



CONSUMERPRO

BOOSTING PROFESSIONALS
IN CONSUMER PROTECTION

Droits numériques

Document de référence théorique

2022-2023

Digital Rights - Belgium (FR)
November 2022 - version 1



TABLE DES MATIÈRES

Table des matières	1
Introduction au document de base théorique	3
1. Protection des données.....	4
1.1. Introduction et historique de la politique de protection des données des consommateurs	4
1.2. Pourquoi la protection des données est importante pour les consommateurs	4
1.3. Principaux défis liés à la politique de protection des données des consommateurs	5
1.4. Les principaux droits et obligations des consommateurs en bref.....	5
1.5. Lois et réglementations européennes et nationales.....	6
1.6. Compétence	7
1.7. Que peuvent faire les consommateurs en cas de problème ?.....	8
1.8. Autres sources - fiches d'information, publications, liens	9
2. Plateformes.....	10
2.1. Introduction et historique de la plate-forme et de la politique des consommateurs	10
2.2. Pourquoi les plateformes sont importantes pour les consommateurs	11
2.3. Principaux défis liés aux plateformes	11
2.4. Les principaux droits et obligations des consommateurs en bref.....	16
2.5. Lois et règlements au niveau de l'UE.....	19
2.6. Compétence	21
2.7. Que peuvent faire les consommateurs en cas de problème ?.....	21
2.8. Autres sources - fiches d'information, publications, liens	21
3. Télécommunications.....	22
3.1. Introduction et historique de la politique des consommateurs en matière de télécommunications Error! Bookmark not defined.	
3.2. Pourquoi les télécommunications sont importantes pour les consommateurs Error! Bookmark not defined.	
3.3. Principaux défis en matière de télécommunications	Error! Bookmark not defined.
3.4. Les principaux droits et obligations des consommateurs en bref.....	Error! Bookmark not defined.
3.5. Lois et règlements au niveau de l'UE.....	Error! Bookmark not defined.
3.6. Compétence	Error! Bookmark not defined.
3.7. Que peuvent faire les consommateurs en cas de problème ?.....	Error! Bookmark not defined.
3.8. Autres sources - fiches d'information, publications, liens	Error! Bookmark not defined.



4. Annexe - Liste de la jurisprudence de la CJUE concernant la directive sur le commerce électronique
Error! Bookmark not defined.

Ce document a été produit dans le cadre du projet **Consumer PRO**, une initiative de la Commission européenne dans le cadre du programme européen des consommateurs. Le soutien de la Commission européenne n'implique pas l'approbation du contenu, qui reflète uniquement l'opinion des auteurs. La Commission ne peut être tenue responsable de l'usage qui pourrait être fait des informations qui y sont contenues.

INTRODUCTION AU DOCUMENT DE REFERENCE THEORIQUE



Cher lecteur,

Ce document théorique fait partie des ressources documentaires développées pour **Consumer PRO**, une initiative de l'UE qui vise à rendre les organisations de consommateurs et les autres acteurs de la politique des consommateurs mieux équipés pour protéger les consommateurs dans leur pays.

L'objectif de ce document est de vous fournir, ainsi qu'à vos collègues, des informations utiles et pertinentes sur les droits numériques. Le contenu a été préparé par les experts politiques du BEUC sur les droits numériques, dans une perspective européenne. Ce faisant, nous souhaitons vous aider à :

- Former rapidement vos équipes de praticiens,
- Trouver facilement des informations pertinentes,
- Permettre à votre personnel de mieux informer les consommateurs sur leurs droits, et,
- Sensibiliser vos autorités nationales au droit du numérique.

Ce document de référence théorique fait partie d'une série d'outils de formation. Ces documents sont à chaque fois adaptés au contexte national. Il existe également des documents de référence théoriques, sur le droit des consommateurs (général) et sur les recours collectifs. Ces documents peuvent être trouvés [en ligne](#) ou peuvent vous être envoyés sur demande.

À propos de Consumer PRO

Consumer PRO est une initiative de la Commission européenne dans le cadre du programme européen des consommateurs et est mis en œuvre par le BEUC – le Bureau européen des unions de consommateurs. Ce projet vise à renforcer les capacités des organisations européennes de consommateurs et d'autres acteurs de la politique des consommateurs à travers l'apprentissage non-formel. Ce projet se déroule dans les États membres de l'UE, en Islande et en Norvège.

Pour plus d'informations, veuillez envoyer un courriel à Info@consumer-pro.eu



1. PROTECTION DES DONNÉES

1.1. Introduction et historique de la politique de protection des données des consommateurs

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental dans l'Union européenne. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne (TFUE) prévoient que toute personne a droit à la protection des données à caractère personnel la concernant. En outre, l'article 7 de la Charte des droits fondamentaux de l'Union européenne prévoit que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Le Règlement général sur la protection des données (RGPD) régit le traitement des données personnelles dans l'UE. Elle oblige les organisations, tant les autorités publiques que les entreprises privées, à utiliser les données personnelles des consommateurs de manière transparente et équitable. Le Règlement renforce vos droits et s'applique à toutes les organisations qui traitent des données personnelles de personnes situées dans l'UE. Ce Règlement s'applique quel que soit le lieu où se trouvent les organisations.

Les règles relatives à la vie privée en ligne (la directive "vie privée et communications électroniques", actuellement en cours de révision) protègent la confidentialité des communications électroniques et prévoient également des protections spécifiques pour les consommateurs contre les communications commerciales non sollicitées envoyées par des services de communication électronique.

1.2. Pourquoi la protection des données est importante pour les consommateurs

Si les technologies de l'information numérique et l'émergence de **nouveaux services en ligne sont bénéfiques** pour les consommateurs, elles constituent également un **défi majeur pour les droits fondamentaux de la vie privée et de la protection des données personnelles**. Les modèles commerciaux qui dominent actuellement le monde numérique sont fondés sur le suivi et l'analyse des moindres gestes des consommateurs. Les entreprises utilisent les informations qu'elles collectent pour créer des profils d'utilisateurs, qui sont échangés en ligne. Ces profils sont ensuite utilisés pour envoyer des publicités adaptées au comportement réel des consommateurs. Ces profils peuvent également être utilisés pour discriminer les consommateurs et influencer leur comportement. Il est important de veiller à ce que les consommateurs puissent garder le contrôle de leurs données personnelles et profiter de produits et services numériques innovants sans renoncer à leur vie privée.



1.3. Principaux défis liés à la politique de protection des données des consommateurs

Il est très difficile pour les consommateurs de contrôler ce qu'il advient de leurs données dans la pratique. Très souvent, leurs droits ne sont pas respectés et ils sont souvent contraints de renoncer à leur vie privée s'ils veulent utiliser des produits et services numériques.

Les consommateurs sont soumis à une surveillance commerciale constante et leurs données personnelles sont exploitées par une multitude d'entreprises dont ils n'ont souvent jamais entendu parler. Les politiques de confidentialité sont vagues, longues, compliquées et très difficiles à comprendre. Les consommateurs n'ont d'autre choix que de les accepter. Les consommateurs ont souvent l'illusion d'un contrôle et, dans les cas où le consentement est demandé, il l'est systématiquement au moyen d'une "case à cocher" vide de sens.

Le RGPD avait pour but de résoudre bon nombre de ces problèmes. Cependant, près de quatre ans après sa promulgation, il n'y a toujours pas de changements significatifs dans les pratiques commerciales. Le respect du nouveau Règlement semble faible dans certains secteurs et l'application n'est pas efficace à 100 %. Les APD (autorités de protection des données) ont du mal à traiter toutes les plaintes qu'elles reçoivent. Elles sont donc confrontées à une série de défis importants liés à cette nouvelle architecture d'application, qui s'articule autour d'un mécanisme de coopération et de cohérence visant à garantir une interprétation et une application cohérentes de la législation dans toute l'UE.

Un autre problème est que la réforme des règles ePrivacy, qui devrait compléter le RGPD et protéger davantage la confidentialité des communications, est en attente depuis plus de cinq ans et qu'il n'y a toujours pas d'accord en vue. (Pour plus d'informations sur le Règlement ePrivacy, voir la fiche d'information du BEUC [ici](#))

1.4. Les principaux droits et obligations des consommateurs en bref

Le RGPD impose aux organisations, qu'il s'agisse d'organismes publics ou d'entreprises, d'utiliser les données personnelles des consommateurs de manière transparente et équitable. Il contient un ensemble de [principes](#) régissant l'utilisation des données personnelles :

Elle donne également aux consommateurs un ensemble de [droits](#) leur permettant de contrôler leurs données. Les consommateurs ont, entre autres, le droit de :

- Être informés de manière claire et facilement compréhensible de la manière dont leurs données personnelles sont utilisées. Elle doit préciser quelles données sont utilisées, par qui et à quelles fins.
- Accéder et obtenir une copie des données que les organisations détiennent à leur sujet.
- Corriger leurs données si elles sont incorrectes.
- Demander aux organisations de supprimer leurs données.

- Demander aux organisations de cesser d'utiliser leurs données (temporairement ou définitivement).
- Recevoir leurs données dans un format communément utilisé afin qu'ils puissent les emporter avec eux et les utiliser ailleurs.
- Contester les décisions automatisées fondées sur leurs données personnelles et qui les affectent de manière significative (par exemple, le refus d'un prêt).
- Être informés en cas de perte ou de vol de leurs données.
- Déposer une plainte auprès de l'autorité nationale chargée de la protection des données ou poursuivre une entreprise en justice.

1.5. Lois et réglementations européennes et nationales

- [Charte des droits fondamentaux de l'UE](#)
- [Règlement \(UE\) 2016/679](#) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (GDPR).¹
- [Directive 2002/58/CE](#) concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)² - Modifiée par la [directive 2009/136/CE](#)³
- [Lignes directrices, recommandations et meilleures pratiques du Conseil européen de la protection des données.](#)
- [Avis du Contrôleur européen de la protection des données](#)
- [Exemple de code de conduite : Fédération du marketing direct](#)

¹ Transposé par la [loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.](#)

² Transposé par la [loi sur les communications électroniques du 13 juin 2005.](#)

³ Transposé par la [loi du 10 juillet 2012 portant des dispositions diverses en matière de dispositions électroniques.](#)

Au niveau national

La [loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données](#) (qui met en œuvre le règlement RGPD en droit belge), a été publiée au Moniteur belge le 5 septembre 2018. Cette loi complète ainsi la [loi du 3 décembre 2017 instituant l'Autorité de protection des données \(APD\)](#). Cette loi a mis la Commission de la protection de la vie privée (CPVP) en conformité avec les règles du RGPD. La Commission de la protection de la vie privée a été rebaptisée "autorité de protection des données". Une modification de ses statuts est actuellement à l'étude. [L'ADP](#) elle-même préconise principalement une expansion de ses ressources.

L'autorité de protection des données est un organe de contrôle indépendant dont la tâche principale est de garantir les principes fondamentaux liés à la protection des données personnelles.

Les avis, recommandations, décisions et autres publications publiés par l'APD peuvent être consultés via [ce lien](#).

Nous pouvons notamment nous référer ici aux éléments suivants, par lesquels l'APD tente de mieux expliquer aux consommateurs quels sont leurs droits à travers un certain nombre d'exemples concrets:

- [Traitement des données à caractère personnel à des fins de marketing direct, mes droits dans le contexte du marketing direct](#), ainsi que la page "[Qu'est-ce que le marketing direct ?](#)"
- [Le droit à la vie privée ne s'arrête pas à la porte de l'école.](#)
- [Le principe du consentement](#)
- [Diverses analyses sur le crédit à la consommation et le fichier central des crédits aux particuliers.](#)

1.6. Jurisprudence

Pour une vue d'ensemble des décisions des autorités et des tribunaux en matière de protection des données, ainsi que pour des articles sur le RGPD, voir : www.GDPRHub.eu.

Sur le portail officiel du droit de l'UE : [Dossier Eurlex sur le GDPR](#). Ceci est une liste des affaires de la CJUE et des questions préliminaires relatives au RGPD : retrouvez la liste de la jurisprudence sous la rubrique « Informations sur le document ».

1.7. Que peuvent faire les consommateurs en cas de problème ?

Si les consommateurs estiment que leurs droits ont été violés en vertu du RGPD, deux options s'offrent à eux :

- Déposer une plainte auprès de l'autorité nationale de protection des données. La liste complète des autorités nationales peut être consultée via https://edpb.europa.eu/about-edpb/board/members_en
- intenter directement une action en justice contre une entreprise/organisation. Cela n'empêche pas les consommateurs de se plaindre auprès des autorités nationales de protection des données s'ils le souhaitent.

En outre, si le consommateur estime que l'APD n'a pas traité correctement sa plainte, s'il n'est pas satisfait de la réponse de l'APD ou si l'APD ne l'informe pas de l'évolution ou de l'issue de la procédure dans un délai de trois mois à compter du jour du dépôt de la plainte, il peut intenter une action contre l'APD directement devant un tribunal.

Autorités publiques

Au niveau national :

Outre l'autorité de protection des données, le SPF Justice, Direction IV (droits fondamentaux), département Vie privée et égalité des chances, dispose également d'un pouvoir législatif. Mais les pouvoirs d'audit et de sanction restent du ressort de l'autorité de protection des données.

Outre les autorités nationales de protection des données, d'autres organismes gouvernementaux méritent d'être pris en considération :

Au niveau européen :

- La Commission européenne, qui doit veiller à ce que les États membres mettent correctement en œuvre le RGPD et qui a également le pouvoir d'"activer" certaines dispositions du RGPD par le biais d'actes délégués (par exemple, pour créer des "icônes de confidentialité" standardisées).
- Le [Comité européen de protection des données](#) (EDPB), qui réunit toutes les autorités nationales de protection des données. Sa tâche principale est d'assurer la cohérence dans l'application et l'interprétation du RGPD.
- Le [Contrôleur européen de la protection des données](#) (CEPD), qui veille à ce que les institutions de l'UE respectent les données personnelles des citoyens et conseille les institutions sur les questions de protection des données.

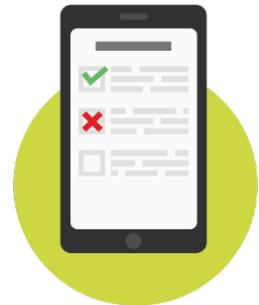
Résolution alternative des conflits

Des procédures extrajudiciaires et d'autres procédures de règlement des litiges entre les responsables du traitement des données et les personnes concernées en ce qui concerne le traitement des données à caractère personnel peuvent être établies par le biais de codes de conduite adoptés par des organismes sectoriels (article 40 du RGPD), sans préjudice du droit des personnes concernées de déposer des plaintes auprès de leur autorité de protection des données et de demander un recours judiciaire.

En Belgique, le premier code de conduite national a été approuvé en septembre 2021. Il s'agit du code de conduite de la Chambre nationale des notaires⁴. Cependant, ce premier code de conduite ne contient pas de section relative à la résolution extrajudiciaire des conflits.

1.8. Autres sources - fiches d'information, publications, liens

- [Site de la Commission européenne avec des informations sur le GDPR](#)
- [Bibliothèque de la Commission européenne sur le GDPR - Infographies, fiches d'information et autres documents destinés aux citoyens et aux entreprises.](#)
- [BEUC Factsheet - Wat betekent de EU-wetgeving inzake gegevensbescherming voor u?](#)
- [AccessNow - Guide de l'utilisateur sur la protection des données dans l'UE : vos droits et comment les exercer](#)
- [Agence des droits fondamentaux - Manuel européen de protection des données](#)
- [Fiches techniques](#) publiées par le Contrôleur européen de la protection des données (CEPD)
- [L'histoire du GDPR](#) et un [glossaire](#) (CEPD)
- www.jedecide.be: Site belge qui explique les règles de privacy aux jeunes, aux parents et à l'enseignement



⁴ Plus d'informations sur [L'APD approuve son tout premier code de conduite national | Autorité de protection des données \(autoriteprotectiondonnees.be\)](#) et [Le notaire - Notaire.be](#)

2. PLATEFORMES

2.1. Introduction et historique de la plateforme et de la politique des consommateurs

Les consommateurs achètent de plus en plus de services et de produits en ligne, notamment par le biais de plateformes.

Dans les premières années du commerce électronique, ces achats se faisaient principalement sur les sites web d'entreprises qui disposaient également des magasins physiques. Aujourd'hui, le comportement d'achat des consommateurs change radicalement : de plus en plus de personnes commandent des services et des produits via des places de marché en ligne qui sont expédiés directement de l'extérieur de l'UE aux consommateurs européens.

Les achats sont effectués non seulement sur des plateformes de commerce électronique telles que Amazon Marketplace, AliExpress, wish.com ou eBay, mais également via les réseaux sociaux telles qu'Instagram.

En 2017, par exemple, environ 100 millions de marchandises ont été expédiées de la Chine vers l'Allemagne. C'est 40 millions de plus qu'en 2016. Des augmentations considérables ont également été signalées dans d'autres pays européens. En Belgique, 63% des Belges ont effectué des achats en ligne en 2022⁵. En outre, le rapport annuel 2021 de l'Inspection économique⁶ montre que les escroqueries en ligne restent le plus gros problème (p.e. faux sites de commerce électronique).

Les problèmes les plus courants concernaient le manque de détails d'identification et l'absence d'indications de prix correctes.

En outre, de plus en plus de boutiques en ligne dans l'UE sont créées par des vendeurs qui se font passer pour des entreprises européennes mais qui en réalité passent des commandes sur des plateformes en Chine et vendent ces produits aux consommateurs à un prix plus élevé (par rapport, par exemple, au prix pratiqué sur wish.com). De telles pratiques ont déjà été observées au Danemark et en France⁷, mais aussi en Belgique⁸.

Il existe également de sérieuses inquiétudes quant au fait que nombre de ces produits ne sont pas conformes aux règles et normes techniques européennes introduites pour protéger les droits des



⁵ <https://statbel.fgov.be/fr/themes/menages/utilisation-des-tic-aupres-des-menages>

⁶ [Près de 48.000 signalements en 2021 - FOD Economie \(communiqué de presse\) \(fgov.be\)](#)

⁷ <http://www.leparisien.fr/economie/consommation/achats-en-ligne-attention-aux-derives-du-dropshipping-16-01-2020-8237226.php>

⁸ Test-Achat, " comment puis-je encore me retrouver avec un fournisseur chinois avec un achat local en ligne ? ", 19 février 2021, article disponible sur le lien suivant : [Vendeur en ligne local mais fournisseur chinois \(test-achat.be\)](#).

consommateurs, la santé, la sécurité et l'environnement. Si les fabricants et les distributeurs établis dans l'UE peuvent être tenus responsables de la sécurité et de la conformité des produits, ce n'est souvent pas le cas pour les producteurs établis en dehors de l'UE, car les intermédiaires, c'est-à-dire les plateformes de commerce électronique, refusent d'assumer la responsabilité de la conformité.

D'importantes initiatives législatives sont actuellement en cours de discussion au niveau européen pour aborder certaines de ces questions, notamment la proposition de Règlement sur les services numériques⁹ et la proposition de Règlement sur la sécurité générale des produits¹⁰.

2.2. Pourquoi les plateformes sont importantes pour les consommateurs

Faire des achats, communiquer avec ses amis et sa famille, partager des expériences, regarder un film, écouter de la musique, lire un livre, réserver un voyage, cuisiner une nouvelle recette, organiser une soirée, se déplacer dans une ville, demander l'aide de voisins et rechercher des informations sur le web : ce ne sont là que quelques exemples d'activités que des millions de consommateurs réalisent chaque jour. Pour chacune de ces activités, il existe une ou plusieurs plateformes en ligne qui facilitent ces services. Les consommateurs ont adopté l'essor de l'économie de plateforme, qui apporte de nombreux avantages, mais aussi des défis pour la protection des consommateurs.

2.3. Principaux défis liés aux plateformes

Lorsque la Directive sur le commerce électronique a été adoptée (en 2000), des plateformes comme Google, Amazon ou Booking.com en étaient à leurs balbutiements. Les autres intermédiaires n'existaient même pas encore. Facebook et Shopify, par exemple, ont été lancés en 2004. Etsy a été fondée en 2005 ; Airbnb en 2008. Instagram, Wish et AliExpress ont vu le jour en 2010.

⁹ [Loi sur les services numériques : assurer une plus grande sécurité et une plus grande responsabilité en ligne | Commission européenne \(europa.eu\)](#)

¹⁰ [EUR-Lex - 52021PC0346 - FR - EUR-Lex \(europa.eu\)](#)

Au cours des 20 dernières années, les modèles économiques de certaines de ces entreprises et d'autres ont changé. La dynamique du pouvoir de marché a également changé.

Le paysage du marché numérique européen a connu une "datafication" (Le transfert de l'information vers des données qui constituent la base des modèles économiques numériques) ; une multiplication des plateformes ; une prolifération de l'économie collaborative¹¹ et une diversification des prestataires de services en termes de fonctions, d'intégration verticale et de taille. Pourtant, chaque entreprise doit respecter les règles du jeu. La protection des consommateurs ne dépend pas - et ne devrait pas dépendre - de la taille de l'entreprise. Après tout, la start-up ou la PME d'aujourd'hui peut devenir l'Alibaba de demain.



La protection des consommateurs ne dépend pas - et ne devrait pas dépendre - de la taille de l'entreprise. Après tout, la start-up ou la PME d'aujourd'hui peut devenir l'Alibaba de demain.

De nombreuses plateformes se sont réinventées. Certaines ne se limitent plus à leur rôle initial de fournisseur d'informations ou d'intermédiaire de confiance (par exemple, les plateformes de comparaison ou de classement telles que Yelp), mais permettent de conclure des transactions sur la plateforme. Il s'agit de modèles commerciaux qui font que la plateforme entre dans la catégorie des "marchés en ligne"¹², sur laquelle les organisations de consommateurs se concentrent actuellement. Ce type de plateforme est défini dans la directive Omnibus comme " *un service utilisant un logiciel, y compris un site internet, une partie de site internet ou une application, exploité par un professionnel ou pour son compte qui permet aux consommateurs de conclure des contrats à distance avec d'autres professionnels ou consommateurs.*"¹³. Cela dit, le rôle de la plateforme ne se limite souvent pas à permettre la conclusion d'un contrat entre vendeurs et acheteurs, mais comprend également d'autres services tels que les services de paiement, les services d'exécution, le traitement des retours et le traitement des plaintes¹⁴.

D'autres plateformes se sont vu attribuer des rôles multiples. Il existe des "plateformes hybrides", qui peuvent combiner différentes fonctions d'intermédiation, ou des plateformes verticalement intégrées. Ces derniers ne font pas seulement office d'intermédiaires mais sont également en concurrence avec les commerçants, soit directement, soit par le biais d'affiliés. Par exemple, Amazon est un détaillant, une place de marché en ligne, une société de cloud computing, une plateforme de

¹¹ http://www.beuc.eu/publications/beuc-x-2016-030_gbe_collaborative_economy_beuc_position.pdf

¹² Étude Vzbv, https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 17.

¹³ Article 2, paragraphe 1, point n), de la directive sur les pratiques commerciales déloyales, telle que modifiée par la directive 2019/2161", L_2019328FR.01000701.xml (europa.eu)

¹⁴ Étude Vzbv, https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 18.

partage de vidéos, un éditeur, une société de publicité, un fabricant d'appareils connectés et une société d'intelligence artificielle.

Les organisations de consommateurs demandent des ajustements du cadre législatif pour faire face à cette nouvelle réalité du marché. La proposition de loi sur les services numériques (Digital Services Act, « DSA ») est une initiative très importante à cet égard. La Commission a déposé la proposition de DSA en décembre 2020. Elle se trouve actuellement dans les dernières étapes du processus législatif. Un accord devrait être conclu en 2022.

Défis spécifiques

Défi n° 1. Diffusion d'un large éventail de contenus illégaux.

Les services numériques sont devenus - dans une certaine mesure - un facilitateur de violations généralisées du droit de la consommation, une source de revenus pour la vente de publicités ou la promotion en ligne de produits dangereux, non sécurisés et illégaux. Par exemple¹⁵ :

	<p>Le membre britannique du BEUC, Which ?, a découvert des guirlandes de Noël vendues en ligne qui pourraient prendre feu ou électrocuter les consommateurs¹⁶.</p>
	<p>Le Conseil danois des consommateurs a révélé que les produits cosmétiques proposés sur wish.com n'étaient pas conformes à la législation européenne.</p>
	<p>Plus récemment, six membres du BEUC ont constaté que deux tiers des 250 produits achetés sur des places de marché en ligne avaient échoué aux tests de sécurité, avec des conséquences telles qu'un choc électrique, un incendie ou une suffocation.¹⁷</p>

¹⁵ Voir des exemples sur https://www.beuc.eu/publications/beuc-x-2019-072_new_evidence_from_beuc_member_organisations_regarding_dangerous_products_available_online.pdf

¹⁶ <https://www.which.co.uk/news/2019/12/these-christmas-tree-lights-bought-online-at-ebay-wish-and-aliexpress-could-catch-fire-or-electrocute-you/>

¹⁷ <https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html>

	<p>L'AFSCA met en garde contre la vente en ligne de compléments alimentaires, tels que les compléments alimentaires illégaux et potentiellement dangereux qui permettraient de renforcer l'immunité au COVID19¹⁸.</p>
	<p>Test-Achats a publié en avril 2020 les résultats d'une enquête concernant les produits vendus sur Internet (notamment par AliExpress, LightInTheBox et Amazon) pour blanchir les dents. La qualité de la plupart de ces produits était au mieux décevante. Beaucoup de ces produits devraient même être déconseillés car ils contiennent plus de 1% de peroxyde d'hydrogène¹⁹.</p>

Défi n°2. Confusion entre les activités de marché en ligne et les autres activités de la plateforme.

Dans une certaine mesure, le débat sur la réforme du commerce électronique s'est concentré sur des questions telles que les discours haineux, les contenus terroristes, le matériel protégé par le droit d'auteur, la liberté d'expression ou les considérations relatives au marché intérieur. S'il s'agit de questions importantes, l'UE ne doit pas non plus perdre de vue les problèmes spécifiques liés à la protection des consommateurs. Il faut s'assurer que les consommateurs qui achètent des produits ou des services sur les places de marché en ligne²⁰ sont pleinement protégés.

Il convient de faire la distinction entre la vente de produits illégaux et les autres activités, par exemple la publication de commentaires sur les médias sociaux. Si le second implique clairement la liberté d'expression, le premier concerne davantage la sécurité des produits et la protection des consommateurs.

Défi 3 : La directive sur le commerce électronique " *ne s'applique pas aux prestataires de services établis dans un pays tiers* "²¹.

¹⁸ [AFSCA - Alerte AFSCA \(favv-afscs.be\)](http://favv-afscs.be)

¹⁹ Test Achats, "Blanchisseurs sur le net, ne touchez pas à vos dents", avril 2020, pp. 36-37.

²⁰ Défini dans la directive omnibus de l'UE comme "un service utilisant un logiciel, y compris un site web, une partie de site web ou une application exploitée par ou pour le compte d'un professionnel, qui permet aux consommateurs de conclure des contrats à distance avec d'autres professionnels ou consommateurs.". Cela dit, le rôle de la plateforme ne se limite souvent pas à permettre la conclusion d'un contrat entre vendeurs et acheteurs, mais comprend également d'autres services tels que des services de paiement, des services d'exécution, des services de retours et de traitement des plaintes.

²¹ Directive sur le commerce électronique, considérant 58.

Certains prestataires de services basés dans des pays tiers abusent des restrictions de territorialité de la directive, créant ainsi des conditions de concurrence inéquitables et inégales.

Défi 4 : La façon dont la directive sur le commerce électronique régit les fournisseurs d'hébergement est utilisée par certaines plateformes - y compris (mais pas seulement) les places de marchés en ligne - pour se protéger de toute responsabilité ou ne pas prendre de mesures significatives par crainte de la responsabilité.

Défi n°5. La législation actuelle présente des lacunes en matière de réglementation des places de marchés en ligne. Peu d'attention est accordée à l'enrichissement des places de marché en ligne par des contenus illégaux.

Défi 6 : Les nouvelles règles peuvent empêcher les États membres de répondre correctement aux objectifs d'intérêt public.

Par exemple, dans l'affaire C-390/18²², la CJUE a jugé qu'Airbnb devait être considéré comme un service de la société de l'information (article 2, point a), de la directive sur le commerce électronique). La France n'ayant pas notifié à la Commission une loi exigeant une licence professionnelle d'agent immobilier à des entreprises comme Airbnb, elle ne peut pas imposer cette obligation à Airbnb, car cela serait contraire à l'article 3, paragraphe 4, point b), de la directive sur le commerce électronique. Ce cas montre que la directive sur le commerce électronique, en mettant le marché intérieur au premier plan, crée des difficultés pour les États membres à adopter des lois et des politiques pour protéger les consommateurs. Toutefois, il est important de noter que cet arrêt ne signifie pas que les gouvernements ne peuvent pas imposer de telles mesures à des entreprises comme Airbnb. La CJUE a clairement indiqué que l'obligation de notification prévue par la directive sur le commerce électronique " n'a pas pour but d'empêcher un État membre d'adopter des mesures relevant de son propre domaine de compétence et qui pourraient affecter la libre prestation de services, mais d'empêcher un État membre d'empiéter sur la compétence, en principe, de l'État membre dans lequel le fournisseur du service de la société de l'information concerné est établi ".

On peut également se référer à la jurisprudence belge à l'encontre d'UberX. La Cour d'appel de Bruxelles, par un arrêt du 15 janvier 2021, a jugé que l'application UberX ne respecte pas la réglementation bruxelloise en matière de taxis. Les UberX de Bruxelles sont donc jugés coupables de concurrence déloyale. Toutefois, cette décision pourrait être interprétée comme contraire au droit européen de la concurrence et à la jurisprudence citée ci-dessus. Pour échapper aux obligations propres au secteur très réglementé, Uber estime qu'il ne fournit qu'un service qui consiste à mettre en relation des individus en ligne, distinct du service que les individus se rendent entre eux. Cela lui permettrait de bénéficier du régime spécial prévu par la directive sur le commerce électronique (qui exempte les plateformes de tout régime d'autorisation (tel que l'octroi de licences) pour exercer leurs activités en ligne).

²² <http://curia.europa.eu/juris/documents.jsf?num=C-390/18>

Défi 7. Absence de contrôle et de mise en œuvre appropriés.

Les marchés numériques évoluent à la vitesse de l'éclair et les autorités compétentes ne semblent pas être à la hauteur de la tâche et ne disposent pas de toute l'expertise ou des ressources nécessaires pour surveiller et traiter les problèmes du marché.

2.4. Les principaux droits et obligations des consommateurs en bref

La **directive sur le commerce électronique** est depuis longtemps l'une des pierres angulaires de l'internet. Entre autres choses, la directive sur le commerce électronique a établi le principe du pays d'origine avec quelques exceptions importantes (notamment les contrats de consommation), des obligations d'information importantes envers les destinataires de services (par exemple les consommateurs) et des exemptions et limitations de responsabilité pour les fournisseurs de services en ligne agissant en tant qu'intermédiaires :

- **Article 1 - 3 : Dispositions générales**

- **Article 4 - 15 : Principes**

Section 1 : Exigences en matière d'établissement et d'information

Section 2 : Communications commerciales

Section 3 : Contrats en ligne

Section 4 : Responsabilité de l'intermédiaire

- **Articles 16 - 20 : Mise en œuvre**

- **Articles 21 - 24 : Dispositions finales**

Où trouver les principales dispositions de la directive sur le commerce électronique ?

- **Objectif principal** : marché intérieur et libre prestation des services de la société de l'information (article 1).
- Les **objectifs** comprennent "la *sécurité juridique et la confiance des consommateurs*" (considérant 7), la garantie d'un niveau élevé de protection des consommateurs et la protection des mineurs (considérant 10).
- **Champ d'application** : sans préjudice de la protection des consommateurs (article 1)
- **Définitions** (article 2)
- **Informations de base** aux consommateurs et autres destinataires (articles 5, 6 et 10)
- **Droits lors de la passation de commandes en ligne** (article 11)
- **Principes de la responsabilité des intermédiaires** (articles 12-15). Les grands principes sont les suivants :
 - Les hébergeurs ne sont pas responsables du contenu de tiers pour autant que, dès qu'ils en ont connaissance, ils suppriment d'urgence le contenu illégal ou en empêchent l'accès (article 14).

- Des mesures pour lutter contre les contenus illégaux en ligne, y compris les biens et services, comme un mécanisme permettant aux utilisateurs de signaler ces contenus et aux plateformes de coopérer avec des "signaleurs de confiance" ;
- De nouvelles règles sur la traçabilité des utilisateurs professionnels sur les places de marché en ligne (également connues sous le nom d'"obligation de connaître son client professionnel"), visant à mieux identifier les vendeurs de marchandises illégales ;
- des garanties pour les utilisateurs, notamment la possibilité de contester les décisions des modérateurs de la plateforme (interdiction de certains contenus) ;
- des mesures de transparence supplémentaires pour les plateformes en ligne, notamment sur les algorithmes utilisés pour les recommandations et sur la publicité ciblée ;
- l'obligation pour les très grandes plateformes en ligne de prévenir les abus de leurs systèmes, notamment en s'attaquant aux risques systémiques et en contrôlant les mesures qu'elles prennent par des audits indépendants ;
- Une nouvelle structure de surveillance pour faire face à la complexité de l'espace en ligne, dans laquelle les États membres joueraient le rôle principal, soutenue par un nouveau Conseil européen des services numériques. Pour les très grandes plateformes en ligne, la Commission se verrait confier un rôle plus important en matière de surveillance et d'exécution.

Si le DSA apportera des améliorations indispensables à la protection des consommateurs dans le domaine des services numériques, il est peu probable qu'il y ait des changements majeurs dans le domaine du régime de responsabilité des places de marché en ligne. Le DSA maintiendra très probablement les principes de l'exemption de responsabilité des intermédiaires de la directive sur le commerce électronique, avec toutefois quelques clarifications et améliorations mineures.

2.5. Lois et règlements au niveau de l'UE

RÈGLEMENT/DIRECTIVE	DATE DE transposition	EXAMEN / ÉVALUATION : TYPE DE MESURE	DATE D'ÉVALUATION	COMMENTAIRE
Directive sur le commerce électronique	17/01/2002 (transposition)	Rapport de réexamen CE (art. 21)	Avant le 17/07/2003, et ensuite tous les deux ans	Nous n'avons pas connaissance d'un examen formel depuis 2012 . L' enquête sectorielle 2017 de la Commission peut être intéressante du point de vue de la concurrence.
		Règlement sur les services numériques (DSA)	Proposition publiée en décembre 2020 - Actuellement au stade final de la procédure de codécision. Adoption prévue en 2022	Proposition de DSA soumise en décembre 2020, en même temps que la loi sur les marchés numériques (DMA, Digital Markets Act), qui comporte des règles spécifiques visant les plateformes de gatekeeper. Les questions clés de la DSA du point de vue du consommateur : <ul style="list-style-type: none"> - la responsabilité des intermédiaires, notamment des places de marché en ligne ; - obligations sur les clients qui connaissent leur entreprise, - procédures de notification et d'action, - les exigences de transparence, - l'application et la coordination entre les États membres, - les obligations liées à la publicité ciblée et à l'utilisation de systèmes de recommandation.



Règlement “plateforme to business” (Règlement P2B)	12/07/2020	Lignes directrices de la CE sur les exigences de transparence des classements (article 5)	Publié le 7 décembre 2022	
		La CE doit encourager les codes de conduite (Art. 17)	Pas de date	Une analyse de leurs performances fera partie de l'évaluation.
		Rapport d'évaluation de la CE (article 18)	13/01/2022 et tous les trois ans	
Directive omnibus	28 novembre 2021 (transposition) 28 mai 2022 (demande)	Article 7 - Conversion	Article 6 - Rapports et évaluation de la Commission. Rapport à publier par la CE d'ici le 28 mai 2024, règles sur les produits alimentaires et sur les mesures de vente en porte-à-porte.	



2.6. Jurisprudence

- **Directive omnibus** : pas encore de jurisprudence car elle ne s'applique qu'à partir du 28 mai 2022. Consultez le document théorique sur le droit de la consommation pour connaître la jurisprudence d'autres instruments du droit de la consommation.
- **Directive sur le commerce électronique** : - cliquez [ici](#) pour la liste complète des affaires.

2.7. Que peuvent faire les consommateurs en cas de problème ?

- Mieux vaut prévenir que guérir : Le [SPF Economie](#) fournit quelques lignes directrices sur la manière dont un consommateur peut reconnaître une boutique en ligne frauduleuse.
- Contacter le vendeur/la plateforme
- Possibilité de règlement alternatif des litiges (ADR)
- Les autorités compétentes des États membres : cela varie d'un pays à l'autre et d'un sujet à l'autre.

Autorités nationales

Autorité de régulation : SPF Economie ([On-line](#) | [SPF Economie \(fgov.be\)](#))

Helpdesk SPF Economie (veuillez noter que l'Inspection économique n'enquête pas sur les plaintes individuelles. Néanmoins, il est toujours utile de signaler tout problème à la hotline. L'Inspection économique peut toujours lancer une enquête générale) : [Où et comment signaler un problème | SPF Economie \(fgov.be\)](#)

Pour les plaintes contre les **opérateurs belges de commerce électronique**, les 3 médiateurs suivants sont compétents :

- Service de médiation pour le consommateur : [Introduire une plainte | Service de Médiation pour le Consommateur \(mediationconsommateur.be\)](#)
- Ombudsman du commerce : [Ombudsman du Commerce](#).
- La plateforme Belmed (médiation en ligne des litiges commerciaux) : [Belmed : médiation en ligne des litiges commerciaux | SPF Economie \(fgov.be\)](#)

Pour les plaintes à l'encontre des **e-commerçants européens**, veuillez contacter ECCNet : [Contact - ECC Belgium \(eccbelgie.be\)](#)

2.8. Autres sources - fiches d'information, publications, liens

- Présentation de la Commission européenne sur les outils et les objectifs de la directive sur le commerce électronique (voir [ici](#))

- Document de position du BEUC « Assurer la protection des consommateurs dans l'économie des plateformes »: ([ici](#))
- Document de position du BEUC "économie collaborative" ([ici](#))
- Position du BEUC sur le Règlement sur les services numériques (DSA) ([ici](#))
- Prise de position du BEUC sur la proposition de DSA ([ici](#))
- Fiche d'information du BEUC sur la proposition de DSA ([ici](#))
- Briefing du Parlement européen sur la proposition de DSA ([ici](#))
- Questions et réponses de la Commission européenne sur la proposition de DSA ([ici](#))

3. INTERNET DES OBJETS

3.1.Introduction et historique

Ces dernières années, les "*appareils connectés*" sont devenus omniprésents dans la vie de nombreux consommateurs. Alors que nous avons l'habitude de nous asseoir devant un ordinateur pour accéder à internet, nous transportons désormais des smartphones connectés à internet partout où nous allons. Et en même temps, de plus en plus d'appareils quotidiens autour de nous sont équipés de capteurs et connectés à internet. Des cafetières connectées aux caméras de sécurité en passant par les voitures et les appareils médicaux, l'essor des appareils connectés est communément appelé "Internet des objets", ou IoT.

3.2. Pourquoi l'IoT est-il important pour les consommateurs ?

Ces dernières années, les appareils connectés sont devenus omniprésents dans la vie de nombreux consommateurs, et leur essor modifie notre mode de vie. Si la numérisation des appareils offre de nombreux avantages aux consommateurs, les risques et les défis qu'elle entraîne sont tout aussi importants, sinon plus. Par exemple, que se passe-t-il si le fournisseur de services de votre système de maison intelligente décide de fermer ses serveurs ? Et qui est responsable si votre télévision intelligente est compromise (par des virus, par exemple) ou devient inutilisable en raison d'un manque de mises à jour logicielles ? Et qu'en est-il de l'impact sur notre vie privée ?



Il est donc important d'élaborer une politique et un cadre juridique européens clairs et tournés vers l'avenir, qui garantissent le respect des droits des consommateurs dans cet environnement connecté.



3.3. Principaux défis concernant l'IoT

La connexion d'un grand nombre d'appareils à l'internet présente à la fois des opportunités et des risques pour les consommateurs. Le monde interconnecté promet une plus grande commodité, des expériences fluides (où différentes étapes se rejoignent de manière transparente) et potentiellement une amélioration significative de la qualité de vie. Les informations agrégées provenant de ces dispositifs pourraient également ouvrir de nouvelles perspectives dans les domaines de la médecine, de l'intelligence artificielle et de l'urbanisme.

Par exemple, une maison intelligente remplie d'appareils et de capteurs connectés peut apprendre les habitudes et les préférences de son propriétaire et adapter ses fonctionnalités en conséquence. En même temps, les différents appareils individuels peuvent communiquer entre eux. Par exemple, lorsqu'un rythme cardiaque faible est détecté par une smartwatch, un message d'urgence peut être envoyé à l'hôpital le plus proche. Les personnes ayant besoin de soins peuvent conserver leur indépendance pendant longtemps grâce aux capacités de l'IoT (par exemple, surveillance/assistance à distance, possibilité de déverrouiller les portes à distance afin que la personne ne doive plus marcher jusqu'à la porte elle-même,...). Dans des secteurs tels que l'industrie et les soins de santé, l'internet des objets aura des effets potentiellement transformateurs sur l'efficacité et la collecte d'informations.

Mais les défis posés par les appareils connectés sont multiples du point de vue des consommateurs. Ils touchent à un large éventail de domaines et de questions politiques : vie privée et protection des données, cybersécurité, obsolescence des produits, durabilité et consommation d'énergie, concurrence, sécurité, droits des consommateurs, etc.

Par exemple, les appareils connectés vont collecter de grandes quantités de données sur leurs utilisateurs et leur environnement. Cette collecte généralisée de données soulève un certain nombre de questions pressantes en matière de protection des données et de vie privée. À mesure que de plus en plus d'aspects de notre vie sont intégrés dans un réseau plus vaste de capteurs et de dispositifs, les risques potentiels et l'ampleur des violations de données et des cyberattaques augmentent également. Chaque nouveau dispositif que nous connectons à internet ajoute une nouvelle surface d'attaque potentielle, et la chaîne de dispositifs est souvent aussi forte que le maillon le plus faible. L'émergence et la mise en œuvre de l'intelligence artificielle dans les technologies IoT entraînent également des défis en termes d'équité, de responsabilité, etc.

Parmi les autres défis introduits ou exacerbés par l'internet des objets figurent la limitation artificielle des cycles de vie des produits, les effets de verrouillage et la responsabilité du fait des produits.

Les dispositifs en réseau ont également une consommation d'énergie plus élevée en raison des composants réseau nécessaires. Une grande partie de cette consommation d'énergie provient de la réactivité permanente des appareils sur le réseau (mode de réveil ou de veille). Friedli et al. (2016) ont prévu que les pertes mondiales en mode veille passeront de 7,5 TWh en 2015 à 47 TWh en 2025, en se basant sur la consommation en mode veille des appareils en réseau connectés en permanence au réseau.



3.4. Les principaux droits et obligations des consommateurs en bref

Lorsqu'il s'agit d'appareils connectés, les droits des consommateurs applicables aux appareils non connectés s'appliquent également. Par exemple, les règles relatives à la garantie légale (directive sur le contenu numérique, directive sur la vente de biens) s'appliquent aux produits de consommation IoT. Les règles relatives à l'information des consommateurs (directive sur les droits des consommateurs) au point de vente s'appliquent également. Pour plus d'informations sur la directive sur la vente de biens et la directive sur les droits des consommateurs, nous vous renvoyons vers le document de référence théorique supplémentaire sur le droit général de la consommation. Dans une certaine mesure, les règles de la législation sur la sécurité des produits s'appliquent également aux dispositifs IoT.

Toutefois, en raison de la connectivité de ces appareils, des obligations spécifiques s'appliquent :

1) Premièrement, les dispositifs qui collectent des données personnelles sur les consommateurs doivent s'assurer qu'ils traitent ces données conformément aux règles énoncées dans le RGPD. Ces règles comprennent, entre autres, les principes de minimisation des données, de limitation de la finalité et de protection des données dès la conception, ainsi que l'obligation d'obtenir le consentement de l'utilisateur, en fonction des finalités du traitement des données.

2) Deuxièmement, à partir de 2024, la directive sur les équipements radio exige des fabricants d'appareils connectés qu'ils garantissent que leurs appareils présentent un certain niveau de sécurité. Ces mesures doivent garantir que les dispositifs (i) ne causent pas de dommages au réseau entraînant une dégradation inacceptable du service ; (ii) contiennent des garanties pour assurer la protection des données personnelles et de la vie privée de l'utilisateur et de l'abonné ; et (iii) prennent en charge certaines fonctions de protection contre la fraude, comme les ransomwares.

3) Selon la directive sur les contenus numériques, les appareils connectés doivent recevoir des mises à jour, y compris des mises à jour de sécurité, pendant la période à laquelle le consommateur peut raisonnablement s'attendre. La durée de cette obligation est liée à la période de garantie légale, mais peut aussi être plus longue.

Au niveau national

Les contrats de vente de biens conclus avant le 1^{er} juin 2022 restent couverts par les anciennes règles de garantie introduites par la <https://www.ejustice.just.fgov.be/eli/loi/2004/09/01/2004011364/justel> : La garantie légale couvre le bien de consommation pendant une période de 2 ans (minimum 1 an pour les biens d'occasion) à compter de la délivrance du bien au consommateur. Tout défaut de conformité constaté dans les 6 premiers mois à dater de la délivrance du bien est présumé exister au moment de la délivrance du bien. Passé ce délai, le consommateur sera tenu de prouver que la non-conformité existait au moment de la délivrance du bien. La période de 2 ans est prolongée de la durée nécessaire à la mise en conformité du bien défectueux (réparation, échange, etc.).

Les nouvelles règles en matière de garantie s'appliquent à tous les **contrats de vente de biens conclus à partir du 1^{er} juin 2022**²⁴. La garantie légale s'applique si la non-conformité est constatée dans les deux ans à compter de la délivrance du bien. Dans le cas de biens comportant des éléments numériques²⁵, si le contrat de vente prévoit la livraison continue du contenu numérique ou du service numérique pendant plus de deux ans, le vendeur est responsable de tout défaut de conformité du contenu numérique ou du service numérique qui survient ou devient apparent au cours de la période pendant laquelle le contenu numérique ou le service numérique doit être fourni conformément au contrat de vente.

Si le défaut apparaît dans les deux ans après la livraison, il est présumé exister depuis la livraison. Le vendeur doit prouver le contraire s'il n'est pas d'accord. Dans le cas de biens contenant des éléments numériques, où le contrat de vente prévoit la fourniture continue du contenu numérique ou du service numérique pendant plus de deux ans, la charge de la preuve de la conformité du contenu numérique ou du service numérique (et non du bien lui-même) incombe au vendeur pour les défauts survenus pendant cette période. Le délai de garantie de deux ans est suspendu pendant la période de réparation ou de remplacement. Dans ce cas, après la réparation ou le remplacement, le consommateur ne bénéficiera pas d'un nouveau délai de garantie de deux ans, mais le délai déjà entamé reprend cours à partir du moment du remplacement ou de l'achèvement de la réparation.

Pour les biens d'occasion, le délai de garantie peut être réduit dans le contrat de vente. Cependant il ne peut pas être inférieur à un an et le vendeur doit en informer le consommateur de manière claire et non ambiguë. Si ce n'est pas le cas, une garantie de deux ans s'applique également aux biens d'occasion.

- 4) Quatrièmement, lorsqu'il existe des systèmes de certification applicables à l'appareil connecté en question, le fabricant de l'appareil concerné doit informer les consommateurs, en vertu de la loi sur la cybersécurité, de la période pendant laquelle les utilisateurs finaux bénéficieront d'une assistance en matière de sécurité, notamment en ce qui concerne la disponibilité des mises à jour liées à la cybersécurité.
- 5) Les consommateurs doivent pouvoir s'attendre clairement à ce que l'accès aux services internet soit fourni de manière neutre et non discriminatoire, conformément au règlement sur l'internet ouvert. Les fournisseurs de services Internet doivent traiter tout le trafic Internet de manière égale, sans discrimination, restriction ou interférence ("neutralité du réseau"). Il est essentiel que l'accès à internet reste ouvert et neutre si nous voulons exercer nos libertés fondamentales et nos droits démocratiques et participer aux sociétés en ligne interconnectées d'aujourd'hui. C'est

²⁴ Pour plus d'informations voir [La loi sur la garantie | SPF Economie \(fgov.be\)](#)

²⁵ Pour plus d'informations, voir [Règles de garantie pour le contenu numérique et les services numériques | SPF Economie \(fgov.be\)](#)

également une condition préalable pour bénéficier de l'internet des objets. Les consommateurs ont besoin d'un internet sans restriction et neutre pour utiliser leurs appareils connectés afin d'accéder aux actualités et aux contenus culturels ou pour faire des achats sans restrictions.

- 6) Quant aux règles relatives à la responsabilité concernant la sécurité des produits, la directive pertinente a été rédigée en 1985, bien avant que les gens puissent prendre en compte l'utilisation des appareils connectés, et encore moins prévoir les défis futurs. La directive n'est plus adaptée pour relever les défis de l'internet des objets et pour garantir la réparation des consommateurs en cas de problème. Le processus de révision de cette directive est en cours. En avril 2020, le BEUC a formulé plusieurs recommandations pour que les règles de l'UE en matière de responsabilité du fait des produits restent adaptées aux consommateurs à l'ère du numérique et de l'Internet des objets.

3.5. Lois et règlements au niveau européen

- [Directive 2014/53/UE](#) du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE.
- [Règlement \(UE\) 2019/881](#) ; règlement sur la cybersécurité
- [Directive 2001/95/CE](#) du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité des produits.
- [Directive \(UE\) 2019/770](#) du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques.
- [Règlement \(UE\) 2015/2120](#) établissant des mesures concernant l'accès ouvert à l'internet et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs.
- Rapport de la Commission européenne sur l'[enquête sectorielle sur l'Internet des objets](#) pour les consommateurs

* D'autres lois pertinentes couvertes dans d'autres modules, telles que le RGPD et l'acquis en matière de droits des consommateurs, ne sont pas mentionnées ici mais, comme expliqué ci-dessus, s'appliquent également dans un contexte IoT, comme tout autre produit ou service. Par exemple, si un appareil connecté traite des données personnelles, il devra se conformer au RGPD.

3.6. Jurisprudence

En ce qui concerne la "neutralité du réseau" (voir le point 5 de la section 3.4), la Cour de justice de l'UE a récemment jugé dans les affaires C-854/19, C-5/20 et C-34/20 que les offres



appliquant un "tarif zéro"²⁶ à des applications spécifiques - et donc les restrictions résultant de l'activation de ces options (sur la largeur de bande, le tethering (partage de connexion) ou en cas d'itinérance) - sont contraires à l'article 3, paragraphe 3, du Règlement relatif à l'internet ouvert et donc illégales en vertu du droit communautaire. Les fournisseurs de services doivent donc revoir leurs pratiques commerciales en fonction de cette interprétation afin de garantir le respect total des règles de l'UE en matière de neutralité du réseau. Un raisonnement similaire pourrait être appliqué par la Cour aux fournisseurs de services qui proposent un "tarif zéro " pour les apps connectées aux appareils connectés (par exemple, dans le cadre d'une campagne de marketing, un fournisseur de services Internet propose d'appliquer un tarif avantageux, c'est-à-dire un tarif zéro, sur l'app permettant de contrôler une caméra intelligente).

3.7. Que peuvent faire les consommateurs en cas de problème ?

Des lois différentes s'appliquent aux appareils connectés. En fonction de la loi applicable, les consommateurs ont différentes options :

- S'il s'agit d'une question liée à leurs données personnelles (voir le point 1) de la section 3.4), le RGDP s'applique.
- Selon la directive sur les équipements radioélectriques, en cas de problème de sécurité de leurs appareils (voir la section 2 du chapitre 3.4), à partir de 2024, les consommateurs peuvent en informer leurs autorités nationales de surveillance du marché (souvent l'autorité des télécommunications), qui enquêteront alors sur cet appareil particulier. La décision de l'autorité de surveillance du marché peut même aller jusqu'à ordonner le retrait de ce produit du marché.
- Si l'appareil n'a pas été livré conformément aux attentes des consommateurs en ce qui concerne la fourniture de mises à jour de sécurité (voir le point 3 de la section 3.4), le consommateur a le droit de résilier le contrat, de recevoir une réduction de prix proportionnelle ou d'exiger que l'appareil soit mis en conformité (voir la directive sur les contenus numériques).
- En vertu de la loi sur la cybersécurité, si la livraison des mises à jour de sécurité est plus courte que celle annoncée par le fabricant (voir la section 4 du chapitre 3.4), les consommateurs peuvent se plaindre auprès d'une autorité nationale. Si les consommateurs ne sont pas satisfaits de la décision de l'autorité nationale, ils ont droit à un recours effectif devant les tribunaux.

²⁶ Le "zero rate" est une pratique commerciale par laquelle un ISP applique un "zero rate" (ou un tarif plus avantageux) à tout ou partie du trafic de données associé à une application ou une catégorie d'applications spécifiques offertes par des partenaires de cet ISP.

- Si la neutralité d'internet n'est pas respectée (voir le point 5 de la section 3.4), les consommateurs peuvent se plaindre auprès du régulateur de leur secteur des télécommunications, qui devra y donner suite.

3.8 documentation

- [Étude du SPF Economie](#) sur l'impact sur la réglementation économique. Les domaines économiques étudiés comprennent la protection des consommateurs et les assurances.
- Avis de la Commission consultative spéciale sur la consommation :
 - [L'Internet des objets](#) ;
 - [La responsabilité en matière d'intelligence artificielle](#) ;
 - [Vers la modernisation des droits des consommateurs](#) et [Vers la modernisation et le renforcement de la protection des consommateurs](#) (transposition de la directive omnibus) ;
 - [Transposition des directives européennes sur les ventes aux consommateurs](#).





This document has been produced under a service contract with the European Commission. The content of it represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.