrekkersrol te spelen in de digitale transitie. Via de D9+ Groep kan België een leidende rol spelen in het bevorderen van de digitale interne markt, wat van fundamenteel belang is voor de open economie van ons land.

Op nationaal niveau pleiten we voor een complementaire 360-graden aanpak, waarbij de rol van verschillende stakeholders wordt erkend, waaronder internet service providers, OTT's, overheidsinstanties en NGO's zoals Child Focus. Met name het prijzenswaardige werk van Child Focus op het gebied van zowel voorlichting als preventie van online bedreigingen, vooral voor jonge mensen, verdient erkenning. Hun inspanningen dragen aanzienlijk bij aan het creëren van een veiligere digitale omgeving, en we moedigen samenwerkingsinitiatieven aan die hun impact versterken. Door deze gezamenlijke inspanningen willen wij een alomvattende en samenhangende strategie bevorderen die de veelzijdige uitdagingen van illegale online inhoud en wangedrag aanpakt, met een bijzondere focus op de bescherming van de veiligheid en privacy van (jonge) kinderen. ISPA staat open voor elke dialoog

[14] Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening).
[15] Voorstel voor een Verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen.

met de betrokken belanghebbenden over oplossingen om van het internet een veiligere omgeving te maken.

Transparante en open raadplegingen – Tijdens de omzetting van de NIS 2-richtlijn heeft het Centrum voor Cyberbeveiliging (CCB) een openbare raadpleging gehouden en input van belanghebbenden verzameld. Als sector steunen wij dit soort processen en moedigen wij de wetgever aan om er een gewoonte van te maken om belanghebbenden- die de gevolgen ondervinden van een specifiek stuk wetgeving- bij het wetgevingsproces te betrekken. Bovendien moedigen wij het sterk aan om de sector er zo vroeg mogelijk te consulteren. En wat nog belangrijker is, we vragen dat deze processen op een transparante en open manier worden uitgevoerd, zodat er gelijke kansen zijn voor alle belanghebbenden die bij het proces betrokken willen worden.

Publiek-private partnerschappen – Het opbouwen van sterke publiek-private partnerschappen tussen ISP's, OTT's, hostingproviders en overheden vergemakkelijkt het delen van informatie en versterkt de collectieve reactie op online fraude. Het bevorderen van open en transparante samenwerking tussen meerdere belanghebbenden bevordert ook een holistische aanpak van cyberbedreigingen, waarbij de expertise en middelen van overheden, industrie en maatschappelijke organisaties worden benut. Het Belgian Anti Phishing Shield (BAPS) is een uitstekend voorbeeld van hoe de directe betrokkenheid van ISP's bij een initiatief van het CCB actief bijdraagt tot een veiliger internet.

3. Regelgevend en investeringsvriendelijk kader

Context

De internetsector vraagt een fundamentele herbeoordeling van het regelgevend kader tot een echt investeringsvriendelijk kader, met wetgeving die geharmoniseerd is tussen de EU en de lidstaten, maar ook intern binnen België (federaal, regionaal en lokaal). Dit vraagt om een sterk bewustzijn van de impact van het EU-beleid in de digitale sector, alsook om onze middelen toe te wijzen aan maatregelen die een toegevoegde waarde hebben. Op deze manier kan de digitale en telecommunicatie-industrie echt een innovatiestimulerende sector zijn.

Probleem

De internetsector wordt voor een groot deel gereguleerd op EU-niveau. Zoals blijkt uit de bijgevoegde tabel (zie Bijlage 1), hebben de voorbije Europese mandaten een **brede waaier** aan initiatieven opgeleverd, onder andere op het gebied van privacy, gegevensbescherming, cyberbeveiliging, *content moderation*[16], enz. De implementatie van deze initiatieven vereist aanzienlijke middelen voor bedrijven, zeker gezien hoe snel de sector evolueert en hoe snel aanpassing aan nieuwe technologieën nodig is.

Soms zien we echter dat hier nationale, regionale of communautaire maatregelen bovenop komen, vaak voor zaken die al op EU-niveau geregeld zijn. Gezien het enorme aantal EU-initiatieven, creëert dit alleen maar een **onduidelijker regelgevend kader** en bedreigt het de harmonisatie van de interne markt.

Bovendien versterkt het afwijken van de door de EU gestelde normen deze fragmentatie alleen maar., vooral wanneer de implementatie ook nog eens verschilt tussen de verschillende regio's in België.

Tot slot moet ons land een **investeringsvriendelijkere omgeving** creëren. Bedrijven worden niet alleen ontmoedigd om te investeren door het hierboven vermelde gefragmenteerde of verouderde regelgevende kader, maar ook het huidige belastingsysteem kan problemen opleveren. Verschillende gemeenten belasten zendmasten of vaste netwerken en dringen aan op een retributie voor de uitrol

[16] Het beheren van online inhoud, of 'content'.

van glasvezel, wat een negatieve impact heeft op het investeringsklimaat in België en ondernemerschap en innovatie belemmert.

Voorgestelde oplossingen

Focus op een grondige herbeoordeling van bestaande regelgevende initiatieven – Onze sector vraagt dat de volgende EU-legislatuur zich concentreert op de implementatie en vereenvoudiging van de bestaande regels. Zoals de bijgevoegde tabel weergeeft, hebben de afgelopen twee Europese legislaturen een breed scala aan initiatieven voor de digitale en telecommunicatiesector voortgebracht. De sector heeft tijd nodig voor de herbeoordeling van de huidige initiatieven.

Duidelijk kader, met bewustzijn van impact EU-beleid – Onze beleidsmakers en stakeholders zouden een sterkere "EU-reflex" moeten hebben. Als we goed weten welke en hoe maatregelen op EU-niveau worden geregeld en wat het effect daarvan is op de Belgische markt, kunnen middelen adequater en efficiënter worden geïnvesteerd in maatregelen die het EU-niveau aanvullen.

Oproep tegen gold-plating – Om een stabiel, complementair regelgevend kader te hebben, wordt geadviseerd om niet af te wijken van de vereisten die door de EU zijn vastgesteld. Uitbreiding van de bevoegdheden van richtlijnen bij de omzetting ervan in nationale wetgeving moet worden vermeden, om een geharmoniseerd digitaal ecosysteem binnen de interne markt te creëren.

Geharmoniseerd Belgisch kader – Onze complexe staatsstructuur kan vaak een belemmerende factor zijn voor een evenwichtig en gecoördineerd beleid. De sector moedigt daarom een effectieve coördinatie tussen de verschillende regio's aan, in het bijzonder bij de implementatie van Europese wetgeving.

Voorbeelden:

- België is het tweede Europese land dat een herstelbaarheidsindex invoert,[17] als onderdeel van het federale actieplan voor de circulaire economie. Aangezien een Europese herstelbaarheidsindex momenteel ook in de maak is met het voorstel van een richtlijn over gemeenschappelijke regels ter bevordering van de herstelling van goederen,[18] dreigt de vroegtijdige Belgische regelgeving af te wijken van de aanpak die op EU-niveau is voorzien en de interne markt te versnipperen. Overweging 2 van de voorgestelde richtlijn vermeldt zelfs dat "verschillende dwingende nationale regels op dit gebied daadwerkelijke of potentiële belemmeringen vormen voor de werking van de interne markt en een negatieve invloed hebben op grensoverschrijdende transacties van marktdeelnemers die op die markt actief zijn".
- De Digital Services Act voorziet in uniforme regels voor een veilige en vertrouwde online omgeving in de digitale eengemaakte markt, gericht op online intermediaire diensten. De regulering van platformen is volledig voorzien in de DSA, wat betekent dat België zich nu moet richten op de noodzakelijke afstemming tussen de verschillende bevoegde autoriteiten voor de uitvoering van de DSA, op het bieden van voldoende transparantie over de reikwijdte van de verschillende betrokken autoriteiten en, ten slotte, op het voorzien van onze coördinator digitale diensten van de nodige instrumenten om zijn taak zo efficiënt mogelijk uit te voeren. Dit omvat ook het verhogen van het bewustzijn, het mogelijk maken van begeleiding en het focussen op preventie met betrekking tot de DSA, de impact ervan en de rechten en plichten

[17] Persbericht Minister Khattabi 2 Juni 2023: België wordt het tweede Europese land dat een herstelbaarheidsindex invoert– link: https://khattabi.belgium.be/nl/pb-repairindex.

[18] Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende gemeenschappelijke regels ter bevordering van de reparatie van goederen en tot wijziging van Verordening (EU) 2017/2394 en de Richtlijnen (EU) 2019/771 en (EU) 2020/1828.

die het creëert. Voor de bescherming van kinderen online kan ons land bijvoorbeeld een coördinerende rol toekennen aan Child Focus.

Investeringsvriendelijk kader – Ten slotte moeten onnodige fiscale lasten worden vermeden om een investeringsvriendelijk kader te versterken. Dubbele belasting en belasting op infrastructuur, zoals zendmasten en pylonen[19] of vaste netwerken, moet worden vermeden. Bovendien moet de vraag van verschillende steden en gemeenten om een retributie voor de uitrol van glasvezel worden tegengegaan.

[19] In het kader van het Giga Région-programma van Digitaal Wallonië werd een nieuw Tax on Pylons-akkoord (3de editie) gesloten tussen de telecomoperatoren en Wallonië. In het akkoord verbindt Wallonië zich ertoe om de afschaffing van de gewestelijke belastingen en de aanbeveling aan provincies en gemeenten om geen belastingen op masten, pylonen en antennes te heffen, te behouden in ruil voor investeringen in een betere connectiviteit. We zouden dergelijke maatregelen graag op het hele grondgebied zien, aangezien verschillende Vlaamse gemeenten momenteel nog steeds belastingen op pylonen heffen. – link: https://www.digitalwallonia.be/fr/publications/giga-region-3eme-accord-top-operateurs/.

Bijlage 1: overzicht van recente EU initiatieven (niet-exhaustief)

	Aangenomen	Hangende	(Mogelijk) nieuwe initiatieven
Onderzoek & Innovatie	• Verordening tot oprichting van het programma Digitaal Europa • Verordening tot vaststelling van Horizon Europa		
Industiebeleid	• Verordening tot oprichting van de Gemeenschappelijke Onderneming Europese high-performance computing • Verordening tot vaststelling van het InvestEU-programma • Besluit tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030 • Europese chipverordening • Verordening tot oprichting van het platform voor strategische technologieën voor Europa (STEP) • Verordening voor nettonulindustrie		
Connectiviteit	• Richtlijn ter verlaging van kosten van de aanleg van elektronische communicatienetwerken met hoge snelheid • Verordening open internettoegang • Europees wetboek voor elektronische communicatie • Roaming verordening • Verordening tot vaststelling van het programma voor beveiligde connectiviteit • Gigabitinfrastructuurverordening		• Verordening digitale netwerken
Gegevensbescherming & Privacy	• Verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens • Richtlijn inzake open data • Datagovernanceverordening • Verordening Interoperabel Europa • Dataverordening	• Verordening privacy en elektronische communicatie • Verordening betreffende de Europese ruimte voor gezondsheidsgegevens • Verordening handhaving AVG	• GreenData4All
Cyberbeveiliging	• Cyberbeveiligingsverordening • NIS 2-richtlijn • Verordening tot oprichting van het Europees kenniscentrum cyberbeveiliging	• Verordening cyberweerbaarheid • Verordening cybersolidariteit	
Handhaving	• Verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud • Tijdelijke CSAM-verordening • Verordening elektronisch bewijsmateriaal	• Nieuwe CSAM-verordening	
Veiligheid	• eIDAS-verordening • Verordening tot oprichting van één digitale toegangspoort • AI-verordening	• Richtlijn AI aansprakelijkheid	
E-commerce & Consumentenbescherming	• Richtlijn elektronische handel • Richtlijn consumentenrechten • GeoBlocking-verordening • Richtlijn voor de levering van digitale inhoud en digitale diensten • Digitaledienstenverordening & digitalemarktenverordening • Verordening betreffende transparantie en gerichte politieke reclame	• Richtlijn ter bevordering van reparatie van goederen	• Multimodale digitale mobiliteitsdiensten
Media	• Richtlijn naburige rechten in de informatiemaatschappij • Richtlijn audiovisuele mediadiensten • Richtlijn auteursrechten • Europese verordening mediavrijheid		
Financiën	• Richtlijn betalingsdiensten 2 (PSD2) • Verordening digitale operationele weerbaarheid voor financiële sector	• Richtlijn betalingsdiensten 3 (PSD3) • Verordening betalingsdiensten (PSR) • Verordening betreffende de vaststelling van de digitale euro	

Bron: Bruegel factsheet – Overzicht van EU-wetgeving in de digitale sector, 16 november 2023