ISPA BELGIQUE

DOCUMENT DE VISION

JUILLET 2024

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

Introduction

En tant qu'association belge des fournisseurs de services internet, ISPA Belgique rassemble les différents acteurs du secteur internet en Belgique, y compris les entreprises qui font fonctionner internet, tels que les fournisseurs de services internet (FSI), les hébergeurs, les fournisseurs de services de cloud et les fournisseurs de contenu. L'association veille à ce que la voix de la communauté internet soit entendue et comprise afin de créer des politiques cohérentes, orientées vers l'avenir et adaptées au numérique en Belgique.

ISPA Belgique opère dans divers secteurs d'activités et vise à défendre les intérêts des entreprises du secteur internet en Belgique, dans le but de maximiser le potentiel économique et social de l'internet. Les activités de l'association se concentrent sur des thématiques telles que l'interaction entre les législations européenne et belge, la rétention de données, l'internet plus sûr et la cybersécurité, l'intelligence artificielle, la vie privée, la protection des données et la durabilité.

Résumé général

1. Stimuler l'utilisation responsable de l'internet et encourager l'innovation

La Belgique est confrontée à des défis en matière de performance numérique, se classant en dessous de la moyenne de l'UE en ce qui concerne les indicateurs clés. L'inclusion numérique est entravée par un manque de compétences numériques de base, qui affecte particulièrement les groupes vulnérables. Bien qu'il existe des initiatives louables, la gouvernance fragmentée et l'hésitation des autorités publiques à adopter des technologies de pointe entravent les progrès. Les solutions proposées comprennent l'intégration des outils numériques dans l'enseignement, des initiatives de formation continue, des partenariats public-privé et un gouvernement qui montre l'exemple pour favoriser une culture de l'innovation.

2. Un internet plus sécurisé

L'augmentation des cybermenaces et des cas de criminalité informatique souligne la nécessité d'une stratégie coordonnée en matière de cybersécurité. La fragmentation des compétences contribue à créer un environnement difficile, et la pénurie de cybercompétences au sein de la main-d'œuvre constitue un risque important. La législation sur les services numériques et la proposition de règlement CSAM au niveau de l'UE pourraient constituer des étapes positives, mais une approche à 360 degrés demeure nécessaire. Les solutions proposées impliquent une coordination politique centrale, des campagnes de sensibilisation, l'amélioration des cybercompétences et l'incitation des entreprises à investir dans la cybersécurité. La collaboration à plusieurs niveaux et les partenariats public-privé sont essentiels pour créer un environnement en ligne plus sûr.

3. Cadre réglementaire et favorable à l'investissement

Le secteur de l'internet exige une réévaluation fondamentale du cadre réglementaire pour en faire un cadre véritablement favorable à l'investissement, avec une législation harmonisée entre l'UE et les États membres, mais aussi au sein de la Belgique (au niveau fédéral, régional et local). La multitude de règlements et de directives, combinée aux mesures nationales, crée un environnement complexe. Pour y remédier, l'ISPA appelle à une période d'arrêt et de réflexion concernant les initiatives réglementaires, afin de permettre une réévaluation approfondie des règles qui devrait conduire à une simplification. Un cadre clair aligné sur les normes de l'UE, une harmonisation au sein de la Belgique et une structure fiscale plus favorable aux investissements sont proposés pour soutenir la croissance du secteur

numérique et des télécommunications. Le renforcement de la sensibilisation des parties prenantes aux politiques de l'UE est essentiel pour une allocation efficace des ressources.

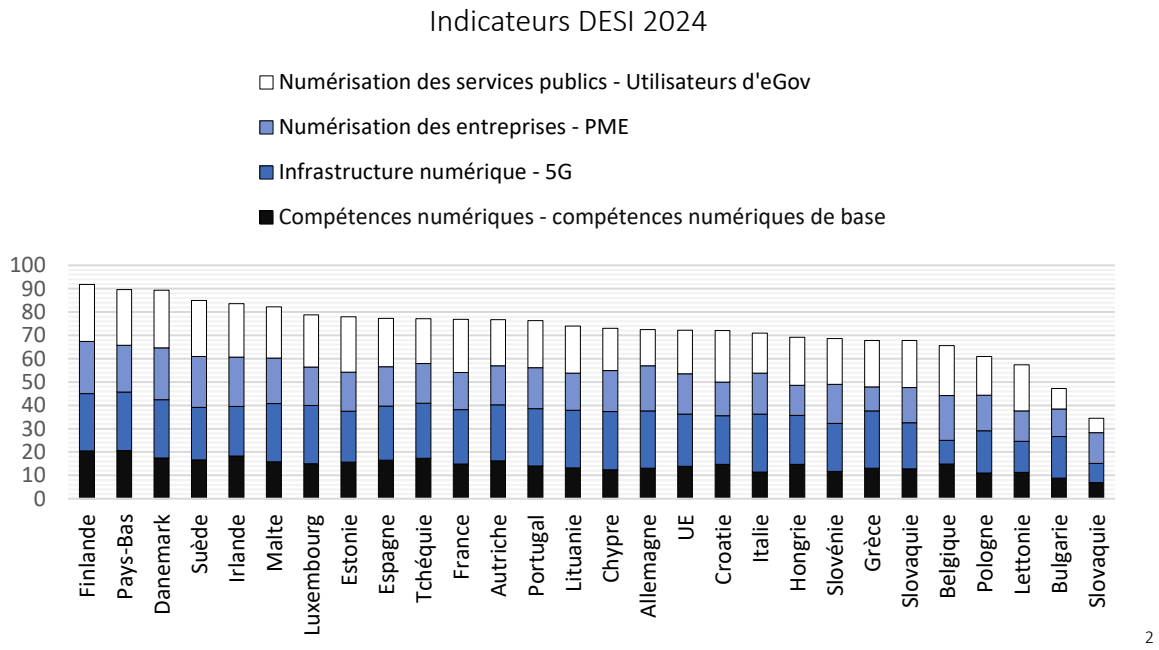
1. Stimuler l'utilisation responsable de l'internet et encourager l'innovation

Contexte

Le Rapport par pays sur la Décennie numérique[1], une publication annuelle de la Commission européenne, donne une évaluation complète des performances numériques d'un pays sur la base de quatre indicateurs : les compétences numériques, l'infrastructure numérique, la transformation numérique des entreprises et la numérisation des services publics (voir figure 1).

Dans la dernière édition de ce rapport, la Belgique se classe en dessous de la moyenne de l'UE pour plusieurs de ces indicateurs. Cette triste réalité met en évidence la nécessité d'une croissance numérique dans notre pays, tant au niveau individuel que sociétal. Adopter l'innovation et veiller à ce que chacun puisse suivre les progrès numériques représentent une étape cruciale vers une croissance numérique durable.

Figure 1 : Indicateurs DESI 2024



[2]

Source : Tableau de bord DESI 2024 pour la Décennie numérique

Problème

L'**inclusion numérique** signifie que chaque individu, indépendamment de son âge, de son sexe ou de son milieu socio-économique, peut prendre pleinement part à la société numérique. Cependant, la Belgique est à la traîne en termes de compétences numériques : seuls 59 % des citoyens belges possèdent des compétences numériques de base, tandis que 28 % à peine d'entre eux disposent de compétences numériques supérieures aux compétences de base.

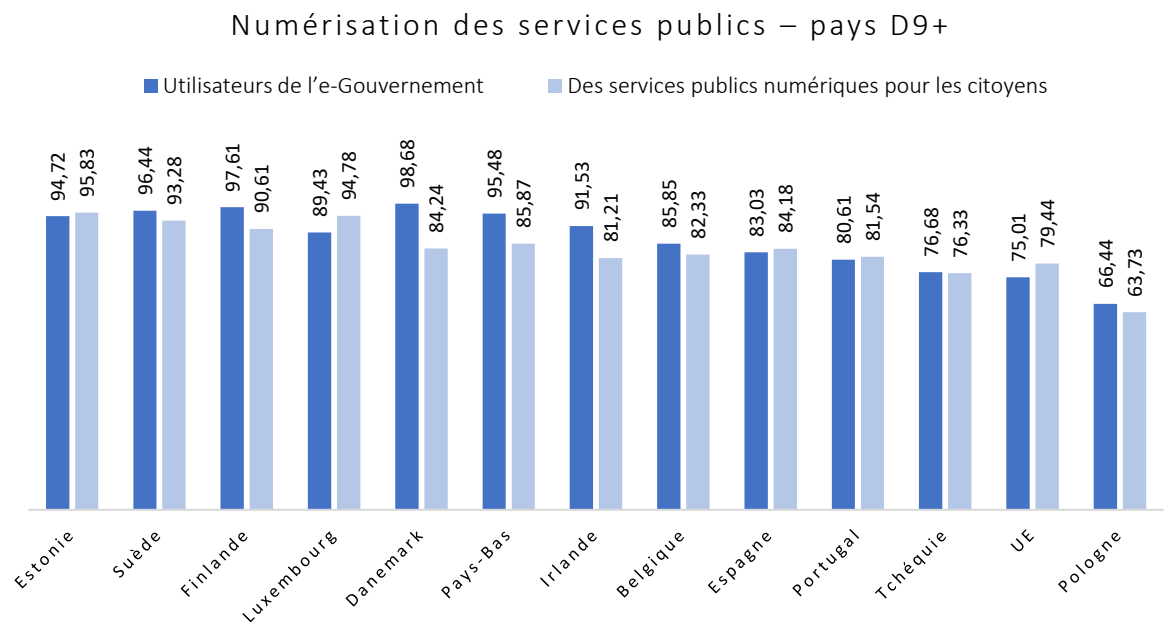
[1] L'ancien nom de cet index était DESI – lien : https://digital-strategy.ec.europa.eu/fr/library/digital-decade-2024-country-reports.
[2] Tableau de bord DESI 2024 pour la Décennie numérique- lien : https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts.

Cette **fracture** empêche les personnes appartenant à des groupes potentiellement vulnérables, les personnes âgées, les personnes à faible revenu et les personnes issues de l'immigration par exemple, de prendre pleinement part à la société numérique, car elle pourrait limiter leur accès à l'information, aux possibilités d'emploi et à l'engagement social. Cette fracture renforce ainsi les inégalités sociales existantes et désavantage un groupe de citoyens belges.

Aujourd'hui, il existe déjà plusieurs initiatives visant à améliorer la culture numérique, émanant tant d'acteurs publics que privés, comme le campus numérique BeCentral[3], DigiSkills Belgium[4], la coalition Digitall[5], les Digibanken flamandes[6] et la stratégie UpSkills Wallonia[7]. L'ISPA soutient et accueille favorablement ces initiatives, puisqu'elles peuvent être très efficaces pour le perfectionnement des adultes. Cependant, elles sont souvent initiées par différents niveaux d'autorités publiques, de sorte que notre pays **gagnerait à disposer d'une stratégie** et d'une campagne **cohérentes** pour sensibiliser suffisamment les citoyens aux différentes options.

Les **autorités publiques** ont également un rôle important à jouer dans ce domaine, car elles doivent donner le bon **exemple** à leurs citoyens. La Belgique, avec un taux impressionnant de 85 % d'utilisation des services publics en ligne, est un exemple notable de progrès numérique. Cependant, un regard critique révèle une réticence au sein des autorités publiques à utiliser pleinement les technologies avancées par rapport à d'autres pays D9+, comme le montre la figure ci-dessous. Cette réticence à innover ne nuit pas seulement à l'efficacité, mais empêche également les citoyens de donner l'exemple. L'utilisation de la technologie du cloud et l'exploitation du potentiel de l'intelligence artificielle sont susceptibles de favoriser la modernisation des services publics.

Figure 2 : Numérisation des services publics – pays D9+



Source : Tableau de bord DESI 2024 pour la Décennie numérique

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

Solutions proposées

Outils numériques dans l'enseignement – L'enseignement est appelé à jouer un rôle central dans l'amélioration des compétences numériques. Si l'utilisation d'outils numériques n'est pas une fin en soi, l'introduction précoce de ces outils auprès des enfants permet non seulement d'adapter leur expérience d'apprentissage, mais aussi de les familiariser avec la technologie numérique, réduisant ainsi la fracture numérique. L'intégration d'outils numériques dans l'apprentissage peut améliorer l'expérience éducative des enfants, faire progresser les compétences en lecture des élèves de langue maternelle étrangère et contribuer de manière générale à un système éducatif plus efficace.

Accent sur les initiatives de perfectionnement et sur l'apprentissage tout au long de la vie – L'ISPA souligne également l'importance vitale des initiatives de formation pour adultes. D'une part, nous demandons une stratégie de perfectionnement bien structurée pour les groupes potentiellement vulnérables. De la sorte, ces personnes ne seront pas exclues de la communauté numérisée, tout en augmentant leurs possibilités sur le marché de l'emploi, compte tenu de la pénurie aiguë de spécialistes des TIC. S'il est essentiel de donner aux citoyens de meilleurs outils pour naviguer dans une société de plus en plus numérique, d'autres options doivent toujours être proposées pour continuer d'œuvrer en faveur d'un cadre social équilibré et inclusif. La fourniture de services publics en ligne, par exemple, est nécessaire dans une société moderne, mais les citoyens devraient toujours avoir la possibilité de prendre rendez-vous avec un fonctionnaire en personne.

D'autre part, l'ISPA soutient les efforts fournis dans le cadre de l'apprentissage tout au long de la vie (par exemple au niveau flamand[8]), car cela aide les individus à s'adapter à l'évolution des paysages technologiques. Le secteur propose une vaste campagne de sensibilisation destinée à promouvoir les avantages et la disponibilité de l'apprentissage tout au long de la vie.

Partenariats public-privé – La collaboration avec le secteur privé est essentielle à la réalisation des objectifs en matière de compétences numériques. Les entreprises disposent de l'expertise et des technologies les plus récentes pour aider les autorités publiques et les structures éducatives à réussir l'élaboration d'une stratégie solide en matière de compétences numériques. L'industrie demande instamment au législateur d'élaborer un programme efficace de partenariats structurels entre les secteurs public et privé afin d'améliorer les compétences numériques.

Collaboration coordonnée à plusieurs niveaux – L'ISPA soutient les initiatives existantes destinées à améliorer la culture numérique. Cependant, nous pensons que ces initiatives ne parviennent pas à atteindre leur plein potentiel d'influence sur la société en raison de leur nature fragmentée. Nous soutenons dès lors un échange constant de connaissances entre les différentes approches et le développement d'une campagne coordonnée pour atteindre les citoyens plus efficacement.

Infrastructure internet performante – La demande de services numériques ne cesse de croître. Pour répondre à cette demande et assurer le succès de la transformation numérique des acteurs tant publics que privés, il faut donner la priorité à une infrastructure internet robuste, y compris le déploiement de réseaux Gigabit. Le secteur plaide en faveur de mesures visant à accélérer et à faciliter le déploiement de cette infrastructure, ainsi qu'en faveur de ressources supplémentaires destinées à garantir une connectivité fiable, en particulier dans les zones reculées, afin que chaque citoyen puisse participer activement à la Décennie numérique.

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

Un secteur public qui montre l'exemple – Pour remédier à la prudence du secteur public face aux nouvelles technologies, la Belgique peut montrer l'exemple. En préconisant une utilisation plus audacieuse des avancées technologiques, en particulier dans des domaines tels que le cloud computing et l'intelligence artificielle, les autorités publiques peuvent non seulement moderniser les services publics, mais aussi donner aux citoyens et aux organisations un exemple convaincant à suivre. Au-delà des avancées technologiques, il s'agit d'établir une norme de gouvernance progressiste et de promouvoir une culture de l'innovation et de l'efficacité correspondant aux besoins numériques de la population. C'est pourquoi l'ISPA salue et encourage le développement d'une politique « cloud-first » pour le secteur public. [9]

2. Un internet plus sécurisé

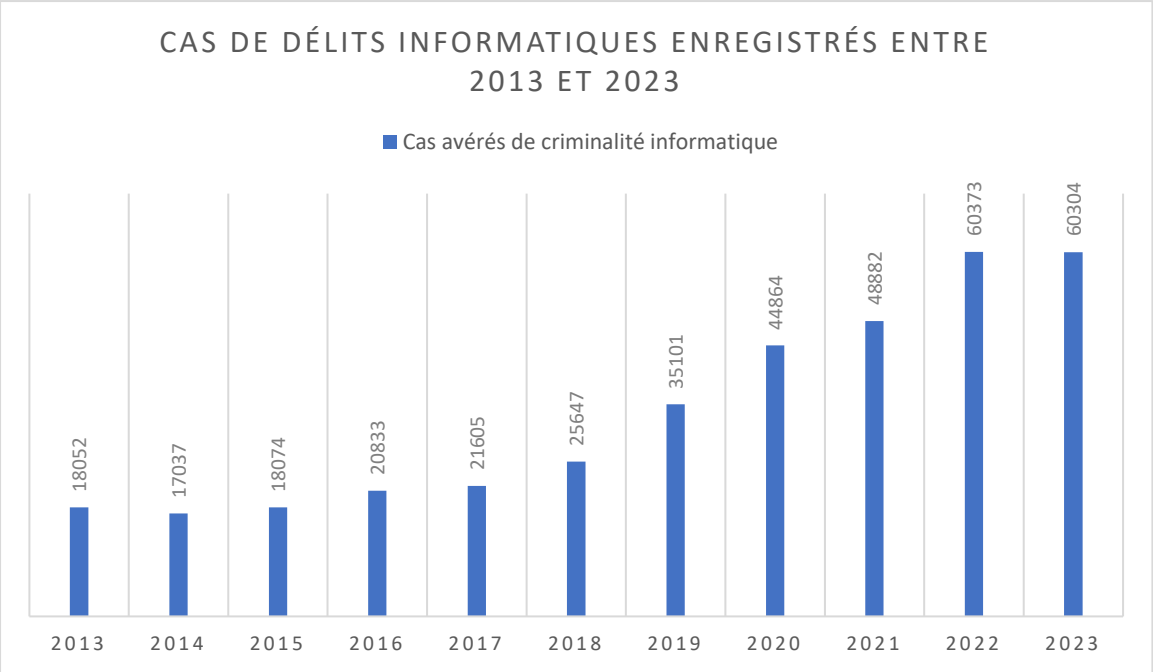
Contexte

La guerre en Ukraine et les cyberattaques constantes contre des entités belges ont encore accentué l'urgence des mesures de cybersécurité. Au-delà de ces préoccupations immédiates, la lutte contre les contenus illicites en ligne et la garantie d'un espace numérique sûr pour les jeunes sont des aspects essentiels de la promotion d'un environnement internet sécurisé. L'hameçonnage, la fraude sur l'internet, les cyberattaques et la diffusion de contenus illicites en ligne ont érodé la confiance des citoyens, des entreprises et des autorités dans la sécurité de l'internet. Cette érosion souligne la nécessité de travailler avec les parties prenantes et les autorités en vue de garantir un environnement internet sécurisé en mesure de gagner la confiance des utilisateurs.

Outre le renforcement des efforts en matière de cybersécurité, il est vital de s'attaquer au problème des contenus illicites en ligne, en particulier ceux liés à l'exploitation des enfants. Le maintien de normes éthiques et la protection des utilisateurs vulnérables d'internet sont des objectifs impératifs. Outre les initiatives existantes telles que les filtres de contenu liés à l'âge, les programmes éducatifs et la promotion d'un comportement en ligne responsable, des politiques adaptables en matière de protection de la vie privée et de sécurité demeurent cruciales. Ces mesures proactives favorisent en effet un environnement en ligne sûr et préservent la valeur sociale et économique de l'internet en mettant l'accent sur des pratiques responsables au sein de l'écosystème en ligne.

[9] Conseil des ministres du 17 mai 2024 : Plan d'action en vue de l'établissement d'un plan transversal d'adoption du cloud pour l'administration fédérale – lien : Plan d'approche en vue de l'établissement d'un plan transversal d'adoption du cloud pour l'administration fédérale | News.belgium.

Figure 3 : Cas de délits informatiques enregistrés entre 2013 et 2023



Source : Statistiques policières de criminalité 2013-2023, Police fédérale

Problème

La **répartition fragmentée des compétences** en matière de cybersécurité et, plus généralement, de thématiques numériques, complique l'élaboration d'une politique efficacement coordonnée en matière de cybersécurité ou même d'internet. Il est donc d'autant plus facile pour les pirates informatiques d'agir dans la sphère numérique belge.

La **criminalité informatique** est en hausse depuis des années, passant de 18 074 cas en 2015 à 60 373 en 2022, selon la police fédérale. Bien que ce chiffre stagne en 2023 (60 304), il existe clairement une préoccupante tendance à la hausse en matière de cybersécurité (figure 3).[10]

Autre problème récurrent, la lutte contre les **contenus** et les **comportements illicites en ligne**, notamment la diffusion de contenus terroristes, les cas d'abus sexuels infligés à des enfants, la diffusion illégale en continu et les cas de grooming ou de sextorsion. Ce problème aux multiples facettes représente une menace importante pour la sécurité et la vie privée en ligne, en particulier pour les (jeunes) enfants.

Les **compétences en matière de cybersécurité** sont d'une importance capitale pour la sécurité d'internet, car chaque utilisateur de l'internet porte une responsabilité dans le bon fonctionnement du système de cybersécurité. Dans l'ensemble, seuls 39 % des Belges ont un niveau de cybercompétences supérieur à la moyenne, tandis que 26 % possèdent des connaissances de base et 28 % n'ont aucune cybercompétence (note : 9 % n'utilisent pas l'internet).[11] Cela signifie qu'un quart de la population de notre pays ne dispose pas des connaissances nécessaires pour sécuriser ses données et sa personne en ligne. Ces problèmes s'inscrivent dans le contexte plus large du manque de compétences numériques en Belgique, comme exposé précédemment dans ce document.

[10] Statistiques policières de criminalité 2013-2022, Police fédérale.
[11] Statbel, digital skills 2021 – Safety.

Les citoyens, mais aussi les **entreprises**, doivent bien comprendre comment mettre en œuvre des pratiques de cybersécurité adéquates et appropriées. Pour ce faire, elles doivent prendre davantage conscience de l'importance de la cybersécurité et attirer les bonnes personnes. Une enquête menée par Agoria et Cefora[12] montre que les profils d'**expert en cybersécurité** sont très recherchés par les entreprises belges, mais qu'il est difficile pour nombre d'entre elles d'attirer le profil adéquat.

De plus, la date limite de mise en conformité avec la **directive SRI 2**[13] approche à grands pas. On estime que d'ici le 18 octobre 2024, environ 3 000 entreprises en Belgique devront prendre des mesures appropriées pour se conformer aux nouvelles règles. L'échéance approche à grands pas et la prise de conscience n'a pas encore eu lieu.

Solutions proposées

Coordination politique centrale de la politique liée à l'internet – Il y a lieu d'aborder le problème de la coordination décentralisée de la politique de l'internet au niveau fédéral. Les politiques en matière de numérique, de télécommunications et de cybersécurité étant de plus en plus complexes et le secteur de l'internet de plus en plus imbriqué, il est essentiel que tous ces aspects soient réglementés de manière centralisée. L'idéal serait d'avoir un seul ministre, en charge de tous ces domaines de compétence fédérale. Ce ministre aurait alors mandat pour proposer une législation et des politiques larges et horizontales dépassant la division traditionnelle entre les différents portefeuilles de ces compétences fédérales. L'ISPA estime que le regroupement des politiques de télécommunications, de cybersécurité et de numérisation sous l'égide d'un seul ministre serait bénéfique à la sécurisation de l'internet.

Investir dans la sensibilisation et la cybersécurité – Des investissements supplémentaires, non seulement dans des programmes qui renforcent la position de la Belgique en matière de cybersécurité, mais aussi dans la sensibilisation générale à l'importance d'une utilisation correcte et sûre de l'internet, sont des éléments essentiels au maintien d'un internet plus sûr. Cela concerne non seulement le secteur public, mais aussi les entreprises et les citoyens.

Améliorer les cybercompétences – Pour permettre aux particuliers et aux entreprises de naviguer dans le paysage numérique de manière sûre et responsable et de réduire efficacement les risques en ligne. Nous saluons les initiatives et les missions d'organisations telles que Molengeek, BeCode, Digiskills Belgium et d'autres, qui contribuent activement à améliorer les compétences numériques de tous ceux qui le souhaitent. Toutefois, comme nous l'avons dit, notre secteur appelle à un échange constant entre les différentes approches existantes. Une stratégie plus cohérente est nécessaire en vue de fournir aux citoyens les outils nécessaires pour reconnaître les cyberrisques et y faire face.

Sensibiliser les entreprises – L'importance d'un comportement adéquat en matière de cybersécurité dans les entreprises en Belgique doit être explicitée. Les entreprises doivent mieux comprendre les risques potentiels, qu'ils soient financiers, opérationnels ou touchent leur réputation, de ne pas investir ou de sous-investir dans la cybersécurité. Le législateur peut anticiper ces risques en les signalant, mais aussi stimuler cette prise de conscience par le biais d'un cadre réglementaire stimulant, mettant l'accent sur des mesures proactives plutôt que réactives. Par exemple, les frais encourus par les entreprises lorsqu'elles sont victimes d'une cyberattaque et doivent payer des ransomwares pour libérer leurs systèmes de données peuvent être considérés comme des frais professionnels déductibles dans le cadre

---

[12] Expert en cybersécurité, nouveau métier en pénurie, Agoria, 2023 – lien : https://www.agoria.be/fr/positionnement/flandres/expert-en-cybersecurite-nouveau-metier-en-penurie.

[13] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

du régime fiscal actuel. Ce régime n'est pas stimulant et sape la volonté des entreprises d'investir. Au lieu d'offrir un emplâtre sur une jambe de bois, l'objectif devrait être d'empêcher les entreprises de tomber dans le panneau.

Attirer des experts en cybersécurité – Afin d'aider les entreprises à attirer les profils en cybersécurité adéquats, nous soutenons le plaidoyer d'Agoria en faveur de l'ajout de ce domaine à la liste des métiers en pénurie dans toutes les régions de Belgique. Malgré la forte demande des entreprises, ce n'est pas encore le cas, ni sur la liste des métiers en pénurie du VDAB, ni sur celle du Forem ou d'Actiris.

Chiffrement de bout en bout (E2EE) – La protection de l'E2EE revêt une importance vitale pour garantir la confidentialité et la sécurité des données des utilisateurs dans les services en ligne, mettre en place une infrastructure internet fiable respectueuse de la vie privée des utilisateurs et protéger les communications personnelles et professionnelles contre les cybermenaces.

Prenons l'exemple des services bancaires en ligne : de nombreuses applications bancaires mobiles utilisent l'E2EE pour garantir une communication sécurisée entre l'appareil de l'utilisateur et les serveurs de la banque. Ce chiffrement protège les informations sensibles telles que les données de connexion, les informations de compte et les données de transaction contre l'interception ou l'accès par des personnes non autorisées. L'E2EE protège également les données que nous enregistrons sur divers services de cloud, nous permet de faire des achats en ligne en toute sécurité et garantit la protection des informations de santé sensibles sur les plateformes de télémédecine ou de télésanté. L'ISPA appelle donc le législateur à ne pas prendre à l'avenir d'initiatives qui sapent l'E2EE au lieu de le protéger.

Approche à plusieurs niveaux – Pour s'attaquer efficacement au problème des contenus ou comportements inappropriés en ligne, il est essentiel d'adopter une approche commune et à plusieurs niveaux. Tout d'abord, il est crucial de reconnaître les efforts proactifs de nos membres, qui jouent un rôle essentiels en aidant leurs clients à naviguer au travers de ces défis et à les relever.

La mise en œuvre du règlement sur les services numériques (DSA)[14] et les discussions en cours sur la proposition de règlement CSAM[15] au niveau de l'UE sont des étapes positives vers des mesures en ce sens. L'ISPA estime que le **niveau européen** est le mieux équipé pour s'attaquer à ce problème transfrontalier.

Utilisation du Groupe D9+ – Notre secteur devrait reconnaître l'importance du Groupe ministériel D9+ et encourager activement les ministres chargés du numérique de ces petits et moyens pays à se joindre aux initiatives politiques de l'UE et à jouer un rôle de premier plan dans la transition numérique. Grâce au Groupe D9+, la Belgique peut jouer un rôle de premier plan dans la promotion du marché unique numérique, dont l'importance pour l'économie ouverte de notre pays est fondamentale.

Au **niveau national**, nous préconisons une approche complémentaire à 360 degrés, reconnaissant le rôle des différentes parties prenantes, y compris les fournisseurs d'accès à internet, les OTT, les autorités publiques et les ONG telles que Child Focus. En particulier, le travail louable de Child Focus en matière d'éducation et de prévention des menaces en ligne, notamment auprès des jeunes, mérite d'être salué. Leurs efforts contribuent de manière significative à la création d'un environnement numérique plus sûr et nous encourageons les initiatives de collaboration qui renforcent leur impact. Grâce à ces efforts conjoints, nous visons à promouvoir une stratégie globale et cohérente qui s'attaque aux multiples défis des contenus et des comportements illicites en ligne, en mettant particulièrement l'accent sur la

[14] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).
[15] Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants.

protection de la sécurité et de la vie privée des (jeunes) enfants. L'ISPA est ouverte à tout dialogue avec les parties prenantes concernées sur des solutions permettant de faire de l'internet un environnement plus sûr.

Consultations transparentes et ouvertes – Lors de la transposition de la directive SRI 2, le Centre pour la Cybersécurité Belgique (CCB) a mené une consultation publique et recueilli les avis de diverses parties prenantes. En tant que secteur, nous soutenons ce type de processus et encourageons le législateur à prendre l'habitude d'impliquer les parties prenantes, qui subissent les conséquences d'un texte législatif spécifique, dans le processus législatif. En outre, nous encourageons vivement à consulter le secteur le plus tôt possible. Plus important encore, nous demandons que ces processus soient menés de manière transparente et ouverte afin que toutes les parties prenantes qui souhaitent s'y impliquer se trouvent sur un pied d'égalité.

Partenariats public-privé – La mise en place de partenariats public-privé solides entre les FSI, les OTT, les hébergeurs et les autorités publiques facilite le partage d'informations et renforce la réponse collective à la fraude en ligne. La promotion d'une collaboration ouverte et transparente entre les différentes parties prenantes favorise également une approche holistique des cybermenaces, en tirant parti de l'expertise et des ressources des autorités, de l'industrie et des organisations de la société civile. Le Belgian Anti Phishing Shield (BAPS) est un excellent exemple de la contribution active à un internet plus sûr de l'implication directe des FSI dans une initiative du CCB.

3. Cadre réglementaire et favorable à l'investissement

Contexte

Le secteur de l'internet exige une réévaluation fondamentale du cadre réglementaire pour en faire un cadre véritablement favorable à l'investissement, avec une législation harmonisée entre l'UE et les États membres, mais aussi au sein de la Belgique (au niveau fédéral, régional et local). Pour ce faire, nous devons être particulièrement conscients de l'impact des politiques de l'UE dans le secteur numérique et affecter nos ressources à des mesures qui apportent une valeur ajoutée. Ainsi, l'industrie du numérique et des télécommunications pourra véritablement être un moteur d'innovation.

Problème

Le secteur de l'internet est en majeure partie réglementé au niveau de l'UE. Comme le montre le tableau ci-joint (voir Annexe 1), les mandats européens antérieurs ont produit un **large éventail** d'initiatives, notamment dans les domaines de la vie privée, de la protection des données, de la cybersécurité, de la *modération des contenus*[16], etc. La mise en œuvre de ces initiatives exige des ressources importantes de la part des entreprises, notamment en raison de la rapidité avec laquelle le secteur évolue et de la nécessité de s'adapter rapidement aux nouvelles technologies.

Cependant, il arrive que des mesures nationales, régionales ou communautaires viennent s'y ajouter, souvent dans des matières déjà réglementées au niveau européen. Compte tenu du grand nombre d'initiatives de l'UE, cela ne fait que créer un **cadre réglementaire plus confus** et menace l'harmonisation du marché unique.

En outre, la dérogation aux normes européennes ne fait que renforcer cette fragmentation, en particulier lorsque la mise en œuvre diffère également d'une région à l'autre en Belgique.

[16] Gestion du contenu en ligne, ou « content ».

Enfin, notre pays doit créer un **environnement plus favorable à l'investissement.** Les entreprises sont non seulement découragées d'investir par le cadre réglementaire fragmenté ou obsolète mentionné plus haut, mais le système fiscal actuel peut également poser des problèmes. Plusieurs communes taxent les antennes ou les réseaux fixes et exigent une redevance pour le déploiement de la fibre optique, ce qui a un impact négatif sur le climat d'investissement en Belgique et entrave l'esprit d'entreprise et l'innovation.

Solutions proposées

Mettre l'accent sur une réévaluation approfondie des initiatives réglementaires existantes – Notre secteur demande que la prochaine législature de l'UE se concentre sur la mise en œuvre et la simplification des règles existantes. Comme le montre le tableau ci-joint, les deux dernières législatures européennes ont produit un large éventail d'initiatives destinées au secteur du numérique et des télécommunications. Le secteur a besoin de temps pour réévaluer les initiatives actuelles.

Un cadre clair, avec une prise de conscience de l'impact des politiques de l'UE – Nos décideurs politiques et nos parties prenantes devraient avoir un « réflexe UE » plus fort. Connaître les mesures qui seront réglementées au niveau de l'UE, comment elles le seront et quel sera leur impact sur le marché belge permettra d'investir les ressources de manière plus adéquate et plus efficace dans des mesures qui complètent le niveau européen.

Appel contre le « gold-plating » – Pour disposer d'un cadre réglementaire stable et complémentaire, il est conseillé de ne pas déroger aux exigences fixées par l'UE. Il faut éviter d'étendre les pouvoirs des directives lors de leur transposition en droit interne afin de créer un écosystème numérique harmonisé au sein du marché unique.

Un cadre belge harmonisé – La complexité de notre structure étatique est souvent un obstacle à la mise en place de politiques équilibrées et coordonnées. Le secteur encourage donc une coordination efficace entre les différentes régions, en particulier lors de la mise en œuvre de la législation européenne.

Exemples :

- La Belgique est le deuxième pays européen à introduire un indice de réparabilité,[17] dans le cadre du plan d'action fédéral pour l'économie circulaire. Alors qu'un indice européen de réparabilité est également en cours d'élaboration avec la proposition de directive sur des règles communes visant à promouvoir la réparabilité des biens,[18] une réglementation belge précoce risque de s'écarter de l'approche envisagée au niveau de l'UE et de fragmenter le marché intérieur. En effet, le considérant 2 de la proposition de directive indique que « des règles nationales impératives divergentes dans ce domaine constituent des obstacles réels ou potentiels au fonctionnement du marché intérieur, qui portent atteinte aux transactions transfrontalières des opérateurs économiques agissant sur ce marché ».
- La législation sur les services numériques prévoit des règles uniformes pour un environnement en ligne sûr et fiable sur le marché numérique unique, ciblant les services intermédiaires en ligne. La réglementation des plateformes est intégralement prévue dans la DSA, ce qui signifie que la Belgique doit maintenant se concentrer sur divers aspects : assurer l'harmonisation nécessaire entre les différentes autorités compétentes pour la mise en œuvre de la DSA, offrir une transparence suffisante quant à la portée des différentes autorités impliquées et, enfin,

[17] Communiqué de presse Ministre Khattabi, 2 juin 2023 : La Belgique devient le deuxième pays européen à instaurer un indice de réparabilité – lien : https://khattabi.belgium.be/fr/cp-repairindex.
[18] Proposition de Directive du Parlement européen et du Conseil établissant des règles communes visant à promouvoir la réparation des biens et modifiant le règlement (UE) 2017/2394 et les directives (UE) 2019/771 et (UE) 2020/1828.

fournir à notre coordinateur des services numériques les outils nécessaires pour accomplir sa tâche aussi efficacement que possible. Il s'agit notamment de sensibiliser davantage, de permettre un encadrement et de mettre l'accent sur la prévention en ce qui concerne la DSA, son impact et les droits et obligations qu'elle crée. Par exemple, en ce qui concerne la protection des enfants en ligne, notre pays peut confier un rôle de coordination à Child Focus.

Cadre favorable à l'investissement – Enfin, il convient d'éviter les charges fiscales inutiles afin de renforcer un cadre favorable à l'investissement. Il y a lieu d'éviter les doubles taxations et la taxation des infrastructures, telles que les mâts et pylônes[19] ou les réseaux fixes. En outre, il convient de combattre la demande de redevance de plusieurs villes et communes pour le déploiement de la fibre optique.

[19] Dans le cadre du programme Giga Région de Digital Wallonia, un nouvel accord Tax on Pylons (3e édition) a été conclu entre les opérateurs de télécommunications et la Wallonie. Dans cet accord, la Wallonie s'engage à maintenir la suppression des taxes régionales et la recommandation aux provinces et aux communes de ne pas taxer les mâts, pylônes et antennes, en échange d'investissements dans une meilleure connectivité. Nous souhaiterions que de telles mesures soient prises sur l'ensemble du territoire, car plusieurs communes flamandes perçoivent encore des taxes sur les pylônes. – lien : https://www.digitalwallonia.be/fr/publications/giga-region-3eme-accord-top-operateurs/.

Annexe 1 : aperçu des initiatives récentes de l'UE (non exhaustif)

	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 – Aperçu de la législation européenne dans le secteur numérique, 16 novembre 2023