



CONSUMER**PRO**

BOOSTING PROFESSIONALS  
IN CONSUMER PROTECTION

# Digitale rechten

## Theoretisch achtergronddocument

### 2022-2023

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



# INHOUDSOPGAVE

Inhoudsopgave .....	1
Inleiding tot het theoretisch achtergronddocument .....	3
1. Gegevensbescherming.....	4
1.1. Inleiding en geschiedenis van het consumentenbeleid inzake gegevensbescherming .....	4
1.2. Waarom gegevensbescherming belangrijk is voor consumenten .....	4
1.3. Belangrijkste uitdagingen in verband met het consumentenbeleid inzake gegevensbescherming...	5
1.4. De belangrijkste consumentenrechten en -plichten in een notendop .....	5
1.5. Wet- en regelgeving op EU- en nationaal niveau .....	6
1.6. Rechtspraak .....	7
1.7. Wat kunnen consumenten doen als zij een probleem hebben?.....	7
1.8. Verdere bronnen - factsheets, publicaties, links .....	9
2. Platformen .....	10
2.1. Inleiding en geschiedenis van het platformen consumentenbeleid .....	10
2.2. Waarom platformen belangrijk zijn voor consumenten .....	11
2.3. Belangrijkste uitdagingen in verband met platformen .....	11
2.4. De belangrijkste consumentenrechten en -plichten in een notendop .....	15
2.5. Wet- en regelgeving op EU-niveau.....	19
2.6. Rechtspraak .....	21
2.7. Wat kunnen consumenten doen als zij een probleem hebben?.....	21
2.8. Verdere bronnen - factsheets, publicaties, links .....	21
3. Telecommunicatie .....	22
3.1. Inleiding en geschiedenis van het telecommunicatieconsumentenbeleid	<b>Error! Bookmark not defined.</b>
3.2. Waarom telecommunicatie belangrijk is voor de consument .....	<b>Error! Bookmark not defined.</b>
3.3. Belangrijkste uitdagingen inzake de telecommunicatie.....	<b>Error! Bookmark not defined.</b>
3.4. De belangrijkste consumentenrechten en -plichten in een notendop .	<b>Error! Bookmark not defined.</b>
3.5. Wet- en regelgeving op EU-niveau.....	<b>Error! Bookmark not defined.</b>
3.6. Rechtspraak .....	<b>Error! Bookmark not defined.</b>
3.7. Wat kunnen consumenten doen als zij een probleem hebben ?.....	<b>Error! Bookmark not defined.</b>
3.8. Verdere bronnen - factsheets, publicaties, links .....	<b>Error! Bookmark not defined.</b>
4. Bijlage - Lijst van rechtspraak van het HvJEU betreffende de richtlijn inzake elektronische handel...	<b>Error! Bookmark not defined.</b>



Dit materiaal werd geproduceerd in de context van het project Consumer PRO, een initiatief van de Europese Commissie in het kader van het Europese consumentenprogramma. De steun van de Europese Commissie houdt geen goedkeuring in van de inhoud, die uitsluitend de mening van de auteurs weergeeft. De Commissie kan niet verantwoordelijk worden gesteld voor het gebruik dat eventueel wordt gemaakt van de informatie die erin is vervat.



## INLEIDING BIJ HET THEORETISCH ACHTERGRONDDOCUMENT



### Beste lezer,

Dit theoretische achtergronddocument maakt deel uit van de opleidingsmiddelen die zijn ontwikkeld voor Consumer Pro, een EU-initiatief dat tot doel heeft consumentenorganisaties en andere actoren in het consumentenbeleid beter uit te rusten om de consumenten in hun land te beschermen.

Het doel van dit document is om u en uw collega's nuttige en relevante informatie te verschaffen over digitale rechten. De inhoud is opgesteld door BEUC-beleidsdeskundigen op het gebied van digitale rechten, vanuit een Europees perspectief. We proberen u zo te helpen bij:

- Opleiden van uw praktijkmedewerkers,
- Relevante informatie makkelijker te vinden,
- Uw personeel in staat stellen consumenten beter te informeren over hun rechten, en,
- Uw nationale autoriteiten bewust te maken van digitale rechten.

Dit theoretisch achtergronddocument maakt deel uit van een reeks opleidingsinstrumenten. Deze documenten worden telkens aan de nationale context aangepast. Er zijn eveneens theoretische achtergronddocumenten, die u op verzoek kunnen worden toegestuurd, over digitale rechten en over class actions.

### Over Consumer PRO

**Consumer PRO** is een initiatief van de Europese Commissie in het kader van het Europese consumentenprogramma en wordt uitgevoerd door BEUC - de Europese consumentenorganisatie. Dit project heeft tot doel de capaciteit van Europese consumentenorganisaties en andere actoren op het gebied van het consumentenbeleid op te bouwen via niet-formeel onderwijs. Dit project loopt in de EU-lidstaten, IJsland en Noorwegen.

Voor meer informatie kunt u mailen naar [Info@consumer-pro.eu](mailto:Info@consumer-pro.eu)



# 1. GEGEVENSBESCHERMING

## 1.1. Inleiding en geschiedenis van het consumentenbeleid inzake gegevensbescherming

De bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens is een grondrecht in de Europese Unie. Artikel 8, lid 1, van het Handvest van de grondrechten van de Europese Unie en artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU), bepalen dat eenieder recht heeft op bescherming van zijn persoonsgegevens. Daarnaast bepaalt artikel 7 van het Handvest van de grondrechten van de Europese Unie dat iedereen recht heeft op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

De Algemene verordening gegevensbescherming (GDPR) regelt de verwerking van persoonsgegevens in de EU. Zij verplicht organisaties, zowel overheidsinstanties als private bedrijven, om de persoonsgegevens van consumenten op een transparante en eerlijke manier te gebruiken. De verordening versterkt uw rechten en is van toepassing op alle organisaties die persoonsgegevens van personen die zich in de EU bevinden, verwerken. Deze verordening geldt ongeacht waar de organisaties zijn gevestigd.

De regels inzake ePrivacy (de ePrivacy-richtlijn, wordt momenteel herzien) beschermen het vertrouwelijke karakter van elektronische communicatie en bevatten ook specifieke beschermingsmaatregelen voor consumenten tegen ongevraagde commerciële communicatie die via elektronische communicatiediensten wordt verzonden.

## 1.2. Waarom gegevensbescherming belangrijk is voor consumenten

Hoewel digitale informatietechnologieën en de opkomst van **nieuwe onlinediensten gunstig zijn** voor de consument, vormen zij ook een **grote uitdaging voor de grondrechten van de persoonlijke levenssfeer en de bescherming van persoonsgegevens**. De bedrijfsmodellen die momenteel de digitale wereld domineren, zijn gebaseerd op het volgen en analyseren van elke beweging van de consument. Bedrijven gebruiken de informatie die zij verzamelen om gebruikersprofielen op te stellen, die online worden verhandeld. Deze profielen worden dan gebruikt om reclame te kunnen versturen die afgestemd is op het concrete gedrag van de consument. Deze profielen kunnen ook worden gebruikt om consumenten te discrimineren en hun gedrag te beïnvloeden. Het is belangrijk ervoor te zorgen dat consumenten de controle over hun persoonsgegevens kunnen behouden en kunnen genieten van innovatieve digitale producten en diensten zonder dat zij hiervoor hun privacy hoeven op te geven.



### 1.3. Belangrijkste uitdagingen in verband met het consumentenbeleid inzake gegevensbescherming

Het is voor consumenten heel moeilijk om te controleren wat er in de praktijk met hun gegevens gebeurt. Hun rechten worden zeer vaak niet gerespecteerd en zij worden vaak gedwongen hun privacy op te geven als zij digitale producten en diensten willen gebruiken.

Consumenten staan onder voortdurend commercieel toezicht en hun persoonsgegevens worden geëxploiteerd door een groot aantal bedrijven waarvan zij vaak zelfs nog nooit hebben gehoord. Het privacy-beleid is vaag, lang, ingewikkeld en zeer moeilijk te begrijpen. De consument heeft geen andere keuze dan ermee in te stemmen. De consument wordt vaak een illusie van controle gegeven en in de gevallen waarin hem om toestemming wordt gevraagd, gebeurt dit systematisch met een betekenisloos "aankruisvakje".

De GDPR was bedoeld om veel van deze problemen aan te pakken. Bijna vier jaar na de inwerkingtreding zijn er echter nog geen significante veranderingen in de bedrijfspraktijken. De nieuwe verordening lijkt in sommige sectoren weinig te worden nageleefd en de handhaving is momenteel nog niet honderd procent efficiënt. De gegevensbeschermingsautoriteiten hebben moeite met het verwerken van alle klachten die zij ontvangen. Ze hebben dan ook te maken met een reeks van belangrijke uitdagingen in verband met deze nieuwe handhavingsarchitectuur, die is opgebouwd rond een samenwerkings- en consistentiemechanisme om te zorgen voor een samenhangende interpretatie en toepassing van de wet in de hele EU.

Een ander probleem is dat de hervorming van de ePrivacy-regels, die de GDPR moeten aanvullen en de vertrouwelijkheid van communicatie verder moeten beschermen, al meer dan vijf jaar op zich laat wachten en er nog steeds geen akkoord in zicht is. (Voor meer informatie over de ePrivacy-verordening, zie de BEUC-factsheet [hier](#))

### 1.4. De belangrijkste consumentenrechten en -plichten in een notendop

De GDPR verplicht organisaties, zowel overheidsinstanties als bedrijven, om de persoonsgegevens van consumenten op een transparante en eerlijke manier te gebruiken. Zij bevat een reeks [beginselen](#) die het gebruik van persoonsgegevens regelen:

Zij geeft de consumenten ook een [reeks rechten](#) om ervoor te zorgen dat zij controle hebben over hun gegevens. Consumenten hebben onder meer het recht om:

- op duidelijke en gemakkelijk te begrijpen wijze te worden geïnformeerd over de manier waarop hun persoonsgegevens worden gebruikt. Daarbij moet worden gespecificeerd welke gegevens worden gebruikt, door wie en voor welke doeleinden.
- Toegang te krijgen tot de gegevens die organisaties over hen bewaren en een kopie van die gegevens krijgen.
- hun gegevens te corrigeren als ze onjuist zijn.
- Organisaties te vragen hun gegevens te wissen.

- Organisaties te vragen hun gegevens niet langer te gebruiken (tijdelijk of permanent).
- hun gegevens in een algemeen gebruikt formaat te ontvangen, zodat ze die kunnen meenemen en ergens anders gebruiken.
- op hun persoonsgegevens gebaseerde geautomatiseerde besluiten die hen in belangrijke mate treffen (bv. een lening geweigerd krijgen), aan te vechten.
- geïnformeerd te worden als hun gegevens verloren gaan of worden gestolen.
- Een klacht in te dienen bij hun nationale gegevensbeschermingsautoriteit of een bedrijf voor de rechter brengen

## 1.5. Wet- en regelgeving op EU- en nationaal niveau

- [Handvest van de grondrechten van de EU](#)
- [Verordening \(EU\) 2016/679](#) betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (GDPR).<sup>1</sup>
- [Richtlijn 2002/58/EG](#) betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)<sup>2</sup> - Gewijzigd bij [Richtlijn 2009/136/EG](#)<sup>3</sup>
- [Richtsnoeren, aanbevelingen en beste praktijken van het Europees Comité voor gegevensbescherming](#)
- [Adviezen van de Europese Toezichthouder voor gegevensbescherming](#)
- [Voorbeeld van een gedragscode: Federatie van Direct Marketing](#)

---

<sup>1</sup> Omgezet door de [wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens](#).

<sup>2</sup> Omgezet door de [wet van 13 juni 2005 betreffende de elektronische communicatie](#).

<sup>3</sup> Omgezet door de [wet van 10 juli 2012 houdende diverse bepalingen inzake elektronische bepalingen](#).

## Op nationaal niveau

De [wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot gegevensverwerking](#) (die de GDPR verordening uitvoert in Belgisch recht), werd op 5 september 2018 in het Belgisch Staatsblad gepubliceerd. Deze wet vult zo de [wet van 3 december 2017 tot oprichting van de gegevensbeschermingsautoriteit \(GBA\)](#) aan. Deze wet bracht de “Commissie voor de bescherming van de persoonlijke levenssfeer (privacycommissie) in overeenstemming met de regels van het GDPR. De Privacycommissie werd herdoopt tot “gegevensbeschermingsautoriteit”. Momenteel wordt er nagedacht over een aanpassing van deze statuten. [De GBA](#) zelf bepleit vooral een uitbreiding van de middelen.

De gegevensbeschermingsautoriteit is een onafhankelijk controle-orgaan dat als belangrijkste taak heeft de fundamentele principes in verband met de bescherming van persoonsgegevens te garanderen.

De adviezen, aanbevelingen, beslissingen en andere publicaties die de gegevensbeschermingsautoriteit heeft gepubliceerd, vindt u via [deze link](#).

We kunnen hier onder meer specifiek verwijzen naar volgende elementen, waar de gegevensbeschermingsautoriteit de consument via een aantal concrete voorbeelden, beter tracht te duiden wat zijn rechten zijn:

- [Verwerking van persoonsgegevens voor directmarketingdoeleinden, mijn rechten in het kader van directmarketingdoeleinden](#), evenals de pagina “[wat is direct marketing?](#)”
- [Het recht op privacy eindigt niet aan de schoolpoort](#)
- [Het beginsel van toestemming](#)
- [Verschillende analyses over het consumentenkrediet en de Centrale voor Krediet aan Particulieren](#).

## 1.6. Rechtspraak

Voor een overzicht van besluiten van de gegevensbeschermingsautoriteiten en het Hof, en voor artikelen over de GDPR, zie: [www.GDPRHub.eu](http://www.GDPRHub.eu)

Op het officiële EU-rechtsportaal: [Eurlex-dossier over GDPR](#). Dit is een lijst van zaken en prejudiciële vragen van het Hof van Justitie die betrekking hebben op de GDPR: vind de lijst van jurisprudentie onder "*document information*".

## 1.7. Wat kunnen consumenten doen als zij een probleem hebben?

Als de consument van mening is dat zijn rechten uit hoofde van de GDPR zijn geschonden, zijn er twee opties:



- Indienen van een klacht bij de nationale autoriteit voor gegevensbescherming. De volledige lijst van de nationale autoriteiten vindt u [hier](#);
- rechtstreeks een rechtszaak aanspannen tegen een bedrijf/organisatie. Dit belet de consument niet om desgewenst een klacht in te dienen bij de nationale gegevensbeschermingsautoriteiten.

Ook kan de consument, indien hij van mening is dat de gegevensbeschermingsautoriteit zijn klacht niet correct heeft behandeld, indien hij niet tevreden is met het antwoord van de gegevensbeschermingsautoriteit, of indien deze hem niet binnen drie maanden na de dag van indiening van de klacht in kennis stelt van de voortgang of het resultaat, rechtstreeks bij een rechterlijke instantie een vordering instellen tegen de gegevensbeschermingsautoriteit.

### Overheidsinstanties

#### **Op nationaal niveau:**

Naast de gegevensbeschermingsautoriteit, heeft ook de FOD Justitie, directie IV (fundamentele rechten), dienst privacy en gelijke kansen, wetgevende bevoegdheid. Maar de audit- en sanctiebevoegdheid blijft bij de gegevensbeschermingsautoriteit.

Naast de nationale gegevensbeschermingsautoriteiten zijn andere overheidsinstanties die het overwegen waard zijn:

#### **Op Europees niveau:**

- De Europese Commissie, die erop moet toezien dat de lidstaten de GDPR correct uitvoeren en ook de bevoegdheid heeft om sommige bepalingen van de GDPR te "activeren" via gedelegeerde handelingen (bv. voor het creëren van gestandaardiseerde "privacy-pictogrammen").
- Het [Europees Comité voor gegevensbescherming](#) (EDPB), waarin alle nationale gegevensbeschermingsautoriteiten zijn verenigd. Zijn belangrijkste taak is te zorgen voor samenhang bij de toepassing en interpretatie van de GDPR.
- De [Europese Toezichthouder voor gegevensbescherming](#) (ETGB), die erop toeziet dat de EU-instellingen de persoonsgegevens van de burgers respecteren en die de instellingen adviseert over aangelegenheden inzake gegevensbescherming.

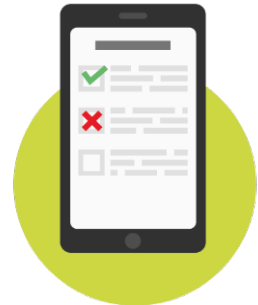
### Alternatieve geschillenbeslechting (ADR)

Buitengerechtelijke procedures en andere procedures voor geschillenbeslechting tussen voor de verwerking verantwoordelijken en betrokkenen met betrekking tot de verwerking van persoonsgegevens kunnen worden vastgesteld via door sectorale organen vastgestelde gedragscodes (artikel 40 GDPR), onverminderd het recht van betrokkenen om klachten in te dienen bij hun gegevensbeschermingsautoriteit en om beroep in te stellen bij de rechter.



## 1.8. Verdere bronnen - factsheets, publicaties, links

- [Website van de Europese Commissie met informatie over GDPR](#)
- [GDPR-bibliotheek van de Europese Commissie - Infografieken, factsheets en ander materiaal voor burgers en bedrijven](#)
- [BEUC Factsheet - Wat betekent de EU-wetgeving inzake gegevensbescherming voor u?](#)
- [AccessNow - Gebruikersgids voor gegevensbescherming in de EU: Uw rechten en hoe u ze kunt uitoefenen](#)
- [Bureau voor de grondrechten - Europees Handboek voor gegevensbescherming](#)
- Door de Europese Toezichthouder voor gegevensbescherming (EDPS) gepubliceerde [informatiebladen](#)
- [De geschiedenis van de GDPR](#) en een [verklarende woordenlijst](#) (EDPS)



## 2. PLATFORMEN

### 2.1. Inleiding en geschiedenis van het platformen consumentenbeleid

Consumenten kopen steeds meer diensten en producten online, met name via platformen.

In de beginjaren van de e-handel vonden dergelijke aankopen vooral plaats op websites van bedrijven die ook over fysieke winkels in de winkelstraten beschikten. Vandaag de dag is het koopgedrag van consumenten radicaal aan het veranderen: steeds meer mensen bestellen via onlinemarktplaatsen diensten en producten die rechtstreeks van buiten de EU naar Europese consumenten worden verzonden.

Aankopen worden niet alleen gedaan via e-commerce platforms zoals Amazon Marketplace, AliExpress, wish.com of eBay, maar ook via sociale media platformen zoals Instagram.

Zo werden in 2017 ongeveer 100 miljoen goederen vanuit China naar Duitsland verzonden. Dat is 40 miljoen meer dan in 2016. Ook in andere Europese landen zijn enorme stijgingen gemeld.

Bovendien worden steeds meer webwinkels in de EU opgezet door verkopers die zich voordoen als Europese bedrijven, maar die in werkelijkheid bestellingen plaatsen op platforms in China en deze producten tegen een hogere prijs (in vergelijking met bijvoorbeeld de prijs op wish.com) aan de consument verkopen. Dergelijke praktijken werden reeds waargenomen in Denemarken en Frankrijk<sup>4</sup>, maar ook in België<sup>5</sup>.

Er bestaan eveneens serieuze bezorgdheden veel van deze producten niet voldoen aan de Europese regels en technische normen die zijn ingevoerd om de rechten van de consument, de gezondheid, veiligheid en het milieu te beschermen. Terwijl fabrikanten en distributeurs die in de EU gevestigd zijn, aansprakelijk kunnen worden gesteld voor productveiligheid en naleving, is dit vaak niet het geval voor producenten die niet in de EU gevestigd zijn, aangezien de tussenpersonen, d.w.z. de platforms voor e-handel, ontkennen de verantwoordelijkheid voor de naleving op zich te nemen.



---

<sup>4</sup><http://www.leparisien.fr/economie/consommation/achats-en-ligne-attention-aux-derives-du-dropshipping-16-01-2020-8237226.php>

<sup>5</sup> Test-aankoop, « hoe kan ik met een lokale onlineaankoop toch bij een Chinese leverancier belanden ? », 19 februari 2021, artikel te raadplegen via volgende link: [Lokale onlineverkoper maar Chinese leverancier \(test-aankoop.be\)](https://www.testaankoop.be/). Ook de BRC Verbruik is aan een advies aan het werken (eenmaal het advies voltooid, kan het [hier](#) geconsulteerd worden).

Er worden op Europees niveau momenteel belangrijke wetgevingsinitiatieven besproken om een aantal van deze problemen aan te pakken, met name het voorstel voor een wet inzake digitale diensten<sup>6</sup> en het voorstel voor een verordening inzake algemene productveiligheid<sup>7</sup>.

## 2.2. Waarom platformen belangrijk zijn voor consumenten


Winkelen, contact leggen met vrienden en familie, ervaringen delen, een film bekijken, naar muziek luisteren, een boek lezen, een reis boeken, een nieuw recept koken, een avondje uit plannen, door een stad trekken, de hulp van de burens inroepen en informatie zoeken op het web; dit zijn slechts enkele basisvoorbeelden van activiteiten die miljoenen consumenten elke dag uitvoeren. Voor elk van deze activiteiten zijn er een of meerdere online platforms die deze diensten faciliteren. Consumenten hebben de opkomst van de platformeconomie omarmd, wat tal van voordelen, maar ook uitdagingen voor de consumentenbescherming, met zich meebrengt.

## 2.3. Belangrijkste uitdagingen in verband met platformen

In het algemeen stonden platforms zoals Google, Amazon of Booking.com nog in de kinderschoenen toen de richtlijn inzake elektronische handel werd vastgesteld (in 2000). Andere tussenpersonen bestonden nog niet eens. Facebook en Shopify werden bijvoorbeeld in 2004 gelanceerd. Etsy werd in 2005 opgericht; Airbnb in 2008. Instagram, Wish en AliExpress zagen het licht in 2010.

**In de afgelopen 20 jaar zijn de bedrijfsmodellen van sommige van deze en andere ondernemingen veranderd. Ook de dynamiek van de marktmacht is veranderd.**

Het Europese digitale marktlandschap heeft een "*dataficatie*" doorgemaakt (de omzetting van informatie in gegevens die de basis vormen van digitale bedrijfsmodellen); een toename van het aantal platforms; een proliferatie van de collaboratieve economie<sup>8</sup>; en een diversificatie van de dienstverleners in termen van functies, verticale integratie en omvang. Toch moet elk bedrijf zich aan de regels houden. Consumentenbescherming hangt niet af - en mag niet afhangen - van de grootte van het bedrijf. De start-up of KMO van vandaag kan immers de Alibaba van morgen worden.



Consumentenbescherming hangt niet af - en mag niet afhangen - van de grootte van het bedrijf. De start-up of KMO van vandaag kan immers de "Alibaba" van morgen worden.

---

<sup>6</sup> [Wet inzake digitale diensten: Zorgen voor meer veiligheid en verantwoordingsplicht online | Europese Commissie \(europa.eu\)](#)

<sup>7</sup> [EUR-Lex - 52021PC0346 - NL - EUR-Lex \(europa.eu\)](#)

<sup>8</sup> [http://www.beuc.eu/publications/beuc-x-2016-030\\_gbe\\_collaborative\\_economy\\_beuc\\_position.pdf](http://www.beuc.eu/publications/beuc-x-2016-030_gbe_collaborative_economy_beuc_position.pdf)

Veel platforms hebben zichzelf opnieuw uitgevonden. Sommige beperken zich niet langer tot hun oorspronkelijke rol van informatieverstrekker of vertrouwde tussenpersoon (bv. vergelijkings- of rangschikkingsplatforms zoals Yelp), maar maken het mogelijk om op het platform transacties te sluiten. Dit zijn bedrijfsmodellen waardoor het platform onder de categorie "*onlinemarktplaats*"<sup>9</sup> valt, waarop de consumentenorganisaties zich momenteel concentreren. Dit type platform wordt in de Omnibus-richtlijn gedefinieerd als "*een dienst die gebruikmaakt van software, waaronder een website, een deel van een website of een door of namens een handelaar beheerde applicatie, en die consumenten in staat stelt op afstand overeenkomsten te sluiten met andere handelaren of consumenten*"<sup>10</sup>. Dit gezegd zijnde, blijft de rol van het platform vaak niet beperkt tot het mogelijk maken van het sluiten van een overeenkomst tussen verkopers en kopers, maar omvat het ook andere diensten zoals betalingsdiensten, fulfilmentdiensten, retourverwerking en klachtenbehandeling <sup>11</sup>.

Andere platformen hebben meerdere rollen gekregen. Er zijn "*hybride platforms*", die verschillende intermediaire functies kunnen combineren, of verticaal geïntegreerde platforms. Deze laatste fungeren niet alleen als tussenpersoon, maar concurreren ook met handelaars, hetzij rechtstreeks, hetzij via verbonden ondernemingen. Amazon is bijvoorbeeld een verkoper, een online marktplaats, een cloud-computing-bedrijf, een video-sharing platform, een uitgever, een reclamebedrijf, een producent van aangesloten apparaten en een kunstmatige intelligentie bedrijf.

Consumentenorganisaties pleiten voor aanpassingen van het wetgevingskader om deze nieuwe marktrealiteit aan te pakken. Het voorstel voor een wet inzake digitale diensten (DSA) is in dit verband een zeer belangrijk initiatief. De Commissie heeft het DSA-voorstel in december 2020 ingediend. Het bevindt zich momenteel in de laatste stadia van het wetgevingsproces. Een akkoord wordt verwacht in 2022.

## *Specifieke uitdagingen*

*Uitdaging #1.* Verspreiding van een breed scala aan illegale inhoud.

Digitale diensten zijn - tot op zekere hoogte - een facilitator geworden voor wijdverspreide inbreuken op de consumentenwetgeving; een inkomstenstroom voor de verkoop van reclame of de promotie van gevaarlijke, onveilige, illegale producten online. Bijvoorbeeld <sup>12</sup>:

---

<sup>9</sup> Vzbv studie,

[https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv\\_gutachten\\_verbraucherrechtliche\\_plattformhaftung.pdf](https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf), p. 17.

<sup>10</sup> Artikel 2, lid 1, onder n), van de richtlijn oneerlijke handelspraktijken, zoals gewijzigd bij Richtlijn 2019/2161", [L\\_2019328NL.01000701.xml \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0216)

<sup>11</sup> Vzbv studie,

[https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv\\_gutachten\\_verbraucherrechtliche\\_plattformhaftung.pdf](https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf), p. 18.

<sup>12</sup> Zie voorbeelden op [https://www.beuc.eu/publications/beuc-x-2019-072\\_new\\_evidence\\_from\\_beuc\\_member\\_organisations\\_regarding\\_dangerous\\_products\\_available\\_online.pdf](https://www.beuc.eu/publications/beuc-x-2019-072_new_evidence_from_beuc_member_organisations_regarding_dangerous_products_available_online.pdf)

	<p>Het Britse lid van de BEUC, Which?, heeft ontdekt dat online kerstboomverlichting wordt verkocht die in brand kan vliegen of consumenten kan electrocuteren<sup>13</sup>.</p>
	<p>De Deense Consumentenraad onthulde dat cosmetica op wish.com niet aan de EU-wetgeving voldoet</p>
	<p>Meer recent hebben zes BEUC-leden vastgesteld dat twee derde van 250 producten die op onlinemarktplaatsen waren gekocht, de veiligheidstests niet hadden doorstaan, met gevolgen zoals elektrische schokken, brand of verstikking.<sup>14</sup></p>
	<p>Het FAVV waarschuwt voor de verkoop van voedingssupplementen online, zoals bijvoorbeeld illegale en potentieel gevaarlijke voedingssupplementen die zouden helpen de immuniteit tegen COVID19 op te krikken<sup>15</sup>.</p>
	<p>Test-Aankoop publiceerde in april 2020 de resultaten van een enquête betreffende producten die op internet verkocht werden (onder meer via AliExpress, LightInTheBox en Amazon) om de tanden te bleken. De kwaliteit van merendeel van deze producten was in het beste geval teleurstellend. Een groot deel van deze producten moeten zelfs afgeraden worden omdat ze meer dan 1% waterstofperoxyde bevatten<sup>16</sup>.</p>

*Uitdaging #2.* Verwarring tussen online marktplaatsactiviteiten en andere platformactiviteiten.

<sup>13</sup> <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/>

<sup>14</sup> <https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html>

<sup>15</sup> [FAVV - Waarschuwing van het FAVV \(favv-afscab.be\)](https://www.favv-afscab.be/)

<sup>16</sup> Test Aankoop, “bleekmiddelen op het net, blijf van je tanden”, april 2020, pp. 36-37.

Het debat over de hervorming van de richtlijn inzake elektronische handel is tot op zekere hoogte toegespitst op kwesties als haat-speechen, terroristische inhoud, auteursrechtelijk beschermd materiaal, vrijheid van meningsuiting of overwegingen in verband met de interne markt. Hoewel dit belangrijke kwesties zijn, mag de EU ook de specifieke problemen in verband met consumentenbescherming niet uit het oog verliezen. Er moet voor worden gezorgd dat consumenten die via onlinemarktplaatsen producten of diensten kopen<sup>17</sup>, volledig worden beschermd.

Er moet een onderscheid worden gemaakt tussen de verkoop van illegale producten en andere activiteiten, bv. het plaatsen van opmerkingen op sociale media. Terwijl in het laatste geval duidelijk sprake is van vrijheid van meningsuiting, gaat het in het eerste geval veeleer om productveiligheid en consumentenbescherming.

*Uitdaging 3.* De richtlijn inzake elektronische handel is "*niet van toepassing op dienstverleners die in een derde land zijn gevestigd*"<sup>18</sup>.

Sommige in derde landen gevestigde dienstverleners maken misbruik van de territorialiteitsbeperkingen van de richtlijn - waardoor een oneerlijk en ongelijk speelveld ontstaat.

*Uitdaging 4.* De manier waarop de eCommerce Richtlijn hosting providers reguleert, wordt door sommige platformen - waaronder (maar niet alleen) online marktplaatsen - gebruikt om zich af te schermen van enige aansprakelijkheid of om geen zinvolle actie te ondernemen uit angst voor aansprakelijkheid.

*Uitdaging #5.* De huidige wetgeving vertoont leemten om onlinemarktplaatsen te reguleren. Er wordt weinig aandacht besteed aan de verrijking van online marktplaatsen door illegale inhoud.

*Uitdaging 6.* De nieuwe regels kunnen voor de lidstaten een belemmering vormen om doelstellingen van algemeen belang correct aan te pakken.

In zaak C-390/18<sup>19</sup> oordeelde het HvJEU bijvoorbeeld dat Airbnb moet worden beschouwd als een dienst van de informatiemaatschappij (artikel 2, onder a), van de richtlijn inzake elektronische handel). Aangezien Frankrijk de Commissie niet in kennis heeft gesteld van een wet die een makelaarsvergunning verplicht stelt voor bedrijven als Airbnb, kan het deze verplichting niet opleggen aan Airbnb, aangezien dit in strijd zou zijn met artikel 3, lid 4, onder b), van de richtlijn inzake elektronische handel. Deze zaak toont aan dat de richtlijn inzake elektronische handel, door de interne markt voorop te stellen, problemen creëert voor lidstaten om wetten en beleid vast te stellen ter bescherming van de consument. Het is echter belangrijk op te merken dat de uitspraak niet betekent dat regeringen dergelijke maatregelen niet kunnen opleggen aan bedrijven als Airbnb.

---

<sup>17</sup> In de EU-omnibusrichtlijn gedefinieerd als "*een dienst die gebruikmaakt van software, waaronder een website, een deel van een website of een door of namens een handelaar beheerde applicatie, en die consumenten in staat stelt op afstand overeenkomsten te sluiten met andere handelaren of consumenten*". Dit gezegd zijnde, blijft de rol van het platform vaak niet beperkt tot het mogelijk maken van het sluiten van een overeenkomst tussen verkopers en kopers, maar omvat het ook andere diensten zoals betalingsdiensten, fulfilmentdiensten, retour en verwerking en klachtenbehandeling.

<sup>18</sup> Richtlijn inzake elektronische handel, overweging 58.

<sup>19</sup> <http://curia.europa.eu/juris/documents.jsf?num=C-390/18>

Het HvJEU was duidelijk dat de kennisgevingsverplichting in de richtlijn inzake elektronische handel *"niet beoogt te voorkomen dat een lidstaat maatregelen vaststelt die binnen zijn eigen bevoegdheid vallen en die de vrijheid van dienstverrichting kunnen aantasten, maar dat een lidstaat in beginsel inbreuk maakt op de bevoegdheid van de lidstaat waar de betrokken verlener van de dienst van de informatiemaatschappij is gevestigd."*

We kunnen eveneens verwijzen naar de Belgische rechtspraak inzake Uber. Het Brusselse Hof van Beroep heeft via een arrest van 15 januari 2021, beslist dat de UberXApplicatie niet in overeenstemming is met de Brusselse taxi- regelgeving. De Brusselse UberX- worden zo schuldig geacht aan oneerlijke concurrentie. Deze beschikking zou echter kunnen worden uitgelegd als strijdig met het Europese mededingingsrecht en de hierboven aangehaalde rechtspraak. Om te ontsnappen aan de verplichtingen die eigen zijn aan de sterk gereguleerde sector, meent Uber dat zij enkel een dienst verleent die erin bestaat personen online met elkaar in contact te brengen, los van de dienst die personen aan elkaar verlenen. Hierdoor zou het kunnen profiteren van de speciale regeling waarin de richtlijn inzake elektronische handel voorziet (die platforms vrijstelt van elke vergunningsregeling (zoals vergunningen) om hun onlineactiviteiten uit te voeren).

*Uitdaging 7.* Gebrek aan goed toezicht en handhaving.

Digitale markten evolueren razendsnel en de bevoegde autoriteiten lijken daar niet tegen opgewassen en beschikken niet over alle deskundigheid of middelen die nodig zijn om de problemen van de markt te monitoren en aan te pakken.

## 2.4. De belangrijkste consumentenrechten en -plichten in een notendop

De **richtlijn inzake elektronische handel** is lange tijd een van de hoekstenen van het internet geweest. In de richtlijn inzake elektronische handel zijn onder meer het beginsel van het land van oorsprong met enkele belangrijke uitzonderingen (met name consumentencontracten), belangrijke informatieverplichtingen ten aanzien van de ontvangers van diensten (bv. consumenten) en aansprakelijkheidsvrijstellingen en -beperkingen voor online-dienstverleners die als tussenpersoon optreden, vastgesteld:

- **Artikel 1 - 3 : Algemene bepalingen**

- **Artikel 4 - 15 : Beginselen**

Afdeling 1: Vestigings- en informatievoorschriften

Afdeling 2: Commerciële communicatie

Afdeling 3: Online-contracten

Afdeling 4: Aansprakelijkheid van de tussenpersoon

- **Artikelen 16 - 20 : Uitvoering**

- **Artikelen 21 - 24 : Slotbepalingen**



Waar vindt u de belangrijkste bepalingen in de richtlijn inzake elektronische handel?

- **Hoofddoelstelling:** interne markt en vrijheid om diensten van de informatiemaatschappij te verlenen (artikel 1).
- **De doelstellingen** zijn onder meer "*rechtszekerheid en consumentenvertrouwen*" (overweging 7), het waarborgen van een hoog niveau van consumentenbescherming en de bescherming van minderjarigen (overweging 10)
- **Werkingsfeer:** onverminderd de bescherming van de consument (artikel 1)
- **Definities** (Artikel 2)
- **Basisinformatie** aan consumenten en andere ontvangers (artikelen 5, 6 en 10)
- **Rechten bij het plaatsen van online bestellingen** (artikel 11)
- **Beginselen van de aansprakelijkheid van tussenpersonen** (artikelen 12-15). De belangrijkste beginselen hier zijn:
  - Hostingproviders zijn niet aansprakelijk voor inhoud van derden zolang zij, zodra zij ervan op de hoogte zijn, illegale inhoud met spoed verwijderen of de toegang daartoe onmogelijk maken (artikel 14)
  - Verbod voor de lidstaten om dienstverrichters een algemene toezichtverplichting op te leggen (artikel 15)
- **Gedragscodes** (artikel 16)
- **Alternatieve geschillenbeslechting** (artikel 17)
- **Gerechtigde stappen** "*om een einde te maken aan de vermeende inbreuken en om te verhinderen dat de betrokken belangen verder worden geschaad*" (artikel 18)
- **Samenwerking tussen de lidstaten** (artikel 19)
- **Sancties** (artikel 20)

Sinds de vaststelling van de richtlijn inzake elektronische handel in 2000 hebben digitale diensten zich verder ontwikkeld, waardoor nieuwe uitdagingen zijn ontstaan. Zo gebruiken sommige platforms het "safe harbour"-beginsel om niet aansprakelijk te kunnen worden gesteld. Sommige aanbieders van digitale diensten nemen geen betekenisvolle verantwoordelijkheid en bieden de consument geen behoorlijke verhaalsmogelijkheden als er iets misgaat. Sommige vrijwillige initiatieven hebben bovendien de broodnodige regelgevende acties vertraagd. Een aantal van deze kwesties wordt aangepakt in het kader van de komende wet inzake digitale diensten.

## 2.5. Vooruitzichten: De Europese wet inzake digitale diensten in ontwerp

De Europese wet inzake digitale diensten (DSA) in ontwerp zal de verplichtingen reguleren van digitale diensten die als tussenpersoon optreden in hun rol van het verbinden van consumenten met goederen, diensten en inhoud.

Het doel is consumenten en hun fundamentele rechten online beter te beschermen, een efficiënt kader voor transparantie en verantwoordingsplicht voor onlineplatforms tot stand te brengen, en zo eerlijkere en meer open digitale markten te bevorderen.

In tegenstelling tot de richtlijn inzake elektronische handel is de DSA een verordening, zodat de regels in de hele EU zullen worden geharmoniseerd en rechtstreeks van toepassing zullen zijn. De nieuwe regels moeten alle burgers in de EU hetzelfde niveau van bescherming bieden.

De DSA zal onder meer volgende maatregelen bevatten<sup>20</sup> :

- Maatregelen om illegale online-inhoud, met inbegrip van goederen en diensten, tegen te gaan, zoals een mechanisme voor gebruikers om dergelijke inhoud te markeren en voor platforms om samen te werken met "betrouwbare markeerders";
- Nieuwe regels voor de traceerbaarheid van zakelijke gebruikers op onlinemarktplaatsen (ook bekend als de "ken-uw-bedrijfsklantenverplichting"), gericht op een betere identificatie van verkopers van illegale goederen;
- waarborgen voor gebruikers, met inbegrip van de mogelijkheid om besluiten moderatoren van platformen (waarbij ze bepaalde inhoud werven) aan te vechten;
- extra transparantiemaatregelen voor onlineplatforms, onder meer met betrekking tot de algoritmen die voor aanbevelingen worden gebruikt en met betrekking tot gerichte reclame;
- verplichtingen voor zeer grote onlineplatforms om misbruik van hun systemen te voorkomen, met name door systeemrisico's aan te pakken en toezicht te houden op de maatregelen die zij nemen via onafhankelijke audits;
- een nieuwe toezichtstructuur om de complexiteit van de onlineruimte aan te pakken, waarbij de lidstaten de hoofdrol zouden spelen, ondersteund door een nieuwe Europese raad voor digitale diensten. Voor zeer grote onlineplatforms zou de Commissie een grotere rol krijgen op het gebied van toezicht en handhaving.



<sup>20</sup> Dit is een algemeen overzicht van enkele van de elementen die naar verwachting zullen worden opgenomen in de definitieve tekst van de verordening, die nog wordt besproken

Hoewel de DSA voor de broodnodige verbeteringen op het gebied van consumentenbescherming bij digitale diensten zal zorgen, is het onwaarschijnlijk dat er grote veranderingen zullen optreden op het gebied van de aansprakelijkheidsregeling voor onlinemarktplaatsen. De DSA zal hoogstwaarschijnlijk de beginselen van de vrijstelling van aansprakelijkheid van tussenpersonen van de richtlijn inzake elektronische handel handhaven, zij het met enkele verduidelijkingen en kleine verbeteringen.



## 2.5. Wet- en regelgeving op EU-niveau

VERORDENING / RICHTLIJN	DATUM VAN TOEPASSING	HERZIENING / EVALUATIE: TYPE MAATREGEL	VERPLICHTINGSDATUM	COMMENTAAR
<a href="#">Richtlijn e-handel</a>	17/01/2002 (omzetting)	EC-verslag van heronderzoek (art. 21)	Vóór 17/07/2003, en daarna om de twee jaar	<a href="#">Sinds 2012</a> is ons geen formele evaluatie bekend. <a href="#">Het sectorale onderzoek van de Commissie van 2017</a> kan interessant zijn vanuit mededingingsoogpunt.
		Verordening digitale diensten (DSA)	Voorstel gepubliceerd in december 2020 - Momenteel in de laatste fase van de medebeslissingsprocedure. Wordt naar verwachting in 2022 goedgekeurd	DSA-voorstel ingediend in december 2020, samen met de Digital Markets Act (DMA), die specifieke regels heeft gericht op gatekeeper-platformen.  De belangrijkste onderwerpen in de DSA vanuit het oogpunt van de consument: <ul style="list-style-type: none"> <li>- aansprakelijkheid en verantwoordelijkheid van tussenpersonen, met name onlinemarktplaatsen;</li> <li>- verplichtingen inzake ken-uw-bedrijfsklanten,</li> <li>- procedures voor notice and action,</li> <li>- transparantievereisten,</li> <li>- handhaving en coördinatie tussen de lidstaten,</li> <li>- verplichtingen in verband met gerichte reclame en het gebruik van aanbevelingssystemen.</li> </ul>
	12/07/2020	EC-richtsnoeren betreffende de transparantievereisten voor rangschikkingen (artikel 5)	Gepubliceerd op 7 december 2022	

<a href="#">Platform voor regelgeving voor bedrijven</a> (P2B-verordening)		EC moet gedragscodes aanmoedigen (art. 17)	Geen datum	Een analyse van hun functioneren zal deel uitmaken van de evaluatie.
		EC-evaluatieverslag (artikel 18)	13/01/2022 en elke drie jaar	
<a href="#">Omnibusrichtlijn</a>	28 november 2021 (omzetting) 28 mei 2022 (toepassing)	Artikel 7 - Omzetting	Artikel 6 - Verslaglegging door de Commissie en evaluatie. Verslag te publiceren door EC tegen 28 mei 2024, regels over voedingsproducten en over huis-aan-huisverkoop maatregelen.	



## 2.6. Rechtspraak

- **Omnibusrichtlijn:** nog geen rechtspraak omdat deze pas vanaf 28 mei 2022 van toepassing wordt. Raadpleeg het theoretisch achtergronddocument over consumentenrecht om de rechtspraak over andere instrumenten van het consumentenrecht te kennen.
- **Richtlijn e-handel:** - klik [hier](#) voor de volledige lijst van zaken.

## 2.7. Wat kunnen consumenten doen als zij een probleem hebben?

- Voorkomen is beter dan genezen: De [FOD Economie](#) geeft een aantal richtlijnen over hoe een consument een frauduleuze webshop kan erkennen.
- Neem contact op met de verkoper/het platform
- Alternatieve geschillenbeslechting (ADR) mogelijk
- Bevoegde autoriteiten van de lidstaten: dit verschilt van land tot land en van onderwerp tot onderwerp.

### Nationale autoriteiten

**Regelgevende autoriteit:** FOD Economie ([Online](#) | [FOD Economie \(fgov.be\)](#))

**Meldpunt FOD Economie** (let op, de economische inspectie onderzoekt geen individuele klachten. Toch blijft het nuttig eventuele problemen aan het meldpunt te melden. De economische inspectie kan steeds een algemeen onderzoek instellen): [Waar en hoe een probleem signaleren?](#) | [FOD Economie \(fgov.be\)](#)

Voor klachten **ten opzichte van Belgische e-handelaars**, zijn volgende 2 ombudsdiensten bevoegde:

- Consumentenombudsdienst: [Klacht indienen](#) | [Consumententombudsdienst \(consumentenombudsdienst.be\)](#)
- Ombudsman van de handel: [Ombudsman voor de Handel](#).
- Het Belmed platform (online bemiddeling commerciële geschillen): [Belmed: onlinebemiddeling van commerciële geschillen](#) | [FOD Economie \(fgov.be\)](#)

Voor klachten **ten opzichte van Europese e-handlaars**, kan je contact opnemen met ECCNet: [Contact - ECC België \(eccbelgie.be\)](#)

## 2.8. Verdere bronnen - factsheets, publicaties, links

- Presentatie van de Europese Commissie over de instrumenten en doelstellingen van de richtlijn inzake elektronische handel (zie [hier](#))



- Standpunt van het BEUC om de consumentenbescherming in de platformeconomie te waarborgen: ([hier](#))
- BEUC-standpuntnota "collaboratieve economie" ([hier](#))
- Standpunt van het BEUC over de wet inzake digitale diensten (DSA) ([hier](#))
- BEUC position paper over het DSA voorstel ([here](#))
- BEUC factsheet over het DSA voorstel ([here](#))
- Briefing van het Europees Parlement over het DSA voorstel ([here](#))
- Q&A van de Europese Commissie het DSA voorstel ([here](#))

## 3. INTERNET OF THINGS

### 3.1. Inleiding en geschiedenis

In de afgelopen paar jaar zijn "*connected devices*" (verbonden apparaten) alomtegenwoordig geworden in het leven van veel consumenten. Terwijl we vroeger normaal achter een computer zaten om toegang te krijgen tot het internet, hebben we nu overal smartphones bij ons die met het internet zijn verbonden. Tegelijkertijd worden steeds meer alledaagse apparaten om ons heen van sensoren voorzien en met het internet verbonden. Van aangesloten koffiezetapparaten en beveiligingscamera's tot auto's en medische apparatuur, de opkomst van aangesloten apparaten staat algemeen bekend als het "internet van dingen", of IoT.

### 3.2. Waarom is IoT van belang voor consumenten?

De afgelopen jaren zijn verbonden apparaten alomtegenwoordig geworden in het leven van veel consumenten, en de opkomst van verbonden apparaten verandert de manier waarop wij ons leven leiden. Hoewel de digitalisering van apparaten de consument veel voordelen biedt, zijn de risico's en uitdagingen die zij met zich meebrengt even belangrijk, zo niet nog groter. Wat gebeurt er bijvoorbeeld als de serviceprovider van uw smart home-systeem besluit zijn servers uit te schakelen? En wie is er verantwoordelijk als uw smart tv wordt gecompromitteerd (bijvoorbeeld door virussen) of onbruikbaar wordt door een gebrek aan software-updates? En wat met de impact op onze privacy?



Daarom is het belangrijk een duidelijk en toekomstgericht EU-beleid en rechtskader te ontwikkelen dat ervoor zorgt dat de rechten van de consument in deze verbonden omgeving worden gehandhaafd.

### 3.3. Belangrijkste uitdagingen betreffende het IoT

De aansluiting van grote aantallen apparaten op het internet brengt zowel kansen als risico's voor de consument met zich mee. De onderling verbonden wereld belooft meer comfort, vlotte ervaringen (waarbij verschillende stappen naadloos in elkaar overvloeien) en mogelijk een aanzienlijke verbetering van de levenskwaliteit. Geaggregeerde informatie van deze apparaten kan ook leiden tot nieuwe inzichten bij de medische wetenschap, kunstmatige intelligentie en bij stadsplanning.

Een slimme woning vol aangesloten apparaten en sensoren kan bijvoorbeeld de gewoonten en voorkeuren van zijn eigenaar leren kennen en de functionaliteit dienovereenkomstig aanpassen. Tegelijkertijd kunnen de verschillende individuele apparaten met elkaar communiceren. Wanneer bijvoorbeeld een laag hartritme door een smartwatch wordt gedetecteerd, kan een spoedbericht naar het dichtstbijzijnde ziekenhuis worden gestuurd. Personen met zorgbehoeften kunnen lang kunnen langer hun onafhankelijkheid bewaren door mogelijkheden van IoT (bijvoorbeeld bewaking/oppas op afstand, mogelijkheid om vanop afstand deuren te ontgrendelen waardoor de persoon zelf niet meer naar de deur moet lopen,...). In sectoren zoals de industrie en de gezondheidszorg zal het internet van dingen potentieel transformerende effecten hebben op de efficiëntie en de informatievergaring.

Maar de uitdagingen die verbonden apparaten met zich meebrengen zijn veelvoudig vanuit het oogpunt van de consument. Zij raken aan een breed scala van beleidsterreinen en vraagstukken: privacy en gegevensbescherming, cyberveiligheid, veroudering van producten, duurzaamheid en energieverbruik, mededinging, veiligheid, consumentenrechten, enz.

Aangesloten apparaten zullen bijvoorbeeld grote hoeveelheden gegevens verzamelen over hun gebruikers en hun omgeving. Deze wijdverspreide gegevensverzameling geeft aanleiding tot een aantal dringende problemen in verband met gegevensbescherming en privacy. Naarmate meer aspecten van ons leven ingebed raken in een groter netwerk van sensoren en apparaten, nemen ook de potentiële risico's en de omvang van gegevensinbreuken en cyberaanvallen toe. Elk nieuw apparaat dat we met het internet verbinden, voegt een nieuw potentieel aanvalsoppervlak toe, en de keten van apparaten is vaak maar zo sterk als de zwakste schakel. De opkomst en implementatie van kunstmatige intelligentie in IoT-technologieën brengt ook uitdagingen met zich mee op het gebied van eerlijkheid, verantwoordingsplicht, enzovoort.

Andere uitdagingen die worden geïntroduceerd of verergerd door het internet van dingen zijn onder meer de kunstmatige beperking van productlevenscycli, lock-in-effecten en productaansprakelijkheid.

Ook hebben netwerkapparaten een hoger energieverbruik door de vereiste netwerkcomponenten. Een groot deel van dit energieverbruik komt voort uit de continue responsiviteit van de apparaten via het netwerk (waakstand of stand-by stand). Friedli et al. (2016) voorspelden dat de wereldwijde stand-byverliezen zullen toenemen van 7,5 TWh in 2015 tot 47 TWh in 2025, op basis van het stand-byverbruik van netwerkapparaten die permanent op het elektriciteitsnet zijn aangesloten.





### 3.4. De belangrijkste rechten en verplichtingen van de consument in een notendop

Wanneer het gaat om aangesloten apparaten, gelden ook de consumentenrechten die van toepassing zijn op niet-aangesloten apparaten. Zo zijn regels inzake wettelijke garantie (richtlijn digitale inhoud, richtlijn verkoop van goederen) van toepassing op IoT-consumentenproducten. Ook regels inzake consumenteninformatie (richtlijn consumentenrechten) op het verkooppunt zijn van toepassing. Zie het aanvullend theoretisch achtergronddocument over het algemeen consumentenrecht voor meer informatie over de richtlijn inzake de verkoop van roerende lichamelijke zaken en de richtlijn inzake consumentenrechten. Tot op zekere hoogte zijn de regels van de wetgeving inzake productveiligheid ook van toepassing op IoT-apparaten.

Vanwege de connectiviteit van deze apparaten gelden er echter specifieke verplichtingen:

- 1) Ten eerste moeten apparaten die persoonsgegevens over consumenten verzamelen, er zeker van zijn dat zij deze gegevens verwerken volgens de regels die in de GDPR zijn vastgelegd. Deze regels omvatten, maar zijn niet beperkt tot, de beginselen van gegevensminimalisering, doelbinding en gegevensbescherming door ontwerp, en de verplichting om de toestemming van de gebruiker te verkrijgen, afhankelijk van de doeleinden van de gegevensverwerking.
- 2) Ten tweede moeten fabrikanten van aangesloten apparaten er volgens de richtlijn radioapparatuur vanaf 2024 voor zorgen dat hun apparaten een bepaald veiligheidsniveau vertonen. Deze maatregelen moeten ervoor zorgen dat de apparaten (i) geen schade toebrengen aan het netwerk waardoor de dienstverlening op onaanvaardbare wijze wordt verslechterd; (ii) waarborgen bevatten om ervoor te zorgen dat de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker en de abonnee worden beschermd en (iii) bepaalde voorzieningen ondersteunen die bescherming bieden tegen fraude, zoals ransomware.
- 3) Volgens de richtlijn digitale inhoud moeten aangesloten apparaten worden voorzien van updates, waaronder beveiligingsupdates, gedurende de periode die de consument redelijkerwijs mag verwachten. De duur van deze verplichting is gekoppeld aan de wettelijke garantieperiode, maar kan ook langer zijn.

#### Op nationaal niveau

Note to trainers: the legal guarantee period is not fully harmonised in the EU. **Some** member states have a longer period than others. Please update as per your country.

Les contrats de vente de biens conclus avant le 1<sup>er</sup> juin 2022 restent couverts par les anciennes règles de garantie introduites par la [loi du 1er septembre 2004 relative à la protection des consommateurs en cas de vente de biens de consommation](#) : 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 1er juin 2022. 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 numériques, 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) Ten vierde moet de fabrikant van het betrokken apparaat, wanneer er certificeringsregelingen bestaan die van toepassing zijn op het betrokken aangesloten apparaat, de consument krachtens de Cybersecuritywet informeren over de periode waarin de eindgebruikers ondersteuning krijgen op het gebied van beveiliging, met name wat betreft de beschikbaarheid van updates in verband met cyberbeveiliging.
- 5) Consumenten moeten er duidelijk van uit kunnen gaan dat de toegang tot internetdiensten overeenkomstig de open-internetverordening op neutrale, niet-discriminerende wijze wordt verleend. Aanbieders van internetdiensten moeten al het internetverkeer gelijk behandelen zonder discriminatie, beperking of inmenging ("netneutraliteit"). Het open en neutraal houden van de internettoegang is van essentieel belang als wij onze fundamentele vrijheden en democratische rechten willen uitoefenen om deel te nemen aan de hedendaagse onderling verbonden online samenlevingen. Het is ook een voorwaarde om te kunnen profiteren van het internet van de dingen. Consumenten hebben een onbeperkt en neutraal internet nodig om hun aangesloten apparaten te kunnen gebruiken om toegang te krijgen tot nieuws en culturele inhoud of om zonder beperkingen te kunnen winkelen.
- 6) Wat de regels inzake productaansprakelijkheid betreft, is de desbetreffende richtlijn - de productaansprakelijkheidsrichtlijn - opgesteld in 1985, lang voordat men rekening kon houden met het gebruik van aangesloten apparaten, laat staan dat men de toekomstige uitdagingen kon voorzien. De richtlijn is niet langer aangepast om de

uitdagingen van het internet van de dingen aan te pakken en om te zorgen voor schadeloosstelling van consumenten wanneer er iets misgaat. Het proces om deze richtlijn te herzien is aan de gang. In april 2020 heeft BEUC verschillende aanbevelingen gedaan om ervoor te zorgen dat de EU-regels inzake productaansprakelijkheid geschikt blijven voor de consument in het digitale tijdperk en voor het internet van dingen.

### 3.5. Wet en regelgeving op Europees niveau

- [Richtlijn 2014/53/EU](#) van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG
- [Verordening \(EU\) 2019/881](#) van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening)
- [Richtlijn 2001/95/EG](#) van het Europees Parlement en de Raad van 3 december 2001 inzake de productveiligheid
- [Richtlijn \(EU\) 2019/770](#) van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten
- Open Internet verordening ([verordening \(EU\) 2015/2120](#)) van 25 november 2015.
- [Verordening \(EU\) 2015/2120](#) tot vaststelling van maatregelen betreffende open-internettoegang en tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten
- Verslag van de Europese commissie over [sectoraal onderzoek naar internet der dingen](#) voor consumenten

\* Andere relevante wetten die in andere modules aan bod komen, zoals GDPR en het acquis inzake consumentenrechten, worden hier niet vermeld maar zijn, zoals hierboven uitgelegd, in een IoT-context ook van toepassing, net als elk ander product of elke andere dienst. Als een aangesloten apparaat bijvoorbeeld persoonsgegevens verwerkt, zal het moeten voldoen aan de GDPR.

### 3.6. Rechtspraak

Wat 'netneutraliteit' betreft (zie punt 5 van hoofdstuk 3.4), heeft het Hof van Justitie van de EU onlangs in de zaken C-854/19, C-5/20 en C-34/20 geoordeeld dat aanbiedingen waarbij een 'nultarief'<sup>21</sup> wordt toegepast op specifieke apps - en dus beperkingen die voortvloeien uit de activering van deze opties (op bandbreedte, tethering of op gebruik bij roaming) - in strijd zijn met artikel 3, lid 3, van de open-internetverordening en dus onwettig zijn volgens

---

<sup>21</sup> Een "nultarief" is een handelspraktijk waarbij een internetprovider een "nultarief" (of een voordeliger tarief) toepast op alle of een deel van het dataverkeer dat samenhangt met een toepassing of een categorie van specifieke toepassingen, aangeboden door partners van die internetprovider.

de EU-wetgeving. Dienstverleners moeten daarom hun commerciële praktijken herzien overeenkomstig deze interpretatie om ervoor te zorgen dat zij de EU-regels inzake netneutraliteit volledig naleven. Een soortgelijke redenering zou door het Hof kunnen worden toegepast op dienstverleners die een "nultarief" aanbieden voor de apps die verbonden zijn met aangesloten apparaten (bv. in het kader van een marketingcampagne biedt een internetdienstverlener een voordelig tarief, d.w.z. een nultarief, aan de app die wordt gebruikt om een slimme camera te bedienen).

### 3.7. Wat kunnen consumenten doen bij een probleem?

Er zijn verschillende wetten van toepassing op aangesloten apparaten. Afhankelijk van de toepasselijke wet, hebben consumenten verschillende opties.

- Als het een probleem is in verband met hun persoonsgegevens (zie punt 1) in hoofdstuk 3.4), is de GDPR van toepassing.
- Volgens de richtlijn radioapparatuur kunnen consumenten, als er een probleem is met de beveiliging van hun apparaten (zie punt 2 in hoofdstuk 3.4), vanaf 2024 hun nationale markttoezichtautoriteiten (vaak de telecomunicatieautoriteit) in kennis stellen, die vervolgens een onderzoek naar dat specifieke apparaat zullen instellen. Het besluit van de markttoezichtautoriteit kan zelfs zo ver gaan dat wordt bevolen dat product uit de handel te nemen.
- Als het apparaat niet is geleverd in overeenstemming met de verwachtingen van de consumenten wat betreft de verstrekking van beveiligingsupdates (zie punt 3 in hoofdstuk 3.4), heeft de consument het recht om de overeenkomst te beëindigen, een evenredige prijsvermindering te krijgen of te eisen dat het apparaat in overeenstemming wordt gebracht (zie richtlijn digitale inhoud).
- Krachtens de Cybersecuritywet kunnen consumenten, als de levering van beveiligingsupdates korter duurt dan door de fabrikant is aangekondigd (zie punt 4 in hoofdstuk 3.4), een klacht indienen bij een nationale instantie. Indien consumenten niet tevreden zijn met het besluit van de nationale instantie, hebben zij recht op een doeltreffende voorziening in rechte.
- Indien de netneutraliteit niet wordt gerespecteerd (zie punt 5 in hoofdstuk 3.4), kunnen de consumenten een klacht indienen bij de regelgevende instantie van hun telecomunicatiesector, die daaraan gevolg zal moeten geven.

### 3.8 documentatie

- [Studie FOD Economie](#) over de impact op de economische reglementering. De economische domeinen die werden onderzocht betreffen onder meer de consumentenbescherming en verzekeringen.
- Advies Bijzondere Raadgevende Commissie Verbruik :
  - [L'Internet of things](#);
  - Digitalisering : Aansprakelijkheid inzake artificiële intelligentie ;
  - [Naar een modernisering van consumentenrechten](#) en [Naar een modernisering en versterking van de consumentenbescherming](#) (omzetting omnibus richtlijn);
  - [Omzetting van de Europese richtlijnen inzake consumentenkoop](#).

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.

