COMMISSION
EUROPÉENNE

Bruxelles, le 19.2.2020
COM(2020) 64 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL ET AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN

Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité

RAPPORT SUR LES CONSEQUENCES DE L'INTELLIGENCE ARTIFICIELLE, DE L'INTERNET DES OBJETS ET DE LA ROBOTIQUE SUR LA SECURITE ET LA RESPONSABILITE

1. Introduction

L'intelligence artificielle (IA)[1], l'internet des objets[2] et la robotique seront sources de nouvelles possibilités et de nouveaux avantages pour la société. La Commission a reconnu l'importance et le potentiel de ces technologies, ainsi que la nécessité d'investir massivement dans ces domaines[3]. Elle est déterminée à placer l'Europe à la pointe dans les domaines de l'IA, de l'internet des objets et de la robotique au niveau mondial. La réalisation de cet objectif nécessite l'instauration d'un cadre juridique clair et prévisible permettant de relever les défis technologiques.

1.1. Le cadre existant en matière de sécurité et de responsabilité

L'objectif général des cadres juridiques en matière de sécurité et de responsabilité est de veiller à ce que tous les produits et services, y compris ceux qui intègrent les technologies numériques émergentes, fonctionnent de manière sûre, fiable et cohérente et qu'il puisse être remédié efficacement aux dommages qui surviendraient. La fixation de niveaux élevés de sécurité pour les produits et les systèmes intégrant les nouvelles technologies numériques et la mise en place de mécanismes solides permettant de remédier aux dommages (c'est-à-dire le cadre en matière de responsabilité) contribuent à une meilleure protection des consommateurs. Ces normes et ces mécanismes permettent également d'instaurer un climat de confiance à l'égard de ces technologies, une condition indispensable à leur adoption par les entreprises et les utilisateurs, ce qui permettra de renforcer la compétitivité de notre industrie et de contribuer aux objectifs de l'Union[4]. Un cadre clair en matière de sécurité et de responsabilité revêt une importance particulière lorsque de nouvelles technologies telles que l'IA, l'internet des objets et la robotique émergent, car il permet de garantir à la fois la protection des consommateurs et la sécurité juridique pour les entreprises.

L'Union dispose d'un cadre réglementaire robuste et fiable en matière de sécurité et de responsabilité du fait des produits, ainsi que d'un solide corpus de normes de sécurité, qui sont complétés par des législations nationales, non harmonisées, en matière de responsabilité. Ensemble, tous ces éléments garantissent le bien-être de nos concitoyens au sein du marché unique et encouragent l'innovation et l'utilisation des technologies. Cependant, les caractéristiques de nombreux produits et services traversent en ce moment une phase de transformation du fait de l'IA, de l'internet des objets et de la robotique.

Dans la communication sur l'intelligence artificielle pour l'Europe[5], adoptée le 25 avril 2018, il était annoncé que la Commission présenterait un rapport évaluant les conséquences des

---

1 La définition de l'intelligence artificielle formulée par le groupe d'experts de haut niveau (GEHN IA) est disponible à l'adresse suivante: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

2 La définition de l'internet des objets fournie dans la recommandation UIT-T Y.2060 est disponible à l'adresse suivante: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 et COM(2018) 795.

4 http://ec.europa.eu/growth/industry/policy_en

5 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM%3A2018%3A237%3AFIN

technologies numériques émergentes sur les cadres existants en matière de sécurité et de responsabilité. Le présent rapport vise à recenser et à analyser les conséquences plus générales des cadres en matière de responsabilité et de sécurité pour l'IA, l'internet des objets et la robotique ainsi que leurs lacunes potentielles. Les orientations énoncées dans le présent rapport accompagnant le livre blanc sur l'intelligence artificielle permettront d'alimenter le débat et s'inscrivent dans le cadre de la consultation plus large des parties prenantes. La section relative à la sécurité s'appuie sur l'évaluation[6] de la directive relative aux machines[7] et sur les travaux menés avec les groupes d'experts concernés[8]. La section relative à la responsabilité s'appuie quant à elle sur l'évaluation[9] de la directive sur la responsabilité du fait des produits[10], sur les contributions des groupes d'experts concernés[11] et sur des contacts noués avec les parties prenantes. Le présent rapport n'a pas pour objectif de donner un aperçu exhaustif des règles en vigueur en matière de sécurité et de responsabilité, mais porte sur les principaux problèmes recensés à ce jour.

1.2. Caractéristiques des technologies de l'IA, de l'internet des objets et de la robotique

L'IA, l'internet des objets et la robotique ont de nombreuses caractéristiques en commun. Ces technologies peuvent associer **connectivité**, **autonomie** et **dépendance aux données** pour exécuter des tâches avec peu d'intervention humaine, voire aucune, pour le contrôle ou la supervision. Les systèmes équipés de l'IA sont également capables d'améliorer leurs propres performances grâce à l'apprentissage par l'expérience. Leur **complexité** se traduit à la fois par la pluralité des opérateurs économiques intervenant dans la **chaîne d'approvisionnement** et par la multiplicité des composants, pièces, logiciels, systèmes ou services qui forment ensemble les nouveaux écosystèmes technologiques. À cela s'ajoute l'**ouverture** des produits aux mises à jour et aux mises à niveau après qu'ils ont été mis sur le marché. En raison des grandes quantités de données concernées, de la dépendance aux algorithmes et de l'**opacité** du processus de décisionnel de l'IA, il devient plus difficile de prédire le comportement d'un produit assisté par l'IA et de comprendre les possibles causes d'un préjudice. Enfin, la

---

Le document de travail des services de la Commission (2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) contient un premier recensement des défis que posent les technologies numériques émergentes en matière de responsabilité.

6 SWD(2018) 161 final.

7 Directive 2006/42/CE.

8 Réseau pour la sécurité des produits de consommation tel qu'établi par la directive 2001/95/CE relative à la sécurité générale des produits (DSGP), groupes d'experts au titre de la directive 2006/42/CE relative aux machines et de la directive 2014/53/UE sur les équipements radioélectriques composés de représentants des États membres, d'entreprises et d'autres parties prenantes telles que les organisations de défense des consommateurs.

9 COM(2018) 246 final.

10 Directive 85/374/CEE.

11 Le groupe d'experts sur la responsabilité et les nouvelles technologies a été mis en place dans le but de doter la Commission de connaissances techniques au sujet de l'applicabilité de la directive sur la responsabilité du fait des produits et des règles nationales en matière de responsabilité civile, ainsi que de l'assister dans l'élaboration de principes directeurs en vue de possibles adaptations des lois applicables dans le domaine des nouvelles technologies. Il se compose de deux formations, la formation «responsabilité du fait des produits» et la formation «nouvelles technologies». Voir http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1
Pour le rapport de la formation «nouvelles technologies» sur la responsabilité dans le domaine de l'intelligence artificielle et d'autres technologies émergentes, voir https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

connectivité et l'ouverture peuvent aussi exposer les produits de l'IA et de l'internet des objets à des **cybermenaces**.

1.3. Possibilités créées par l'IA, l'internet des objets et la robotique

Le renforcement de la confiance des utilisateurs à l'égard des technologies émergentes et de l'acceptation de celles-ci dans la société, l'amélioration des produits, des processus et des modèles d'entreprise, ou encore un possible gain d'efficience pour les fabricants européens ne sont que quelques-unes des perspectives offertes par l'IA, l'internet des objets et la robotique.

Au-delà des gains de productivité et d'efficience, l'IA promet également de porter le niveau d'intelligence à des niveaux encore jamais atteints, ouvrant ainsi la voie à de nouvelles découvertes et contribuant à résoudre certains des plus grands problèmes qui se posent au niveau mondial: traitement des maladies chroniques, prévision de l'apparition d'épidémies, réduction des taux de mortalité dans les accidents de la route, ou encore lutte contre le changement climatique et anticipation des menaces qui pèsent sur la cybersécurité.

Ces technologies peuvent apporter de nombreux avantages en améliorant la sécurité des produits et par là même en réduisant leur exposition à certains risques. Par exemple, les véhicules connectés et automatisés pourraient améliorer la sécurité routière, dans la mesure où les accidents de la route résultent la plupart du temps d'une erreur humaine[12]. En outre, les dispositifs de l'internet des objets sont conçus de manière à recevoir et à traiter de grandes quantités de données provenant de différentes sources. Ce niveau d'information accru pourrait être utilisé de manière à permettre aux produits de s'adapter de manière autonome, ce qui les rendrait plus sûrs. Les nouvelles technologies peuvent contribuer à rendre les rappels de produits plus efficaces. Les produits pourraient ainsi avertir les utilisateurs en amont et permettre d'éviter un problème de sécurité[13]. Si un problème de sécurité se pose au cours de l'utilisation d'un produit connecté, les fabricants peuvent communiquer directement avec les utilisateurs afin, d'une part, de les avertir des risques et, d'autre part, pour autant que cela soit possible, de régler directement le problème en lançant, par exemple, une mise à jour de sécurité. Par exemple, au cours du rappel d'un de ses appareils en 2017, un fabricant de smartphones a procédé à une mise à jour logicielle afin de réduire à zéro la capacité de la batterie des téléphones rappelés[14], afin que les utilisateurs cessent d'utiliser les appareils dangereux.

Les nouvelles technologies peuvent en outre contribuer à améliorer la traçabilité des produits. Par exemple, grâce aux fonctions de connectivité de l'internet des objets, les entreprises et les autorités de surveillance du marché peuvent suivre les produits dangereux et déceler les risques dans les chaînes d'approvisionnement[15].

---

[12] Selon les estimations, environ 90 % des accidents de la route sont causés par une erreur humaine. Voir le rapport de la Commission intitulé «Sauver des vies: renforcer la sécurité des véhicules dans l'Union» [COM(2016) 787 final].

[13] Par exemple, le conducteur d'une voiture peut être prévenu qu'il doit ralentir en raison d'un accident survenu plus loin.

[14] OCDE (2018), «Measuring and maximising the impact of product recalls globally: OECD workshop report», *OECD Science, Technology and Industry Policy Papers*, n° 56, Éditions OCDE, Paris, https://doi.org/10.1787/ab757416-en

[15] OCDE (2018), «Enhancing product recall effectiveness globally: OECD background report», *OECD Science, Technology and Industry Policy Papers*, n° 58, Éditions OCDE, Paris, https://doi.org/10.1787/ef71935c-en

Outre les possibilités qu'ils peuvent offrir à l'économie et à nos sociétés, l'IA, l'internet des objets et la robotique peuvent également comporter un risque de préjudice pour des intérêts juridiquement protégés, aussi bien matériels qu'immatériels. Le risque de voir de telles atteintes se produire s'accentuera à mesure que le champ des applications s'élargira. Dans ce contexte, il est essentiel d'analyser si et dans quelle mesure le cadre juridique actuel en matière de sécurité et de responsabilité reste adapté pour protéger les utilisateurs.

2. Sécurité

Dans sa communication intitulée «Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain», la Commission affirme que «***les systèmes d'IA devraient intégrer des mécanismes de sécurité par conception et de sûreté permettant d'en vérifier l'innocuité à chaque étape,*** *en tenant compte de la* ***sécurité physique et mentale*** *de toutes les personnes concernées*»[16].

L'évaluation de la législation de l'Union relative à la sécurité des produits dans la présente section vise à déterminer si le cadre législatif actuel de l'Union est doté des éléments idoines permettant de faire en sorte que les technologies émergentes, et les systèmes d'IA en particulier, intègrent des mécanismes de sécurité par conception et de sûreté.

Le présent rapport examine principalement la directive relative à la sécurité générale des produits[17] ainsi que la législation harmonisée sur les produits qui suit les règles horizontales de la «nouvelle approche»[18] et/ou du «nouveau cadre législatif» (ci-après «la législation ou le cadre législatif de l'Union relatif à la sécurité des produits»)[19]. Les règles horizontales garantissent la cohérence entre les règles sectorielles relatives à la sécurité des produits.

La législation de l'Union relative à la sécurité des produits a pour objectif de veiller à ce que les produits mis sur le marché de l'Union satisfassent à des exigences élevées en matière de santé, de sécurité et d'environnement et qu'ils puissent circuler librement sur tout le territoire de l'Union. La législation sectorielle[20] est complétée par la directive relative à la sécurité générale des produits[21], en vertu de laquelle tous les produits de consommation, même ceux qui ne relèvent pas de la législation sectorielle de l'Union, doivent être sûrs. Les règles de sécurité sont complétées par un mécanisme de surveillance du marché, et les compétences en la matière sont conférées aux autorités nationales dans le cadre du règlement relatif à la surveillance du marché[22] et de la directive relative à la sécurité générale des produits[23]. Dans

---

16 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain, Bruxelles, COM(2019) 168 final du 8.4.2019.

17 Directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits (JO L 11 du 15.1.2002, p. 4).

18 JO C 136 du 4.6.1985, p. 1.

19 Règlement (CE) n° 2008/765 et décision n° 2008/768/CE.

20 Ce régime ne comprend pas la législation de l'Union en matière de transport et de véhicules automobiles.

21 Directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits (JO L 11 du 15.1.2002, p. 4).

22 Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93, JO L 218 du 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj, et, à partir de 2021, règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) n° 765/2008 et (UE) n° 305/201,1 JO L 169 du 25.6.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj

le domaine des transports, la mise en service d'un véhicule à moteur[24], d'un avion ou d'un navire est soumise à des règles supplémentaires édictées au niveau des États membres et de l'UE, et des règles claires régissent la sécurité pendant leur exploitation, précisant notamment les tâches des opérateurs et les tâches des autorités en matière de surveillance.

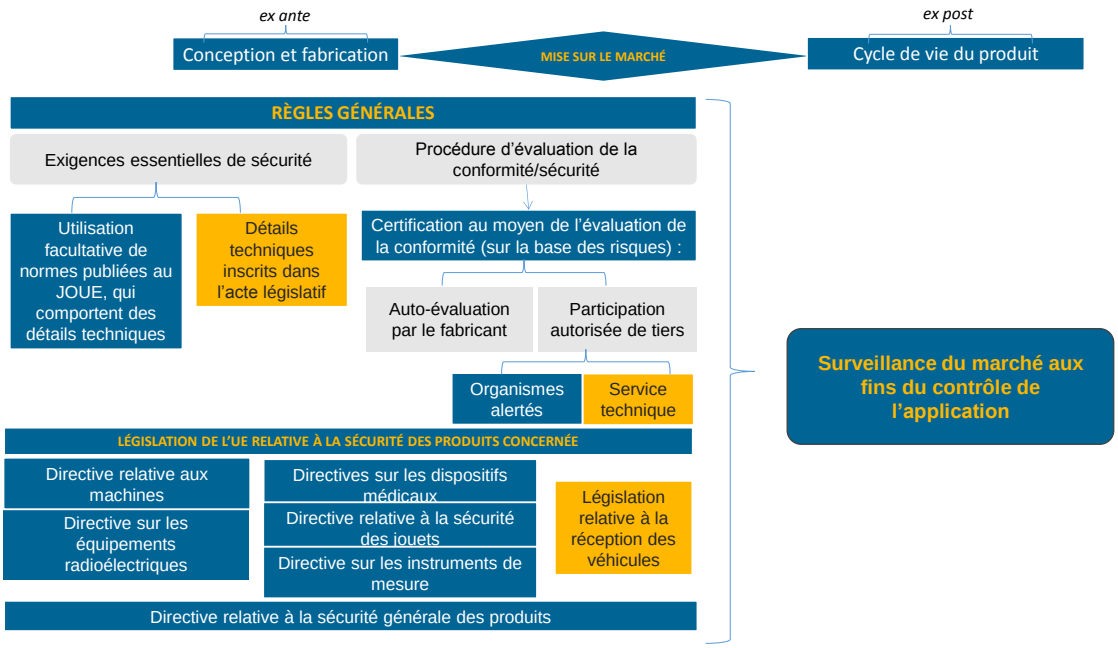
La normalisation européenne est également un élément essentiel de la législation de l'Union relative à la sécurité des produits. Compte tenu de la nature mondiale de la numérisation et des technologies numériques émergentes, la coopération internationale en matière de normalisation revêt une importance particulière pour la compétitivité des entreprises européennes.

Le cadre de l'Union relatif à la sécurité des produits a été en grande partie élaboré avant l'émergence des technologies numériques telles que l'IA, l'internet des objets ou la robotique. Aussi ne contient-il pas toujours de dispositions concernant explicitement les nouveaux défis et les nouveaux risques liés à ces technologies émergentes. Toutefois, la neutralité technologique de l'actuel cadre relatif à la sécurité des produits ne signifie pas pour autant qu'il ne s'appliquerait aux produits intégrant ces technologies. En outre, les actes législatifs ultérieurs qui relèvent de ce cadre, par exemple dans les secteurs des dispositifs médicaux ou des véhicules automobiles, ont déjà tenu explicitement compte de certains aspects de l'émergence des technologies numériques, tels que les décisions automatisées, le logiciel en tant que produit distinct et la connectivité.

[23] Article 8, paragraphe 1, point b), et paragraphe 3, de la directive sur la sécurité générale des produits.

[24] Par exemple, directive 2007/46/CE relative à la réception des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, et règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE.

La logique sous-tendant l'actuelle législation de l'Union relative à la sécurité des produits[25]



Les défis que posent les technologies numériques émergentes pour le cadre de l'Union en matière de sécurité des produits sont exposés ci-après.

La **connectivité** est un élément central d'un nombre sans cesse croissant de produits et de services. Cette caractéristique remet en question le concept traditionnel de sécurité, étant donné que la connectivité peut compromettre la sécurité du produit de manière directe, mais aussi indirecte en cas de piratage du produit, et ainsi faire peser des menaces sur la sécurité et porter atteinte à la sécurité des utilisateurs.

Citons à titre d'exemple l'alerte envoyée par l'Islande dans le cadre du système d'alerte rapide de l'UE au sujet d'une montre intelligente pour les enfants[26]. Ce produit ne nuirait pas directement à l'enfant qui la porte, mais, en l'absence d'un niveau minimum de sécurité, la montre pourrait facilement être utilisée pour entrer en contact avec lui. La fonction initiale du produit étant de garantir la sécurité des enfants au moyen de la localisation, le consommateur ne s'attendrait pas à ce que ledit produit fasse courir aux enfants des risques pour leur sécurité parce qu'il permet de les localiser et/ou d'entrer en contact avec eux.

Citons comme autre exemple une alerte envoyée par l'Allemagne au sujet d'une voiture particulière[27]. La radio du véhicule peut présenter certaines failles de sécurité du logiciel, ce qui permet à des tiers d'accéder sans autorisation aux systèmes de contrôle interconnectés du véhicule. L'exploitation de ces failles de sécurité du logiciel par un tiers à des fins malveillantes pourrait provoquer un accident de la route.

Lorsqu'elles ne possèdent pas les niveaux de sécurité adéquats, les applications industrielles peuvent elle aussi être exposées à des cybermenaces portant atteinte à la sécurité des personnes à plus grande échelle. Tel peut être le cas, par exemple, de cyberattaques contre un

[25] Ce schéma n'inclut pas les exigences législatives relatives au cycle de vie des produits, à savoir l'utilisation et la maintenance, et n'est présenté qu'à titre d'exemple général.
[26] Alerte RAPEX envoyée par l'Islande, publiée sur le site web «Safety Gate» de l'UE (A12/0157/19)
[27] Alerte RAPEX envoyée par l'Allemagne, publiée sur le site web «Safety Gate» de l'UE (A12/1671/15)

système de contrôle critique d'une installation industrielle dans le but de déclencher une explosion susceptible d'entraîner la perte de vies humaines.

La législation de l'Union relative à la sécurité des produits ne prévoit généralement pas d'exigences essentielles spécifiques et obligatoires en matière de cybermenaces portant préjudice à la sécurité des utilisateurs. Il existe toutefois des dispositions relatives aux aspects liés à la sécurité dans le règlement sur les dispositifs médicaux[28], dans la directive sur les instruments de mesure[29], dans la directive sur les équipements radioélectriques[30] ou dans la législation relative à la réception par type de véhicules[31]. Le règlement sur la cybersécurité[32] établit un cadre de certification de cybersécurité facultatif pour des produits, services et processus liés aux technologies de l'information et de la communication (TIC), tandis que la législation pertinente de l'Union relative à la sécurité des produits prévoit des exigences obligatoires.

En outre, le risque de perte de connectivité des technologies numériques émergentes peut également faire peser des menaces sur la sécurité. Par exemple, une alarme incendie connectée qui perd sa connectivité risque de ne pas alerter l'utilisateur en cas d'incendie.

La sécurité est inscrite dans la législation actuelle de l'Union relative à la sécurité des produits en tant qu'objectif de politique publique. Le concept de sécurité est lié à l'utilisation du produit et aux risques (mécaniques, électriques, etc.) auxquels il convient de remédier pour rendre le produit sûr. Il y a lieu de noter qu'en fonction de l'acte législatif de l'Union en matière de sécurité des produits concerné, l'utilisation du produit couvre non seulement l'utilisation prévue, mais aussi l'utilisation prévisible, voire, dans certains cas, comme dans la directive relative aux machines[33], la mauvaise utilisation raisonnablement prévisible.

Le concept de sécurité dans l'actuelle législation de l'Union relative à la sécurité des produits correspond à un concept de sécurité élargi afin de protéger les consommateurs et les utilisateurs. Par conséquent, le concept de sécurité des produits englobe la protection contre tous les types de risques liés au produit et couvre non seulement les risques mécaniques, chimiques et électriques, mais aussi les cyberrisques et les risques induits par la perte de connectivité des dispositifs.

Il pourrait être envisagé d'inclure dans le champ d'application des actes législatifs de l'Union concernés des dispositions explicites à cet égard afin de mieux protéger les utilisateurs et d'assurer une plus grande sécurité juridique.

L'**autonomie**[34] est l'une des caractéristiques principales de l'IA. L'obtention de résultats non souhaités à partir de l'IA pourrait causer un préjudice aux utilisateurs et aux personnes exposées.

---

28 Règlement (UE) 2017/745 relatif aux dispositifs médicaux.

29 Directive 2014/32/UE concernant la mise à disposition sur le marché d'instruments de mesure.

30 Directive 2014/53/UE sur les équipements radioélectriques.

31 Directive 2007/46/CE — réception des véhicules à moteur, de leurs remorques et des systèmes, des composants et des entités techniques destinés à ces véhicules. La directive sera abrogée et remplacée par le règlement (UE) 2018/858 relatif à la réception des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE, avec effet au 1er septembre 2020.

32 Règlement (UE) 2019/881.

33 Directive 2006/42/CE relative aux machines.

34 Si les produits basés sur l'IA peuvent agir de manière autonome en percevant leur environnement et sans suivre une série d'instructions prédéterminées, leur comportement est limité par l'objectif qui leur a été assigné et par d'autres choix de conception pertinents posés par leurs concepteurs.

Dans la mesure où le «comportement» futur des produits de l'IA peut être déterminé à l'avance par l'évaluation des risques effectuée par le fabricant avant que les produits ne soient mis sur le marché, le cadre de l'Union relatif à la sécurité des produits impose déjà aux fabricants de tenir compte, lors de l'évaluation des risques, de l'«utilisation»[35] des produits tout au long de leur cycle de vie. Il impose également aux fabricants l'obligation de fournir des instructions et des informations de sécurité à l'intention des utilisateurs ou des avertissements[36]. Dans ce contexte, par exemple, la directive sur les équipements radioélectriques[37] prévoit que le fabricant doit inclure des instructions contenant des informations sur la manière d'utiliser les équipements radioélectriques conformément à l'utilisation prévue.

On pourrait également être confrontés à l'avenir à des situations dans lesquelles les résultats engendrés par des systèmes d'IA ne peuvent être entièrement déterminés à l'avance. Dans de telles situations, il est possible que l'évaluation des risques effectuée avant la mise du produit sur le marché ne corresponde plus à l'utilisation, au fonctionnement ou au comportement du produit. Dans ces cas, dans la mesure où l'utilisation initialement prévue par le fabricant est modifiée[38] en raison du comportement autonome et où les exigences en matière de sécurité ne sont plus respectées comme il se doit, il pourrait être envisagé d'exiger une réévaluation du produit doté de capacités d'auto-apprentissage[39].

Dans le cadre actuel, le producteur qui constate qu'un produit, tout au long de son cycle de vie, comporte des risques pour la sécurité est tenu d'en informer immédiatement les autorités compétentes et de prendre des mesures visant à prévenir les risques pour les utilisateurs[40].

Outre l'évaluation des risques réalisée avant la mise sur le marché d'un produit, une nouvelle procédure d'évaluation des risques pourrait être mise en place lorsque le produit subit des changements importants au cours de sa durée de vie, par exemple, une fonction de produit différente que le fabricant n'avait pas prévue dans son évaluation initiale des risques. L'accent devrait être mis sur les effets résultant du comportement autonome du produit sur la sécurité, pendant toute sa durée de vie. L'évaluation des risques devrait être effectuée par l'opérateur économique approprié. En outre, les actes législatifs pertinents de l'Union

[35] Dans la législation de l'Union relative à la sécurité des produits, les producteurs effectuent l'évaluation des risques sur la base de l'utilisation prévue du produit, de l'utilisation prévisible et/ou de la mauvaise utilisation raisonnablement prévisible.

[36] Décision nº 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82). L'article R2, paragraphe 7, de l'annexe I est libellé comme suit: «*Les fabricants veillent à ce que le produit soit accompagné d'instructions et d'informations de sécurité fournies dans une langue aisément compréhensible par les consommateurs et autres utilisateurs finals, déterminée par l'État membre concerné.*»

[37] Article 10, paragraphe 8, qui évoque les instructions données à l'utilisateur final, et annexe VI renvoyant à la déclaration de conformité de l'UE.

[38] Jusqu'à présent, «l'auto-apprentissage» est utilisé dans le contexte de l'IA la plupart du temps pour indiquer que les machines sont capables d'apprendre pendant leur formation; le fait que les machines d'intelligence artificielle continuent à apprendre une fois qu'elles ont été déployées n'est pas encore une obligation; au contraire, particulièrement dans le secteur des soins de santé, les machines d'IA cessent normalement d'apprendre dès que leur formation a été clôturée avec succès. Ainsi, à ce stade, le comportement autonome résultant de systèmes d'IA n'implique pas que le produit exécute des tâches que n'ont pas prévues les concepteurs.

[39] Et ce conformément à la section 2.1 du «Guide bleu relatif à la mise en œuvre de la réglementation de l'Union européenne sur les produits 2016».

[40] Article 5 de la directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits.

pourraient revoir à la hausse les exigences imposées aux fabricants en matière d'instructions et d'avertissements destinés aux utilisateurs.

Des évaluations de risques similaires sont déjà requises dans la législation sur les transports[41]. Par exemple, dans la législation relative au transport ferroviaire, lorsqu'un véhicule ferroviaire est modifié après sa certification, une procédure spécifique est imposée à l'auteur de la modification et des critères clairs sont définis afin de déterminer si l'autorité doit être associée, ou non.

La caractéristique d'auto-apprentissage des produits et systèmes d'IA peut permettre à la machine de prendre des décisions qui s'écartent de ce qui était initialement prévu par les fabricants et, par conséquent, du résultat attendu par les utilisateurs. Cela soulève des questions sur le contrôle humain, de sorte que les personnes pourraient choisir de déléguer des décisions aux produits et systèmes d'IA et déterminer la manière de procéder en vue d'atteindre des objectifs qu'elles ont elles-mêmes fixés[42]. La législation existante de l'Union relative à la sécurité des produits ne traite pas explicitement le contrôle humain dans le contexte des produits et systèmes d'IA dotés de capacités d'auto-apprentissage[43].

Les actes législatifs pertinents de l'Union peuvent prévoir des exigences spécifiques pour le contrôle humain, en tant que garde-fou, dès la conception du produit et tout au long du cycle de vie des produits et systèmes d'IA.

Le «comportement» futur des applications d'IA pourrait générer des **risques pour la santé mentale**[44] des utilisateurs résultant, par exemple, de leur collaboration avec des robots humanoïdes et des systèmes d'IA, à la maison ou dans les environnements de travail. À cet égard, aujourd'hui, la sécurité est en général invoquée en rapport avec la menace, perçue par l'utilisateur, d'un dommage physique qui pourrait émaner de la technologie numérique émergente. Parallèlement, dans le cadre juridique de l'Union, les produits sûrs s'entendent comme des produits qui ne présentent aucun risque ou seulement des risques minimaux pour la sécurité et la santé des personnes. Il est communément admis que la définition de la santé inclut le bien-être physique et mental. Toutefois, les risques pour la santé mentale devraient être explicitement couverts par le concept de sécurité des produits dans le cadre législatif.

Par exemple, l'autonomie ne devrait pas causer de gêne ni de stress excessifs pendant de longues périodes ni nuire à la santé mentale. Sur ce point, on considère que les facteurs

---

41 En cas de modification du système ferroviaire susceptible d'avoir des conséquences sur la sécurité (par exemple, modification technique, opérationnelle ou encore organisationnelle susceptible d'avoir une incidence sur le processus d'exploitation ou de maintenance), la procédure à suivre est décrite à l'annexe I du règlement d'exécution (UE) 2015/1136 de la Commission (JO L 185 du 14.7.2015, p. 6).
En cas de «changement significatif», un rapport d'évaluation de la sécurité devrait être remis au proposant par un «organisme d'évaluation» indépendant (par exemple l'autorité nationale de sécurité ou tout autre organisme compétent sur le plan technique).
À la suite de la procédure d'analyse des risques, le proposant appliquera les mesures appropriées pour atténuer les risques (si le proposant est une entreprise ferroviaire ou un gestionnaire de l'infrastructure, l'application du règlement relève de son système de gestion de la sécurité, dont l'application est supervisée par l'ANS).

42 Recommandations pour les actions et les investissements en vue d'une IA digne de confiance, groupe d'experts de haut niveau sur l'intelligence artificielle, juin 2019.

43 Cela n'exclut toutefois pas qu'un contrôle puisse être nécessaire dans une situation donnée en raison de certaines obligations plus générales en vigueur en ce qui concerne la mise sur le marché du produit.

44 Constitution de l'OMS, premier point de l'énumération: «La santé est un état de complet bien-être physique, mental et social et ne consiste pas seulement en une absence de maladie ou d'infirmité» (https://www.who.int/fr/about/who-we-are/constitution).

suivants exercent une incidence positive sur le sentiment de sécurité des personnes âgées[45]: entretenir des relations de confiance avec le personnel des services de soins de santé, disposer d'un contrôle sur les routines du quotidien et en être informés. Les fabricants de robots qui interagissent avec les personnes âgées devraient tenir compte de ces facteurs afin de prévenir les risques pour la santé mentale.

Il pourrait être envisagé d'introduire, dans le champ d'application de la législation pertinente de l'Union, des obligations imposant explicitement aux fabricants, entre autres, de robots humanoïdes basés sur l'IA de tenir expressément compte du préjudice immatériel que leurs produits pourraient causer aux utilisateurs, en particulier aux utilisateurs vulnérables, tels que les personnes âgées dans des environnements de soins.

Une autre caractéristique essentielle des produits et systèmes basés sur l'IA est la **dépendance aux données**. L'exactitude et la pertinence des données sont essentielles pour garantir que les systèmes et les produits basés sur l'IA prennent les décisions prévues à l'origine par le fabricant.

La législation de l'Union relative à la sécurité des produits ne traite pas explicitement les risques pour la sécurité induits par des données erronées. Toutefois, selon l'«utilisation» du produit, les fabricants devraient tenir compte, lors des phases de conception et d'essai, de l'exactitude des données et de leur pertinence pour les fonctions de sécurité.

Par exemple, un système basé sur l'IA conçu pour détecter des objets spécifiques pourrait éprouver des difficultés à reconnaître des objets dans de mauvaises conditions d'éclairage, de sorte que les concepteurs devraient inclure des données provenant d'essais réalisés sur les produits aussi bien dans des conditions normales que dans des environnements mal éclairés.

Un autre exemple a trait aux robots agricoles, tels que les robots cueilleurs de fruits, conçus pour détecter et localiser les fruits mûrs sur les arbres ou au sol. Alors que les algorithmes qui interviennent dans ces opérations montrent déjà des taux de réussite de plus de 90 %, une faille dans les ensembles de données alimentant ces algorithmes pourrait amener ces robots à prendre une mauvaise décision et, par conséquent, à blesser un animal ou une personne.

La question se pose de savoir si la législation de l'Union relative à la sécurité des produits devrait contenir des exigences spécifiques concernant les risques que comportent des données erronées en matière de sécurité au stade de la conception, ainsi que des mécanismes garantissant le maintien de la qualité des données tout au long de l'utilisation des produits et des systèmes d'IA.

L'**opacité** est un autre trait caractéristique de certains produits et systèmes basés sur l'IA qui peut résulter de la capacité qu'ont ces derniers d'améliorer leurs performances grâce à l'apprentissage par l'expérience. En fonction de l'approche méthodologique retenue, les produits et les systèmes basés sur l'IA peuvent être caractérisés par différents degrés d'opacité. De par cette opacité, le processus de prise de décision peut s'avérer difficile à tracer («effet boîte noire»). L'être humain n'a pas forcément besoin de comprendre chaque étape du processus de prise de décision, mais, dans la mesure où les algorithmes d'IA ne cessent d'évoluer et sont déployés dans des domaines critiques, il est crucial qu'il puisse être en mesure de saisir comment les décisions algorithmiques du système ont été prises. Cette compréhension revêt une importance particulière pour les mécanismes ex post d'exécution,

[45] Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, p. 237 à 264, Research, Neziha Akalin, Annica Kristoff ersson et Amy Loutfi, juillet 2019.

car elle permettra aux autorités chargées de faire appliquer la législation de tracer la responsabilité des comportements des systèmes d'IA et des choix qu'ils opèrent. Ce constat ressort également de la communication de la Commission intitulée «Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain»[46].

La législation de l'Union relative à la sécurité des produits ne contient pas de dispositions visant à parer explicitement aux risques croissants liés à l'opacité des systèmes basés sur des algorithmes. Il est donc nécessaire d'envisager de fixer des exigences en matière de transparence des algorithmes, ainsi que de robustesse, d'obligation de rendre des comptes et, lorsqu'il y a lieu, de contrôle humain et de résultats non biaisés[47]; ces exigences seront particulièrement importantes pour garantir le fonctionnement du mécanisme ex post d'exécution et susciter la confiance dans l'utilisation de ces technologies. Pour remédier à ce problème, une solution consisterait à imposer aux concepteurs des algorithmes de divulguer les paramètres de conception et les métadonnées des ensembles de données en cas d'accident.

Parmi les autres risques susceptibles d'avoir une incidence sur la sécurité figurent ceux liés à la **complexité des produits et des systèmes**, lesquels peuvent intégrer divers composants, dispositifs et produits dont le fonctionnement influence celui des autres (comme c'est le cas des différents produits qui composent un écosystème de maison intelligente).

Cette complexité est déjà prise en compte par le cadre juridique de l'UE en matière de sécurité mentionné au début de la présente section[48]. Plus particulièrement, lorsqu'un fabricant évalue le risque présenté par un produit, il doit tenir compte de l'utilisation prévue, de l'utilisation prévisible et, le cas échéant, d'une mauvaise utilisation raisonnablement prévisible de ce dernier.

Dans ce contexte, **s'il est prévu que l'appareil soit interconnecté et interagisse avec d'autres, le fabricant devrait en tenir compte lors de l'évaluation des risques**. L'utilisation ou les mauvaises utilisations peuvent être déterminées sur la base, par exemple, de l'expérience de l'utilisation qui a été faite antérieurement du même type de produit, des enquêtes menées sur les accidents ou du comportement humain.

Par ailleurs, la complexité des systèmes est plus spécifiquement prise en compte dans les actes législatifs sectoriels en matière de sécurité, tels que le règlement sur les dispositifs médicaux, et, dans une certaine mesure, dans la législation relative à la sécurité générale des produits[49]. Par exemple, le fabricant d'un appareil connecté, destiné à entrer dans la composition d'un écosystème de maison intelligente, devrait être en mesure de prévoir raisonnablement que ses produits auront une incidence sur la sécurité d'autres produits.

En outre, la législation applicable aux transports tient compte de cette complexité au niveau des systèmes. Dans les transports routier, ferroviaire et aérien, tant les différents composants que le véhicule automobile, le train ou l'avion dans sa totalité sont soumis aux procédures de

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

[47] Sur la base des exigences essentielles proposées par le groupe d'expert de haut niveau dans les lignes directrices en matière d'éthique pour une IA digne de confiance: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

[48] Règlement (CE) n° 765/2008, décision 2008/768/CE et législation sectorielle harmonisée de l'Union en matière de sécurité des produits, par exemple la directive 2006/42/CE (directive relative aux machines).

[49] L'article 2 de la directive sur la sécurité générale des produits précise qu'un produit sûr tient compte «de l'effet […] sur d'autres produits au cas où on peut raisonnablement prévoir l'utilisation du premier avec les seconds».

réception et de certification. Le contrôle technique automobile, le contrôle de la navigabilité aérienne et l'interopérabilité ferroviaire font partie intégrante de l'évaluation de la sécurité. Dans le domaine des transports, les «systèmes» doivent être «agréés» par une autorité, soit sur la base d'une évaluation, effectuée par une tierce personne, de la conformité avec des normes techniques claires, soit après démonstration de la manière dont les risques sont pris en compte. La solution consiste généralement en une combinaison de mesures prises au niveau du «produit» et du «système».

Les dispositions de la législation de l'Union relative à la sécurité des produits, y compris en matière de transports, qui visent à parer aux risques susceptibles d'avoir une incidence sur la sécurité des utilisateurs tiennent déjà compte, dans une certaine mesure, de la complexité des produits et des systèmes.

Les systèmes complexes intègrent souvent des **logiciels**, qui sont des composants essentiels de tout système basé sur l'IA. De manière générale, dans le cadre de l'évaluation initiale des risques, le fabricant du produit final est tenu de prévoir les risques que présente le logiciel qui y est intégré au moment où le produit est mis sur le marché.

Certains actes de la législation de l'Union relative à la sécurité des produits font explicitement référence aux logiciels intégrés dans le produit. La directive relative aux machines[50], par exemple, exige qu'une défaillance du logiciel du système de commande n'entraîne pas de situation dangereuse.

Dans la législation de l'Union relative à la sécurité des produits, les mises à jour logicielles pourraient être considérées comme des opérations de maintenance pour raisons de sécurité pour autant qu'elles n'entraînent pas de modifications substantielles d'un produit déjà mis sur le marché et qu'elles n'introduisent pas de nouveaux risques qui n'avaient pas été prévus lors de l'évaluation initiale des risques. Toutefois, si la mise à jour logicielle modifie de manière substantielle le produit dans lequel elle est installée, le produit dans son ensemble pourrait être considéré comme un nouveau produit dont la conformité avec la législation applicable en matière de sécurité des produits devra être réévaluée au moment de la modification[51].

Les logiciels autonomes, mis tels quels sur le marché ou installés après que le produit a été mis sur le marché, ne font généralement pas l'objet de dispositions spécifiques dans la législation sectorielle harmonisée de l'Union relative à la sécurité des produits. Néanmoins, certains actes législatifs de l'Union, tels que le règlement sur les dispositifs médicaux, traitent des logiciels autonomes. En outre, les logiciels autonomes installés dans des produits connectés qui communiquent par certains modules radio[52] peuvent également être réglementés, au moyen d'actes délégués, par la directive sur les équipements radioélectriques. Cette directive exige que certaines classes ou catégories d'équipements radioélectriques soient compatibles avec certaines caractéristiques visant à garantir que la conformité de l'équipement en question n'est pas compromise lorsqu'un logiciel est installé[53].

[50] Section 1.2.1 de l'annexe I de la directive relative aux machines.

[51] Le Guide bleu relatif à la mise en œuvre de la réglementation de l'Union européenne sur les produits 2016»,

[52] Les modules radio sont des dispositifs électroniques qui émettent et/ou reçoivent des signaux radio (WIFI, Bluetooth) entre deux dispositifs.

[53] Article 3, paragraphe 3, point i), de la directive sur les équipements radioélectriques.

Si la législation de l'Union relative à la sécurité des produits tient compte des risques en matière de sécurité liés aux logiciels intégrés dans les produits au moment de leur mise sur le marché et à leurs mises à jour potentiellement prévues par le fabricant, des exigences spécifiques et/ou explicites pourraient devoir être fixées pour les logiciels autonomes (par exemple, l'obligation de prévoir une application à installer). Une attention particulière devrait être portée aux logiciels autonomes qui assurent des fonctions de sécurité dans les produits et les systèmes d'IA.

Des obligations supplémentaires devraient peut-être être imposées aux fabricants afin qu'ils prévoient des fonctions destinées à empêcher l'installation de logiciels ayant une incidence sur la sécurité pendant la durée de vie des produits d'IA.

Enfin, les technologies numériques émergentes se caractérisent par des **chaînes de valeur complexes**. Cependant, cette complexité ne constitue pas une nouveauté et n'est pas le seul fait des technologies numériques émergentes telles que l'IA ou l'internet des objets. Elle concerne, par exemple, des produits comme les ordinateurs, les robots de services ou encore les systèmes de transport.

En vertu du cadre de l'Union relatif à la sécurité des produits, peu importe la complexité de la chaîne de valeur: la responsabilité en matière de sécurité des produits incombe toujours au producteur qui met le produit sur le marché. Les producteurs sont responsables de la sécurité du produit final, y compris des éléments qui y sont intégrés, tels que les logiciels d'un ordinateur.

Certains actes de la législation de l'Union relative à la sécurité des produits contiennent déjà des dispositions qui renvoient explicitement à des situations dans lesquelles plusieurs opérateurs économiques interviennent sur un produit donné avant que celui-ci ne soit mis sur le marché. La directive sur les ascenseurs[54], par exemple, exige de l'opérateur économique qui conçoit et fabrique l'ascenseur qu'il fournisse à l'installateur[55] «*toutes les documentations et indications nécessaires pour lui permettre d'assurer l'installation correcte et sûre ainsi que les essais de l'ascenseur*». La directive relative aux machines impose aux fabricants d'équipements de fournir à l'opérateur des informations sur la façon d'assembler ces équipements à une autre machine[56].

La législation de l'Union relative à la sécurité des produits tient compte de la complexité des chaînes de valeur et impose des obligations à plusieurs opérateurs économiques selon le principe de la «responsabilité partagée».

Bien que le principe selon lequel la responsabilité du produit final incombe au producteur se soit avéré suffisant pour les chaînes de valeur complexes actuelles, des dispositions explicites prévoyant spécifiquement une coopération entre les opérateurs économiques au sein de la chaîne d'approvisionnement et les utilisateurs pourraient garantir la sécurité juridique dans des chaînes de valeur peut-être plus complexes encore. Plus particulièrement, les différents acteurs de la chaîne de valeur qui ont une influence sur la sécurité du produit (par exemple, les producteurs de logiciels) et les utilisateurs (qui modifient le produit, par exemple)

[54] Article 16, paragraphe 2, de la directive 2014/33/UE

[55] Dans la directive 2014/33/UE (ascenseurs), l'installateur est l'équivalent du fabricant et il doit assumer la responsabilité de la conception, de la fabrication, de l'installation et de la mise sur le marché de l'ascenseur.

[56] Le point 1.7.4.2 de l'annexe I de la directive relative aux machines est libellé comme suit: *«Chaque notice doit contenir, le cas échéant, au moins les informations suivantes:»* i) *«les instructions de montage, d'installation et de raccordement, y compris les plans, les schémas, les moyens de fixation et la désignation du châssis ou de l'installation sur laquelle la machine doit être montée;»*

assumeraient leur responsabilité et communiqueraient à l'acteur suivant de la chaîne les mesures à prendre et les informations nécessaires.

3. Responsabilité

Au niveau de l'Union, les dispositions en matière de sécurité des produits et de responsabilité du fait des produits sont deux mécanismes complémentaires qui visent le même objectif, à savoir un marché unique des biens qui soit performant et qui garantisse des niveaux élevés de sécurité, c'est-à-dire qui réduise autant que possible le risque de dommages pour les utilisateurs et prévoie une indemnisation en cas de dommages résultant de produits défectueux.

Ces règles de l'Union sont complétées au niveau national par des cadres de responsabilité civile non harmonisés qui prévoient une indemnisation en cas de dommages d'origines diverses (causés par des produits ou des services, par exemple) et permettent d'obtenir réparation auprès de différents responsables (tels que les propriétaires, les exploitants ou les fournisseurs de services).

L'optimisation des règles de sécurité de l'Union en matière d'IA peut certes contribuer à éviter les accidents, mais le risque zéro n'existe pas. C'est là qu'intervient la responsabilité civile. Les règles de responsabilité civile jouent un double rôle dans notre société: d'une part, elles garantissent que les victimes de dommages causés par des tiers obtiennent réparation et, d'autre part, elles prévoient des incitations économiques destinées à encourager les parties responsables à éviter de causer des dommages. Les règles de responsabilité doivent toujours viser un juste équilibre entre la protection des citoyens et la capacité d'innovation des entreprises.

Les cadres de responsabilité de l'Union se sont avérés efficaces. Ils reposent sur l'application parallèle de la directive sur la responsabilité du fait des produits (directive 85/374/CEE), qui a harmonisé les règles de responsabilité du producteur en cas de produits défectueux, et d'autres régimes nationaux de responsabilité non harmonisés.

La directive sur la responsabilité du fait des produits établit un niveau de protection que les régimes nationaux de responsabilité pour faute n'offrent pas à eux seuls. Elle introduit un régime de responsabilité stricte du producteur pour les dommages causés par un défaut de ses produits. En cas de dommage physique ou matériel, la partie lésée a droit à réparation si elle prouve le dommage, le défaut du produit (à savoir que celui-ci n'offrait pas la sécurité à laquelle le public pouvait légitimement s'attendre) et le lien causalité entre le produit défectueux et le dommage.

Les régimes nationaux non harmonisés prévoient des règles de responsabilité pour faute en vertu desquelles les victimes de dommages doivent prouver la faute de la personne responsable, le dommage et le lien de causalité entre la faute et le dommage pour que leur demande de réparation puisse aboutir. Ces régimes prévoient aussi des règles de responsabilité stricte dans les cas où le législateur national a attribué la responsabilité d'un risque à une personne spécifique sans que les victimes aient à prouver la faute/le défaut ou le lien de causalité entre cette faute/ce défaut et le dommage.

Les régimes nationaux de responsabilité permettent aux victimes de dommages causés par des produits et des services d'introduire parallèlement plusieurs demandes en réparation, fondées, soit sur la faute, soit sur la responsabilité stricte. Ces demandes sont souvent dirigées contre différentes personnes responsables et sont assorties de conditions différentes.

Par exemple, une victime d'accident de voiture peut généralement former une action en responsabilité stricte contre le propriétaire de la voiture (c'est-à-dire la personne assurée en responsabilité civile automobile) et une action en responsabilité pour faute contre le conducteur, toutes deux régies par le droit civil national, et elle peut aussi demander réparation au producteur, en vertu de la directive sur la responsabilité du fait des produits, si la voiture présentait un défaut.

En vertu des règles harmonisées en matière d'assurance automobile, l'utilisation du véhicule doit être couverte par une assurance[57] et, dans la pratique, l'assureur est toujours le premier interlocuteur en cas de demande en réparation pour des dommages corporels ou matériels. En vertu de ces règles, l'assurance obligatoire indemnise la victime et protège l'assuré qui, conformément aux règles nationales de droit civil[58], est tenu de verser une compensation financière pour l'accident ayant impliqué le véhicule automobile. La directive sur la responsabilité du fait des produits n'oblige pas les producteurs à prendre une assurance. Pour ce qui est de l'assurance automobile, la législation de l'Union ne fait pas de distinction entre les véhicules selon qu'ils sont autonomes ou non. Les véhicules autonomes, à l'instar de tous les autres, doivent être couverts par une assurance responsabilité civile pour les véhicules à moteur, qui est la voie la plus simple par laquelle la partie lésée peut obtenir réparation.

Bien s'assurer peut contribuer à atténuer les conséquences négatives des accidents en facilitant la procédure d'indemnisation des victimes. Des règles claires en matière de responsabilité aident les compagnies d'assurance à calculer leurs risques et à demander un remboursement à la partie responsable en dernier ressort du dommage. Par exemple, si un accident a été causé par un défaut, l'assureur automobile peut, après avoir indemnisé la victime, demander à être remboursé par le fabricant.

Toutefois, les caractéristiques des technologies numériques émergentes telles que l'IA, l'internet des objets et la robotique, remettent en question certains aspects des cadres de responsabilité de l'Union et nationaux et pourraient en réduire l'efficacité. Certaines de ces caractéristiques pourraient rendre difficiles la traçabilité du dommage et son imputabilité à un comportement humain susceptible de constituer le fondement d'une procédure en responsabilité pour faute en vertu des règles nationales. Cela signifie qu'il pourrait s'avérer difficile ou excessivement coûteux d'établir le bien-fondé des procédures en responsabilité sur la base des droits nationaux relatifs à la responsabilité civile et que les victimes pourraient par conséquent ne pas être correctement indemnisées. Il importe que les victimes d'accidents causés par des produits et des services intégrant des technologies numériques émergentes telles que l'IA bénéficient du même niveau de protection que les victimes d'accidents causés par d'autres produits et services similaires, pour lesquels elles obtiendraient réparation au titre du droit national relatif à la responsabilité civile. Si tel n'était pas le cas, ces technologies émergentes pourraient être moins bien acceptées par la société et les citoyens pourraient se montrer réticents à les utiliser.

Il faudra déterminer si les questions que les nouvelles technologies soulèvent à l'égard des cadres existants pourraient aussi générer une insécurité juridique quant à la façon dont les législations existantes s'appliqueraient (par exemple, la façon dont la notion de faute s'appliquerait aux dommages causés par l'IA). Ces questions pourraient également avoir pour

[57] Harmonisée pour les véhicules à moteur par la directive 2009/103/CE concernant l'assurance de la responsabilité civile résultant de la circulation de véhicules automoteurs et le contrôle de l'obligation d'assurer cette responsabilité.

[58] Dans la plupart des États membres, la responsabilité stricte est appliquée à la personne au nom de laquelle le véhicule est immatriculé.

effets de décourager les investissements et d'entraîner une augmentation des coûts d'information et d'assurance pour les producteurs et d'autres entreprises de la chaîne d'approvisionnement, en particulier pour les PME européennes. En outre, si, à terme, les États membres venaient à résoudre les problèmes qui se posent pour leurs cadres nationaux de responsabilité, il pourrait en résulter une nouvelle fragmentation qui se traduirait par une hausse des coûts liés à la mise sur le marché de solutions d'IA innovantes et par un ralentissement des échanges transfrontières au sein du marché unique. Il importe que les entreprises aient conscience des risques liés à leur responsabilité tout au long de la chaîne de valeur et qu'elles puissent réduire ou prévenir ces risques et s'assurer efficacement contre eux.

Le présent chapitre explique la façon dont les nouvelles technologies remettent les cadres existants en question et comment il serait possible d'y remédier. De plus, les spécificités de certains secteurs, tel que le secteur des soins de santé, pourraient mériter un examen plus approfondi.

Complexité des produits, des services et de la chaîne de valeur: la technologie et l'industrie ont évolué de manière spectaculaire au cours des dernières décennies. Plus particulièrement, la démarcation entre produits et services n'est plus aussi nette que par le passé. Les produits et la fourniture de services sont de plus en plus inextricablement liés. Bien que les produits et les chaînes de valeur complexes ne constituent pas une nouveauté pour l'industrie européenne ou son modèle réglementaire, les logiciels ainsi que l'IA méritent une attention spécifique pour ce qui est de la responsabilité du fait des produits. Les logiciels sont essentiels au fonctionnement d'un grand nombre de produits et peuvent avoir une incidence sur leur sécurité. Ils sont intégrés dans les produits, mais ils peuvent aussi être fournis séparément pour permettre d'utiliser le produit aux fins prévues. Ni un ordinateur ni un téléphone intelligent ne seraient d'une quelconque utilité sans logiciels. Il en découle que les logiciels peuvent être à l'origine de la défectuosité d'un produit concret et entraîner des dommages physiques (voir l'encadré consacré aux logiciels dans la partie sur la sécurité). Ces dommages pourraient in fine engager la responsabilité du fabricant du produit au titre de la directive sur la responsabilité du fait des produits.

Toutefois, les logiciels se présentant sous différents types et formes, il peut ne pas toujours être évident de les classer dans les services ou les produits. Ainsi, si un logiciel qui commande le fonctionnement d'un produit concret pourrait être considéré comme une partie ou un composant de ce produit, certaines formes de logiciels autonomes pourraient s'avérer plus difficiles à classer.

Bien que la directive sur la responsabilité du fait des produits donne une définition large de la notion de produit, celle-ci pourrait être précisée pour mieux traduire la complexité des technologies émergentes et faire en sorte qu'il existe toujours une possibilité de réparation en cas de dommages causés par des produits rendus défectueux par un logiciel ou d'autres fonctionnalités numériques. Une telle évolution permettrait aux acteurs économiques tels que les concepteurs de logiciels de mieux évaluer s'ils pourraient être considérés comme des producteurs au sens de la directive sur la responsabilité du fait des produits.

Des applications d'IA sont souvent intégrées dans des **environnements complexes de l'internet des objets**, dans lesquels différents dispositifs et services connectés interagissent. Du fait de la combinaison de différents composants numériques dans un écosystème complexe et de la pluralité des acteurs concernés, il peut être difficile de déterminer l'origine d'un dommage potentiel et de remonter à la personne qui en est responsable. De par la complexité de ces technologies, il peut être très difficile pour les victimes d'identifier la

personne responsable et de prouver, ainsi que l'exige le droit national, que toutes les conditions requises pour pouvoir obtenir réparation sont réunies. Le coût d'une telle expertise peut s'avérer prohibitif sur le plan économique et dissuader les victimes de demander réparation.

En outre, les produits et les services faisant appel à l'IA interagiront avec les technologies traditionnelles, ce qui compliquera encore la détermination des responsabilités. Par exemple, les voitures autonomes cohabiteront pendant un certain temps avec les véhicules traditionnels. Des interactions d'une complexité similaire entre plusieurs acteurs seront observées dans certains secteurs des services (tels que la gestion du trafic et les soins de santé) dans lesquels des systèmes d'IA partiellement automatisés viendront soutenir la prise de décision humaine.

Selon le rapport[59] du sous-groupe «Nouvelles technologies» du groupe d'experts «Responsabilité et nouvelles technologies», il pourrait être envisagé d'adapter les législations nationales de manière à faciliter la charge de la preuve pour les victimes de dommages liés à l'IA. La charge de la preuve pourrait, par exemple, être liée au respect (par l'opérateur concerné) d'obligations juridiques spécifiques portant sur la cybersécurité ou d'autres aspects de la sécurité: si l'opérateur concerné ne respecte pas ces obligations, un renversement de la charge de la preuve concernant la faute et le lien de causalité pourrait s'appliquer.

La Commission souhaite recueillir des avis afin de déterminer si et dans quelle mesure il pourrait s'avérer nécessaire que l'UE adopte une initiative visant à atténuer les conséquences de la complexité en allégeant/inversant la charge de la preuve exigée par les règles nationales de responsabilité pour les dommages causés par les applications d'IA.

En ce qui concerne la législation de l'Union, selon la directive sur la responsabilité du fait des produits, un produit qui ne satisfait pas aux règles de sécurité obligatoires serait considéré comme défectueux qu'il y ait faute ou non du fabricant. Cependant, certaines raisons pourraient aussi justifier d'envisager les moyens de faciliter la charge de la preuve pour les victimes dans le cadre de la directive, laquelle s'appuie sur les règles nationales en matière de preuve et d'établissement du lien de causalité.

Connectivité et ouverture: il est actuellement difficile de savoir avec exactitude quelles pourraient être les attentes en matière de sécurité en ce qui concerne les dommages résultant d'atteintes à la cybersécurité au niveau des produits et de déterminer si la directive sur la responsabilité du fait des produits permettrait de réparer ces dommages comme il se doit.

Un produit peut présenter des faiblesses en matière de cybersécurité dès le départ, au moment de sa mise en circulation, mais ces faiblesses peuvent aussi apparaître à un stade ultérieur, bien après cette mise en circulation.

Dans les cadres de responsabilité pour faute, établir des obligations claires en matière de cybersécurité permet aux opérateurs de déterminer ce qu'ils doivent faire pour éviter les conséquences de leur responsabilité.

Dans le cadre de la directive sur la responsabilité du fait des produits, la question de savoir si un producteur aurait pu prévoir certains changements compte tenu de l'utilisation raisonnablement prévisible du produit pourrait occuper une place plus importante. Par

[59] Rapport sur la responsabilité en matière d'intelligence artificielle et d'autres technologies numériques émergentes (*Liability for Artificial Intelligence and other emerging technologies*), disponible en anglais uniquement, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

exemple, on pourrait observer un recours accru au moyen de défense fondé sur le défaut ultérieur («later defect defence»), selon lequel un producteur n'est pas responsable si le défaut n'existait pas au moment où le produit a été mis en circulation, ou au moyen de défense fondé sur le risque de développement («development risk defence»), selon lequel l'état des connaissances à l'époque de la mise en circulation ne permettait pas de prévoir le défaut). En outre, la responsabilité pourrait être réduite si la partie lésée n'effectue pas les mises à jour ayant une incidence sur la sécurité. Le fait de ne pas effectuer ces mises à jour pourrait potentiellement être considéré comme une négligence concurrente de la part de la personne lésée et donc réduire la responsabilité du producteur. Dans la mesure où la notion d'utilisation raisonnablement prévisible et les questions liées à la négligence concurrente, comme le fait de ne pas procéder à une mise à jour de sécurité, pourraient être plus fréquemment invoquées, les personnes lésées pourraient avoir plus de mal à obtenir réparation pour des dommages causés par un défaut du produit.

Autonomie et opacité: lorsque les applications d'IA sont capables d'agir de manière autonome, elles exécutent des tâches sans que chaque étape ne soit prédéfinie et avec moins voire pas du tout de supervision ni de contrôle humain immédiat. Les algorithmes fondés sur l'apprentissage automatique peuvent être difficiles voire impossibles à comprendre (effet «boîte noire»).

Outre la complexité évoquée plus haut, il pourrait, en raison de cet effet «boîte noire», devenir difficile d'obtenir réparation pour des dommages causés par des applications d'IA autonomes. La compréhension nécessaire de l'algorithme et des données utilisées par l'IA requiert des capacités d'analyse et des compétences techniques dont le coût pourrait être jugé prohibitif par les victimes. En outre, il pourrait s'avérer impossible d'accéder à l'algorithme et aux données sans la coopération de la partie potentiellement responsable. Dans la pratique, les victimes pourraient donc ne pas être en mesure de demander réparation. De plus, il serait difficile de savoir comment démontrer la faute d'une IA agissant de manière autonome, ou ce qui serait considéré comme la faute d'une personne recourant à l'IA.

Un certain nombre de solutions ont déjà été introduites en droit national pour réduire la charge de la preuve pour les victimes dans de telles situations.

L'un des principes directeurs de la sécurité des produits et de la responsabilité du fait des produits dans l'Union reste qu'il appartient aux producteurs de garantir la sécurité de tous les produits mis sur le marché pendant toute leur durée de vie et dans le cadre d'une utilisation raisonnablement prévisible. Ce principe signifie que les fabricants doivent veiller à ce que les produits ayant recours à l'IA respectent certains paramètres de sécurité. Les propriétés de l'IA ne s'opposent pas à l'existence d'un droit à des attentes en matière de sécurité des produits, que ces derniers soient des tondeuses à gazon automatiques ou des robots chirurgicaux.

L'autonomie peut avoir une incidence sur la sécurité du produit, car elle peut modifier profondément les caractéristiques de celui-ci, notamment ses dispositifs de sécurité. La question est de savoir dans quelles conditions les propriétés d'autoapprentissage prolongent la responsabilité du producteur et dans quelle mesure ce dernier devrait avoir prévu certains changements.

La notion de «mise en circulation» actuellement utilisée dans la directive sur la responsabilité du fait des produits pourrait être revue, en étroite coordination avec les changements correspondants apportés au cadre de sécurité de l'Union, afin de tenir compte des risques d'évolution et de modification des produits. Pareille révision pourrait également aider à préciser qui est responsable de tout changement apporté au produit.

Selon le rapport[60] du sous-groupe «Nouvelles technologies» du groupe d'experts «Responsabilité et nouvelles technologies», l'utilisation de certains services et dispositifs d'IA autonomes pourraient présenter un risque spécifique en termes de responsabilité, car ces services et dispositifs peuvent nuire gravement à des intérêts importants, juridiquement protégés, tels que la vie, la santé et la propriété, et exposer le grand public à des risques. Cela pourrait concerner principalement les dispositifs d'IA qui se déplacent dans les espaces publics (par exemple, des véhicules entièrement autonomes, des drones[61] et des robots livreurs de colis) ou les services basés sur l'IA présentant des risques similaires (par exemple, les services de gestion du trafic qui guident ou contrôlent les véhicules ou les services de gestion de la distribution d'électricité). Il pourrait être remédié aux problèmes que posent l'autonomie et l'opacité pour les droits nationaux en matière de responsabilité civile en adoptant une approche fondée sur les risques. Des régimes de responsabilité stricte pourraient garantir l'indemnisation de la victime, indépendamment de toute faute, chaque fois qu'il y a matérialisation du risque. L'incidence que le choix de la personne devant être considérée comme strictement responsable pourrait avoir sur le développement et l'adoption de l'IA devrait être soigneusement évaluée et une approche fondée sur les risques devrait être envisagée.

En ce qui concerne les applications d'IA présentant un profil de risque spécifique, la Commission cherche à obtenir des avis afin de déterminer si et dans quelle mesure l'application de la responsabilité stricte, telle qu'elle existe en droit national pour des risques similaires auxquels le public est exposé (par exemple, l'exploitation des véhicules à moteur, des aéronefs ou des centrales nucléaires, par exemple) pourrait s'avérer nécessaire pour garantir une indemnisation effective des victimes potentielles. La Commission cherche aussi à obtenir des avis sur la possibilité de coupler la responsabilité stricte à une éventuelle obligation de contracter une assurance disponible, à l'instar de ce que prévoit la directive sur l'assurance automobile, afin de garantir l'indemnisation indépendamment de la solvabilité de la personne responsable et de contribuer à réduire les coûts d'indemnisation.

Pour toutes les autres applications d'IA, soit la grande majorité, la Commission examine s'il y a lieu d'adapter la charge de la preuve concernant le lien de causalité et la faute. À cet égard, l'un des problèmes épinglés dans le rapport[62] du sous-groupe «Nouvelles technologies» du groupe d'experts «Responsabilité et nouvelles technologies» renvoie à la situation dans laquelle la partie potentiellement responsable n'a pas collecté les données nécessaires à l'évaluation de la responsabilité ou n'est pas disposée à les communiquer à la victime.

[60] Rapport sur la responsabilité en matière d'intelligence artificielle et d'autres technologies numériques émergentes (*Liability for Artificial Intelligence and other emerging technologies*), disponible en anglais uniquement, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[61] Voir les systèmes d'aéronefs sans équipage à bord visés dans le règlement d'exécution (UE) 2019/947 de la Commission du 24 mai 2019 concernant les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord.

[62] Rapport sur la responsabilité en matière d'intelligence artificielle et d'autres technologies numériques émergentes (*Liability for Artificial Intelligence and other emerging technologies*), disponible en anglais uniquement, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

4. Conclusion

L'émergence de nouvelles technologies numériques telles que l'IA, l'internet des objets et la robotique soulève, en matière de sécurité des produits et de responsabilité du fait des produits, de nouvelles questions qui ont trait à la connectivité, à l'autonomie, à la dépendance aux données, à l'opacité, à la complexité des produits et des systèmes, aux mises à jour logicielles, à la gestion, plus complexe, de la sécurité et aux chaînes de valeur.

La législation actuelle relative à la sécurité des produits présente un certain nombre de lacunes qu'il convient de combler. C'est le cas, tout particulièrement, de la directive sur la sécurité générale des produits, de la directive relative aux machines, de la directive sur les équipements radioélectriques et du nouveau cadre législatif. Les futurs travaux visant à adapter différents actes législatifs dans ce cadre seront effectués dans un souci de cohérence et d'harmonisation.

Les nouvelles questions qui se posent en matière de sécurité en soulèvent également de nouvelles en matière de responsabilité. Ces questions de responsabilité doivent être traitées de manière à garantir un niveau de protection égal à celui dont bénéficient les victimes de dommages causés par les technologies traditionnelles tout en maintenant l'équilibre avec le besoin d'innovation technologique. Régler ces questions permettra d'instaurer la confiance dans ces technologies numériques émergentes et apportera de la stabilité aux investissements.

Bien qu'en principe, la législation existante au niveau de l'Union et des États membres permette d'appréhender les technologies émergentes, l'importance et l'effet conjugué des problèmes posés par l'IA pourraient compliquer l'indemnisation des victimes dans tous les cas où elle se justifierait[63]. Ainsi, la répartition des coûts en cas de dommage pourrait s'avérer inéquitable ou inefficiente dans le cadre des règles actuelles. Pour y remédier et éliminer les incertitudes potentielles du cadre existant, il pourrait être envisagé d'apporter, au moyen d'initiatives de l'UE, certains ajustements à la directive sur la responsabilité du fait des produits et aux régimes nationaux de responsabilité, sur la base d'une approche ciblée et fondée sur les risques, c'est-à-dire une approche qui tienne compte des différences de risques que présentent les différentes applications d'IA.

[63] Voir le rapport de la formation «Nouvelles technologies», p. 3 et la recommandation 27.2 du groupe d'experts de haut niveau sur l'intelligence artificielle.