AVIS

CCE 2019-1661

Internet des Objets

CONSOMMATION
Commission consultative spéciale

Avis Internet des Objets

Bruxelles
03.09.2019

Saisine

Dans le cadre de l'exécution par le CCE et le CNT de l'Accord Interprofessionnel 2017-2018, le Bureau du CCE a décidé de faire appel à l'aide de la CCS Consommation sur un certain nombre de questions juridiques liées à la numérisation telles que la vie privée, les aspects relatifs aux assurances, la protection des consommateurs, les pratiques du commerce, … La CCS Consommation a décidé de s'orienter vers le thème de l'Internet des Objets (IdO).

Suite à l'audition sur ce thème du Prof. Eva Lievens le 10 juillet 2018, les organisations des consommateurs ont rédigé une note de discussion. Au cours de la réunion de la sous-commission Digitalisation du 18 janvier 2019, il a été convenu d'approfondir la note avec référence à la législation européenne en préparation. Plus précisément, l'accent serait mis sur l'aspect de la responsabilité. Dans ce cadre le secrétariat a communiqué aux membres un article de M. Jarich Werbrouck relatif à la responsabilité du fait des produits pour les véhicules automoteurs (Tijdschrift voor Privaatrecht).

Une nouvelle note révisée a donc été examinée et discutée par la sous-commission Digitalisation au cours de sa réunion du 1er avril 2019.

Chargée de préparer un projet d'avis, la sous-commission Digitalisation s'est par la suite réunie à cet effet, sous présidence de M. Ducart, les 7 mai et 9 juillet 2019. Ont participé à ses activités : Mmes Dammekens (rapporteur, FEB), Pint (Comeos), Vanden Abeele (Agoria), Van Overbeke (rapporteur, AB-REOC) et MM. Boghaert (CGSLB), Steennot (UGent), Spreuwers (Agoria), Van Oldeneel tot Oldenzeel (Assuralia).

Pour ses activités, la sous-commission a également pu compter sur M. Willaert (SPF Economie).

Le projet d'avis a été soumis mardi 3 septembre 2019, pour approbation, à l'assemblée plénière de la CCS Consommation, qui l'a approuvé sous la présidence de M. Reinhard Steennot.

Introduction

D'un réseau d'ordinateurs interconnectés, le monde évolue rapidement vers un réseau d'objets interconnectés pour créer ce que l'on appelle désormais "l'Internet des Objets".

L'Internet des Objets (abrégé en « IdO » ou anglicisé en « IoT ») fait l'objet d'une abondante littérature et beaucoup de définitions sont utilisées car l'expression est encore jeune et le concept encore en train de se construire. La Commission européenne a aussi naturellement la sienne[1].

[1] Voir le document de travail de la Commission européenne de 2016 [SWD(2016) 110 final, p. 5. Selon ce document de travail, qui n'existe qu'en anglais, « Based on existing communication technologies like the Internet of Things represents the next step towards digitalisation where all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment". Par comparaison, l'UIT (l'union Internationale des Télécommunications) a défini en 2012 l'IdO comme « une « *infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physique ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* ».

Il est par conséquent évident, qu'au milieu de la multitude de ces définitions, on a quelques difficultés à comprendre exactement ce dont on parle. Exprimée de la manière la plus vulgarisée possible, l'IdO a trait à un vaste réseau d'objets physiques qui ont été équipés de la connectivité internet et d'outils pour le collecte et l'échange de données. En bref, dès que l'on parle de l'IdO, on parle d'objets connectés. Et ensuite, tout dépendra du niveau d'intelligence ou d'autonomie dont seront dotés ces différents objets connectés.

En ce qui concerne les perspectives de marché de l'IdO, il faut ainsi s'attendre pour le futur à une mise sur le marché d'objets connectés toujours plus intelligents et toujours plus autonomes qui permettront indubitablement des services plus subtils et mieux adaptés au cas par cas.

Actuellement, néanmoins, le marché de ces objets connectés n'est encore qu'à ses débuts. Mais nombreuses sont déjà les voix qui confirment l'important impact que ce marché aura sur le quotidien des individus et sur la compétitivité des entreprises. Pour les premiers, les objets connectés devraient surtout leur simplifier la vie et leur apporter des réponses innovantes à de multiples besoins essentiels. Pour les seconds, les objets connectés devraient entre autres les aider à créer de nouveaux services à commercialiser.

En outre, ce déploiement à grande échelle d'objets connectés n'est pas sans risque de générer des inconvénients. Il soulève de nombreuses questions complexes en matière de vie privée et de protection des données à caractère personnel, de sécurité, de propriété intellectuelle, d'éthique, de responsabilité, de concurrence, etc.

Initialement, la CCS Consommation a envisagé quatre thématiques touchant à l'IdO et constituant une priorité tant pour les consommateurs que pour les entreprises qui interagissent (in)directement avec celui-ci. Il s'agissait de la sécurité, la responsabilité, la vie privée et la concurrence. Etant donné que ces quatre thèmes sont particulièrement transversaux, il s'est avéré compliqué de formuler des recommandations concrètes. De plus, ils comportent de nombreux aspects qui sont traités actuellement au niveau européen et font l'objet de vives discussions. En outre, concernant la vie privée, le RGDP fête à peine son année d'entrée en vigueur (25.05.18), il convient donc d'attendre qu'il produise pleinement ses effets. Quant à la concurrence, elle touche directement au champ de compétences de la CCS Concurrence. Ainsi, il a finalement été convenu de s'orienter davantage vers un seul thème spécifique, à savoir la responsabilité, que la CCS Consommation a identifié comme problématique essentielle. C'est donc sur celle-ci que va se concentrer plus particulièrement le présent avis car une absence de solutions adéquates pourrait constituer une entrave, d'une part, à une acceptation en masse de l'IdO de la part des consommateurs et, d'autre part, à la poursuite de son développement au détriment des entreprises.

AVIS

1 Remarques générales

La CCS Consommation rejoint le point de vue de la Commission européenne[2] selon lequel l'IdO devrait créer des débouchés et de la croissance pour les entreprises, de nouveaux emplois, un élan pour la compétitivité globale de l'Europe, tout en améliorant la qualité de vie des citoyens.

La CCS Consommation accueille favorablement les initiatives, mesures et propositions législatives élaborées par la Commission européenne qui posent un jalon dans la bonne direction pour essayer de faire face aux défis soulevés par les objets connectés et lever les obstacles à leur déploiement. Elle encourage les autorités belges à assurer un suivi de leur mise en œuvre une fois adoptées et à réagir efficacement si des infractions sont constatées. Le développement des nouvelles technologies et leur accueil par le marché dépendra en partie de la manière dont les éventuels problèmes de responsabilité civile seront appréhendés[3].

2 La cybersécurité

2.1 Le Règlement (UE) 2019/881

Une de ces propositions législatives est devenue, suite à son adoption définitive, le Règlement (UE) 2019/881 (dit « Cybersecurity Act »)[4]. Il y est entre autres prévu d'instaurer un cadre européen de certification volontaire en matière de cybersécurité des produits et services TIC. La CCS Consommation se réjouit que l'UE fasse de la cybersécurité une priorité et estime que les autorités belges devraient à leur tour faire une priorité de l'exécution du Cybersecurity Act. Par ailleurs, la CCS Consommation souligne que la création d'un organisme de certification belge est une méthode pour aider les utilisateurs, y compris les consommateurs, à identifier plus facilement les produits dont la sécurité a été vérifiée par une instance indépendante, mais que ce n'est pas la seule initiative à prendre. Dans l'intérêt de la cybersécurité, il est en effet aussi important de continuer d'investir dans la sensibilisation des consommateurs que dans celle des entreprises. La cybersécurité est en effet encore trop souvent perçue comme un coût inutile, ou du moins comme un point d'attention secondaire, alors que de plus en plus d'exemples de l'actualité montrent que le cybersécurité est *un must*... Il convient donc de prendre en considération les coûts que cela représente, particulièrement pour les consommateurs et les PME, et de mettre à leur disposition des moyens et formations efficaces et accessibles, dans l'objectif de diminuer ces coûts et d'optimiser leur rendement.

---

[2] Commission Staff Working Document, *Advancing the Internet of Things in Europe*, accompanying the document Communication from the Commission tot the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Digitising European Industry Reaping the full benefits of a Digital Single Market, SWD(2016) 110 final.

[3] N. Nevejans, Traité de droit et d'éthique de la robotique civile, Bordeaux, LEH Edition, 2017, p. 553 cité par H. Jacquemin, J.-B. Hubin, « Chapitre 2. - La responsabilité extracontractuelle du fait des robots ou des applications d'intelligence artificielle » dans *L'intelligence artificielle et le droit*, Bruxelles, Éditions Larcier, 2017, pp. 139 à 141.

[4] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no526/2013 (règlement sur la cybersécurité) (JOUE 2019, L151/15).

2.2 La directive SRI

Au vu des risques accrus liés à la cybersécurité au sein des Etats membres, la mise en œuvre intégrale de la directive (UE) 2016/1148 (dite SRI)[5], est particulièrement essentielle pour assurer la sécurité et la résilience des secteurs critiques. Cette directive devait être transposée en droit national pour le 9 mai 2018. La CCS Consommation insiste auprès des autorités belges pour que la loi de transposition du 7 avril 2019[6], adoptée avec près d'un an de retard sur le calendrier, soit rapidement mise en œuvre par l'adoption des arrêtés royaux nécessaires.

La CCS Consommation presse également le gouvernement à accélérer la révision de la stratégie nationale de cybersécurité de 2012, comme exigé par la directive SRI et la loi du 7 avril 2019. De plus, pour supprimer l'incertitude dans laquelle sont actuellement laissées les entreprises concernées, la CCS Consommation recommande aux autorités sectorielles (désignées par l'arrêté royal du 12 juillet 2019[7]) de dresser au plus vite la liste des opérateurs de services essentiels (OSE) et de déterminer quelle partie de leurs activités sera considérée comme service essentiel. Enfin, la CCS Consommation salue la création d'une plateforme de notification sécurisée unique offrant la possibilité de notifier à la fois les incidents SRI et les violations de données à caractère personnel qui en découlent.[8] Elle recommande que cette plateforme soit fonctionnelle le plus vite possible.

Certains appareils et services IdO grand public sont vulnérables aux attaques. Face à cela, la CCS Consommation recommande de considérer plusieurs actions. Premièrement, pour ses propres procédures de passation des marchés, le gouvernement devrait préciser un ensemble de résultats en matière de sécurité. Il doit tirer parti de son rôle en tant que grand acheteur. Ainsi le gouvernement jouerait un rôle d'exemple en matière de sécurité. Deuxièmement, les décideurs politiques devraient informer proactivement la population et les entreprises sur l'importance de la cybersécurité, de la cybersécurité *par design* et sur le coût de celle-ci.

Le déficit de connaissance et de compétence en matière de cybersécurité tant dans le chef des entreprises que chez les consommateurs reste une situation fort préoccupante. La gestion des risques est toutefois incontournable. Un moyen de les réduire est de suivre un certain nombre de règles de base de sécurité (« cyber-hygiène »). Malgré les importants efforts des acteurs clés, ces règles de base restent malheureusement insuffisamment connues et les canaux de diffusion utilisés restent limités dans leur nombre et dans le temps. Par exemple, le CCB (Centre pour la Cybersécurité Belgique) , en association avec la Cyber Security Coalition, organise chaque année en octobre une campagne de sensibilisation à la cybersécurité sur son site web en attirant l'attention sur un thème précis.[9] De même Test-Achat en association avec Google a lancé une campagne sur son site web et un site web dédié pour améliorer la sécurité en ligne[10]. La CCS Consommation recommande dès lors pour améliorer la situation que ces activités de sensibilisation soient organisées de manière régulière et répétée, durant toute l'année, via divers canaux de diffusion proposés en nombre suffisant et accessibles à tous les publics et profils (ex : chaînes de télévision publiques, YouTube, réseaux sociaux, affichages, radios, etc.).

---

[5] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JOUE 2016, L194/1).
[6] *M.B.* 3 mai 2019, p. 42857.
[7] *M.B.* 18 juillet 2019.
[8] Article 31 de la loi précitée du 7 avril 2019.
[9] Voir la dernière campagne de sensibilisation ici de 2018 ici .
[10] Voir la campagne de sensibilisation ici.

3 La transition numérique

Certaines personnes éprouvent des difficultés à opérer la transition numérique car elles n'ont pas les aptitudes, les moyens, les possibilités, l'envie, la volonté ou la capacité d'utiliser des applications et des appareils numériques. Ce phénomène étroitement lié au statut socioéconomique des individus est désigné dans la littérature spécialisée sous l'expression de « fracture numérique ». En Belgique, tout le monde n'est pas suffisamment habile dans l'emploi des TIC : un habitant sur cinq avec un revenu familial faible (21.5%) n'a encore jamais utilisé internet. Pour la catégorie d'âge 55 ans - 74 ans et pour les personnes peu qualifiées, il s'agirait d'une personne sur quatre (24%) (SPF Économie, 2018)[11]. C'est pourquoi la CCS Consommation estime nécessaire, à l'approche de la 5G et au vu des perspectives de marché de l'IdO à grande échelle, que les pouvoirs publics prennent des mesures pour réduire la fracture numérique. Il y a lieu de stimuler de plusieurs manières l'enseignement d'aptitudes numériques simples à la population et la familiarisation de celle-ci à internet pour la recherche d'informations ou l'interaction avec la commune via e-gov. L'étude d'Agoria *Be the Change* pointe les défis à relever pour favoriser la transition numérique. Les pouvoirs publics doivent également stimuler le « digital first » et offrir du soutien là où nécessaire, via les canaux les plus appropriés : CPAS, activités destinées aux seniors et encadrement de ceux-ci, écoles, accompagnement des demandeurs d'emploi, ... Si aucune mesure suffisante n'est prise, la fracture numérique entre les plus forts et les plus faibles sur le plan numérique risque de s'accentuer davantage.

Il ne suffit pas d'avoir les équipements et d'être connecté, le renouvellement permanent des technologies demande un effort d'apprentissage et de remise en question continu, quel que soit le capital de départ de l'individu. De ce fait, la CCS Consommation considère que les autorités ont un rôle important à jouer en mettant en place des politiques publiques inclusives via des programmes (d'accompagnement, de formation, voire de médiation) pensés en faveur de tous, avec une attention particulière à l'égard des couches les moins favorisées et de certaines catégories de personnes plus vulnérables ou moins averties. Les retombées ne pourront qu'être bénéfiques pour tous, y compris pour les entreprises en ligne.

Par ailleurs, les pouvoirs publics doivent veiller à ce que leur service à la population demeure accessible à ceux qui ne sont pas parvenus à franchir le fossé numérique. Les pouvoirs publics doivent prendre des mesures et fournir des outils soit pour donner à ces personnes accès aux nouvelles technologies soit pour proposer une alternative physique, faute de quoi la fracture numérique risque d'augmenter au lieu de diminuer.

4 Les régimes de responsabilité

Les objets connectés, associés de plus en plus à des applications d'intelligence artificielle (et, à l'avenir, à la faculté d'apprentissage automatique) seront de plus en plus autonomes, et ne doivent pas se développer dans un vide juridique.

[11] SPF Economie, « Baromètre de la société de l'information (2018) ».

Les régimes juridiques existants peuvent aisément les approcher sous différents angles en réglementant divers aspects (sécurité, responsabilité d'un dommage, traitement et protection des données). Toutefois, il faut se poser la question de savoir si ces régimes juridiques existants peuvent couvrir ou résoudre adéquatement les nouvelles questions juridiques qui sont soulevées par les objets connectés. Pour cela, il faut tenir compte : (1) des divers niveaux de complexité technique, (2) de la multiplicité des intervenants impliqués à différents titres dans la conception, la fabrication, la production, la distribution et la commercialisation de l'objet connecté et (3) des nouveaux risques engendrés par l'objet connecté.

L'écart entre le rythme rapide de l'innovation technologique et la lenteur des changements législatifs a un impact sur la sécurité juridique. C'est pourquoi la CCS Consommation est convaincue de l'utilité de pointer les principales problématiques liées à l'application des régimes de responsabilité en cas de dommage causé par un objet connecté. Le régime de responsabilité contractuelle ne sera néanmoins pas abordé dans cet avis.

4.1 La responsabilité du fait des produits défectueux

4.1.1 Aperçu des règles applicables

La directive 85/374/CEE concernant la responsabilité du fait des produits défectueux est transposée en droit belge par la loi du 25 février 1991 relative à la responsabilité du fait des produits défectueux[12].

La directive dispose notamment qu'un produit est défectueux lorsqu'il n'offre pas la sécurité à laquelle le consommateur peut légitimement s'attendre compte tenu de toutes les circonstances[13].

Des discussions sont en cours depuis un certain temps déjà, pour savoir si la directive reste adaptée aux défis soulevés par les innovations technologiques (à savoir logiciels, cloud, IdO, etc.), si elle couvre les dommages causés par des applications et des logiciels intégrés défectueux (ex. : compteurs intelligents qui renseignent des données supérieures à la quantité réelle consommée[14]) et si une éventuelle décision autonome inattendue de la part d'un objet connecté (ex. : mauvaise gestion de l'éclairage des pièces de la maison par des éléments domotiques ou accident causé par les navettes autonomes dans le secteur du transport public comme celles mises en circulation et à disposition des passants à Bruxelles par la STIB) pourrait être considérée comme un défaut au sens de la directive. De même, la question de savoir comment imputer la responsabilité sans faute entre les différents participants en cas de dommages causés dans le contexte de l'IdO a également été posée. La Commission européenne a lancé une consultation[15] qui venait à échéance le 26 avril 2019 et a annoncé qu'elle remettrait de la guidance et un rapport à la mi-2019 (dont la publication est toujours attendue à ce jour). Par conséquent, la CCS Consommation est d'avis que les défis soulevés par ces nouveaux produits n'ont pas encore été suffisamment approfondis. Elle suggère dès lors que les autorités compétentes prennent en compte les remarques et éventuelles recommandations reprises dans le rapport.

---

[12] *M.B*, 22 mars 1991, p. 5884.
[13] Art. 6.
[14] Au Pays-Bas, des chercheurs ont testé et comparé 9 compteurs, fabriqués entre 2004 et 2014 : 5 compteurs ont renseigné des données supérieures à la quantité d'électricité réellement consommée avec un écart allant jusqu'à 582% et 2 compteurs ont affiché des relevés 30% inférieurs à la consommation réelle.
[15] Le document de travail de la Commission est disponible ici ; le rapport sur l'application de la directive est disponible ici.

La CCS Consommation souligne qu'elle estime que si de nouvelles initiatives étaient prises, elles devraient l'être à l'échelon européen. Toutefois, les discussions doivent d'ores et déjà avoir lieu au niveau belge pour ne pas prendre trop de retard sur l'expansion des technologies.

4.1.2 Les défis d'application

Défis quant au produit couvert

La loi de transposition du 25 février 1991 est une réplique quasi fidèle de la directive, à une exception près : son champ d'application est limité aux biens meubles corporels (la directive s'appliquant à tous les biens meubles sans se prononcer s'ils sont corporels ou non). Le Code civil belge en cours de modernisation (moyennant l'avant-projet de loi du 28 mars 2018) n'apporte par ailleurs aucun changement en ce qui concerne le champ d'application de la loi de 1991[16].

Dans le contexte de l'IdO, on pourrait considérer que le programme informatique, étant une chose immatérielle, est exclu du champ d'application de la loi belge. Toutefois, à la lecture des travaux parlementaires belges, la loi pourrait trouver à s'appliquer lorsque les données informatiques sont matérialisées sur un support et « une fois introduite dans la machine, ont un effet matériel, concret et bien visible (affichage de résultats, impression sur papier) »[17]. Assimiler le programme informatique au support matériel sur lequel il est enregistré (et ainsi en faire un bien corporel) est également soutenu par la doctrine actuelle majoritaire. Cette interprétation présente l'avantage d'être pragmatique car une décision automatisée d'un objet connecté (p. ex. de fermer une porte) peut causer des dommages physiques à quelqu'un.

Selon certains auteurs[18], le fait qu'un logiciel soit fixé sur un support matériel n'implique pas nécessairement que tous les codes logiciels soient sur ce support (p. ex. lorsque le développeur du programme n'est pas le producteur du support). Or, aujourd'hui, étant donné que des acteurs peuvent être amenés à intervenir sur le programme après la mise en circulation du produit, ils échappent à l'application de la loi du 25 février 1991, alors qu'ils peuvent jouer un rôle décisif dans l'apparition du risque d'accident.

Tout comme dans le cas de la Directive, la CCS Consommation constate que la question de l'application de la loi du 25 février 1991 aux logiciels reste controversée. La CCS Consommation demande dès lors que le législateur lève cette incertitude car il est devenu inconcevable qu'à l'heure actuelle, et encore plus avec l'expansion des objets connectés à grande échelle, les dommages causés par les logiciels défectueux ne puissent pas être réparés. D'autant que la doctrine majoritaire, comme on l'a vu, a tendance à assimiler les logiciels au support matériel sur lequel ils sont enregistrés, ce qui contribue à en faire un bien corporel. Cette incertitude va à l'encontre de la sécurité juridique, tant dans le chef des consommateurs que des entreprises.

---

[16] Art. 5.198 de l'avant-projet de loi du 28 mars 2018 portant insertion des dispositions relatives à la responsabilité extracontractuelle dans le nouveau code civil.

[17] Projet de loi relatif à la responsabilité du fait des produits défectueux, *Doc. Parl.*, Ch. Repr., sess. Ord., 1989-1990, n°1262/5, pp. 5-6; *voy.* également L. DOMMERING-VAN RONGEN, "Productaansprakelijkheid en software", *Computerr.*, 1988, p. 228 cité par J. WERBROUCK, « De productaansprakelijkheid voor zelfrijdende motorrijtuigen », *T.P.R.*, 2018, p. 547; Gent 3 oktober 2007, *Computerr.*, 2008, p. 202 noot E. KINDT.

[18] J. TANGHE, J. DE BRUYNE, "Aansprakelijkheid voor schade veroorzaakt door autonome motorrijtuigen", *R.W.*, n° 25, 18 février 2017, p.979.

Plusieurs pistes de solutions peuvent être envisagées : assimiler les logiciels à des composants ou encore rechercher un critère légal au niveau européen pour déterminer si un logiciel peut être considéré comme un produit au sens de la directive.

La CCS Consommation souligne l'importance de faire le suivi de la guidance annoncée et du rapport de la Commission européenne, ainsi que de sa mise en œuvre éventuelle afin de créer de cette manière de la sécurité juridique par-delà les frontières européennes.

Défis au regard des causes d'exonération de responsabilité

Dans certains cas, les producteurs peuvent être exonérés de leur responsabilité, notamment lorsque le défaut est apparu après la mise en circulation. Toutefois, cette cause d'exonération posera problème dans le cas où le défaut de l'objet connecté provient de son apprentissage et n'est donc pas, par essence, prévisible lors de sa mise en circulation.

Un autre facteur d'exonération de responsabilité est ce que l'on appelle les « risques de développement ou d'innovation ». Il signifie que les producteurs peuvent être exonérés de leur responsabilité s'ils établissent que l'état objectif des connaissances techniques et scientifiques, à son niveau le plus avancé, au moment de la mise en circulation du produit, ne permettait pas de déceler le défaut de celui-ci. Pour qu'elle puisse être valablement opposée aux producteurs, les connaissances pertinentes doivent être accessibles au moment de la mise en circulation du produit en cause[19]. Aujourd'hui, certains Etats membres ont pris l'initiative de déterminer un responsable des risques de développement soit pour tous types de produits (cas du Luxembourg ou de la Finlande) soit pour certains secteurs (par exemple, denrées alimentaires et les médicaments en Espagne, les produits du corps humains dans le cas de la France, les produits pharmaceutiques dans le cas de l'Allemagne). Face à cela, la CCS Consommation constate qu'il y a peu de données disponibles concernant les répercussions pratiques de tels systèmes de responsabilités objectives. En effet, dans quelle mesure cela découragerait-il l'innovation ou engendrerait-il des coûts de mise en œuvre potentiellement exorbitants ? Elle propose alors, dans un premier temps, qu'une étude soit effectuée à cet égard.

Défis par rapport à la charge de la preuve pesant sur la victime

Le régime de responsabilité visé ici impose à la victime de prouver les dommages, la défectuosité du produit et le lien de causalité entre le défaut et les dommages subis. Or, en pratique, il peut s'avérer difficile de prouver qu'un produit était défectueux et/ou qu'un lien de causalité existe, et ce en raison de la complexité technique du produit concerné, du niveau élevé des frais d'expertise ou de la disparition du produit concerné. Dans le cas d'objets connectés cette difficulté est bien réelle. En pratique, un rééquilibrage de la charge de la preuve pourrait être étudié : par exemple, l'éventuel dysfonctionnement d'un objet connecté devrait pouvoir être apprécié en fonction d'un historique fourni par l'objet lui-même, dont le défaut de sécurité pourrait éventuellement être présumé en cas d'accident.

[19] Commission contre Royaume-Uni, C-300/95, arrêt du 30.05.1997, REC. [1997], p. I-2649, point 29;

On pourrait étudier s'il est utile de s'inspirer de la directive 2019/771 relative à la vente des biens[20] qui prévoit que le défaut de conformité qui apparaît dans l'année de la livraison du bien est présumé exister au moment de la livraison, sauf preuve contraire par le vendeur ou si cette présomption est incompatible avec la nature du bien ou du défaut[21].

Bien que le nouveau droit de la preuve permette de renverser la charge de la preuve dans certains cas (nouveau livre 8 du Code civil[22]), la charge de la preuve incombe toujours à la victime dans l'application des règles de responsabilité du fait des produits. Il ne peut être dérogé à cette règle dans le cas de la responsabilité objective prévue par la directive, compte tenu du principe de l'harmonisation maximale. Toutefois, la Cour de justice a reconnu que la preuve d'un défaut et la preuve d'un lien de causalité peuvent être apportées sur la base d'informations sérieuses et concordantes. Une preuve scientifique concluante n'est pas requise et son exigence peut être contraire au principe d'efficacité (voir CJCE 2017, affaire C-621/1).

Enfin, il semble qu'une mise en conformité de la loi belge de transposition soit plus que nécessaire, la dernière modification datant du 12 décembre 2000[23].

4.2 La responsabilité extracontractuelle

Si les quelques articles qui expriment la responsabilité extracontractuelle ont connu une interprétation évolutive du fait de la jurisprudence, nul doute que le déploiement des objets connectés constitue un nouveau défi en la matière.

Tout comme l'homme, les objets connectés peuvent causer un dommage aux personnes avec lesquelles ils interagissent et à leurs biens. Vu que le système actuel d'indemnisation est centré sur la personne humaine, ces technologies de plus en plus autonomes à l'avenir confrontent le droit de la responsabilité extracontractuelle à certaines limites.

4.2.1 La responsabilité du fait personnel (articles 1382 et 1383 du Code civil)

Aperçu des règles applicables

Les articles 1382 et 1383 du Code civil fixent les règles fondamentales de la responsabilité du fait personnel et constituent le régime de droit commun de la responsabilité délictuelle. Selon le premier ; « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer.* » Selon le second qui le complète : *« Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »*

---

[20] *JOUE* 22.05.2019, pp. 28-50.
[21] Art. 11.1.
[22] La loi du 13 avril 2019 portant création d'un Code civil et y insérant le livre 8 « la preuve » (publié au Moniteur belge le 14 avril 2019).
[23] Loi du 12 décembre 2000 modifiant la loi du 25 février 1991 relative à la responsabilité du fait des produits défectueux, *M.B.*, 19.12.2000, p. 42220.

Les difficultés d'application futures

Les objets connectés ne sont ni des humains ni pourvus de conscience et, de part ce fait, ne peuvent être évalués au regard du standard du « bon père de famille », expression qui se réfère de surcroît à un « individu abstrait ».

Toutefois, la CCS Consommation pose les questions suivantes :

Soutenir un concept de « personnalité électronique », comme cela a été évoqué au niveau européen, ne rendrait-elle pas perméable la frontière entre sujet et objet de droit, entre « l'homme et la machine »[24], ou du moins, créer une certaine confusion ?

Comment déterminer si une faute a été commise dans le contexte de l'objet connecté, sans que la possibilité d'obtenir une indemnisation, ne soit rendue trop complexe ? Par exemple, comment la personne lésée pourra-t-elle démontrer son dommage consistant en la perte de certaines données personnelles en raison d'une faille de sécurité causée par l'objet connecté ?

La création d'un standard de sécurité auquel le public peut légitimement s'attendre, compte tenu en particulier du niveau d'information qui lui a été procuré, pourrait-elle être pertinente en l'espèce pour garantir la sécurité juridique ?

Au vu de la complexité des logiciels (plusieurs programmeurs pouvant participer à l'élaboration d'un même logiciel), il sera souvent impossible de déterminer quelle partie du code exactement a fait l'objet de négligence. Comment déterminer quel intervenant aura eu un comportement fautif [25] ?

Par ces interrogations, la CCS Consommation entend attirer l'attention des décideurs politiques sur les difficultés de mise en œuvre du régime de responsabilité du fait personnel aux objets connectés. Difficultés qui ne feront que s'accroître au fur et à mesure que les objets connectés gagneront en autonomie. Il est donc essentiel que les décideurs politiques entament au plus tôt une réflexion pour trancher les questions de responsabilité et d'indemnisations qui y sont liées.

4.2.2 La responsabilité du fait des choses (article 1384 du Code civil)

Aperçu de la règle applicable

L'article 1384, al 1er du Code civil dispose que l'on est responsable du dommage causé par les choses que l'on a sous sa garde. Ce mécanisme ne peut être invoqué que par les personnes directement lésées par le dommage.[26] Il s'agit d'une responsabilité sans faute (objective) dans le chef du gardien de la chose qui verra sa responsabilité engagée même s'il n'avait pas connaissance du vice de l'objet et peu importe l'origine du vice. Les causes d'exonération possibles sont la force majeure et le fait d'un tiers, en lien causal avec le dommage.

---

[24] N. Nevejans, « Règles européennes de droit civil en matière de robotique », 2016, p. 16, http://www.europarl.europa.eu/committees/fr/supporting-analyses-search.html.

[25] Thomas Leemans, La responsabilité extracontractuelle de l'intelligence artificielle. Aperçu d'un système bientôt obsolète, mémoire sous la direction d'Hervé Jacquemin, année académique 2016-2017, master en droit, pp. 11-12.

[26] Cass., 1er ch., 14 février 2013, R.G.I. C.I. 11.0793.F ; Cass., 1ère ch., 4 février 2011, R.G.C.10.0236.N ; Cass., 3ème ch., 22 octobre 2007, R.G.A.R., 2008, n° 14410 et concl. Proc. Gén. Leclercq; Cass., 5 décembre 1997, *J.T.*, 1998, p. 273. Il existe des dérogations pour les personnes subrogées dans leurs droits (ex. : assureurs).

La notion de « chose » est à interpréter largement comme toute chose « corporelle », mobilière ou immobilière, qui est susceptible de garde.

En outre, la Cour de Cassation définit le gardien comme la personne « qui use de cette chose pour son propre compte ou qui en jouit ou la conserve avec un pouvoir de surveillance, de direction et de contrôle »[27].

Enfin, dans le cadre de la modernisation du Code civil, l'avant-projet de loi précité instaure de nouvelles définitions de « chose affectée d'un vice » et de « gardien »[28] ainsi qu'une présomption à charge du gardien, ce qui emportera d'importantes conséquences sur l'application de ce régime et l'interprétation donnée par la jurisprudence.

Les défis d'application

Ce régime pourrait être invoqué pour des dommages causés par des objets connectés. Il pourrait s'agir soit d'un vice « matériel » qui affecte l'objet connecté lui-même soit d'un vice « immatériel » affectant le logiciel implémenté au sein de l'objet connecté. Or, ce dernier, étant vu comme une chose « immatérielle » pourrait être exclu par la jurisprudence de la Cour de Cassation qui refuse l'application de ces dispositions aux choses incorporelles, considérant qu'elles ne sont pas susceptibles d'être gardées.[29] Toutefois, elle a plusieurs fois octroyé réparation concernant des choses complexes (une chose en incorporant une autre) si elle apparaît comme un ensemble aux yeux des tiers. L'exclusion de principe des choses incorporelles est donc aujourd'hui à nuancer. De plus, il n'existe pas de jurisprudence appliquant cette responsabilité au logiciel. Sachant cela, plusieurs questions se posent.

Est-ce que le dommage causé par un logiciel implémenté dans un objet connecté peut être réparé sur la base de ce régime de responsabilité ? Dans la négative, comme la personne lésée pourra-t-elle obtenir réparation lorsque aucun autre régime de responsabilité ne s'applique ?

Ensuite, la cause d'exonération liée au fait d'un tiers à l'origine du vice pourrait-elle être invoquée par le responsable lorsqu'il s'agit d'une erreur de programmation du logiciel implémenté dans l'objet connecté ?

Concrètement, la majorité des consommateurs et des entreprises ayant des connaissances techniques très limitées en la matière, comment appliquer ce régime sans imposer des difficultés disproportionnées aux personnes lésées ?

---

[27] Voy. note Cass.,1ère ch., 13 septembre 2012, R.G. C. 10.0226.F ; Cass., 1ère ch., 18 décembre 2008, R.G. C. 07.0424.F ; Cass., 26 juin 198011, *Pas*, 1980, I, p. 1338 et note.

[28] Article 5.160 de l'avant-projet de loi du 28 mars 2018 portant insertion des dispositions relatives à la responsabilité extracontractuelle dans le nouveau code civil.

[29] Cass., 1er Ch, 21 avril 1972, *Pas*., 1972, I, p. 773.

En effet, comment prouver l'existence d'un vice de fonctionnement affectant un logiciel implémenté au sein d'un objet connecté ? Par exemple, l'hypothèse d'une enceinte intelligente qui déduirait de mauvaises informations de l'historique de recherches de l'utilisateur et se tromperait dans ses préférences pourrait-elle être assimilée à un vice affectant l'objet connecté ? Un résultat anormal donné par un logiciel n'est pas nécessairement un vice[30]. Concrètement, un appareil (par exemple l'enceinte intelligente) qui ne fonctionnerait pas correctement en raison du logiciel pourrait-il être vu comme un ensemble complexe susceptible d'engager la responsabilité de son gardien ? Ainsi, de vives discussions risqueront d'avoir lieu concernant le caractère normal ou anormal des résultats rendus par l'objet connecté[31].

Enfin, concernant la notion de gardien et son pouvoir de surveillance, de direction et de contrôle, certaines incertitudes peuvent d'ores et déjà être formulées quant aux objets connectés. En effet, le logiciel implémenté dans l'objet connecté est une chose incorporelle mais est-il réellement possible de détenir un pouvoir de direction, de contrôle et de surveillance sur un bien immatériel ? Par ailleurs, qui est le gardien d'un programme sous licence (qui n'appartient donc pas au preneur de licence) ?

5 Conclusion

A côté des enjeux de cybersécurité et de transition numérique, les objets connectés révèlent, qu'en matière de responsabilité, de nombreux fondements (contrat, responsabilité délictuelle, du fait des produits défectueux, ..) pourront être invoqués sans tout résoudre et nul doute que les litiges seront potentiellement nombreux eu égard à la chaîne des acteurs et eu égard aussi à la complexité des technologies en cause, rendant délicate la détermination à la fois du fait générateur du dommage et des répartitions de responsabilité. Comme toujours, la CCS Consommation est prête à continuer à apporter sa contribution constructive à toute initiative qui pourrait être prise à l'avenir dans ce domaine.

[30] Cass., 24 février 2006, *Pas*., 2006, p. 442.

[31] H. Jacquemin, J.-B. Hubin, « La responsabilité extracontractuelle du fait des robots ou des applications d'intelligence artificielle » dans *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, p. 126.