



REVUE

de la gendarmerie nationale

REVUE TRIMESTRIELLE / SUPPLEMENT THEMATIQUE / GRATUIT

Le Supplément

Le droit des robots



>> AVERTISSEMENT

La Direction Générale de la Gendarmerie Nationale n'entend donner aucune approbation ou improbation aux opinions émises par les auteurs. Ces opinions doivent être considérées comme propres à leur auteur.

>> COUVERTURE

– M. David Chrétien (CPMGN)

Dans son *Traité*¹ consacré au droit et à l'éthique de la robotique civile, Nathalie NEVEJANS conclue son ouvrage en empruntant une citation du Philosophe Peter Kempf : « *L'éthique de la technologie n'est pas une déclaration de guerre à toute technologie. Au contraire. Elle doit être, de part en part, un plaidoyer pour la bonne technologie, elle doit garantir un développement respectueux de l'Autre, en fixant des limites qui à la fois nous promettent une vie plus riche et nous interdisent de ruiner notre existence commune* ».

Cette réflexion de ce philosophe serait susceptible de constituer une des trames qui pourrait inspirer les régulateurs nationaux et supranationaux en charge de réfléchir sur l'orientation souhaitable ou pas à donner au droit positif et aux normes qui en découleraient. Sur le continent européen, il convient de souligner l'adoption le 16 février 2017, par le Parlement européen, de la première Résolution² consacrée aux règles de droit civil sur la robotique. Elle invite la Commission, entre-autre, « d'examiner, d'évaluer et de prendre en compte les conséquences de toutes les solutions juridiques envisageables, telles que : ³ la création, à terme, d'une personnalité juridique spécifique aux robots.... ». Ce point constitue une des pierres d'achoppement qui fait débat dans l'ensemble des disciplines s'intéressant aux questions de la robotique, cristallisant les débats. Le régulateur français s'est saisi de ces enjeux en saisissant l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST). Cet organisme a rendu public au mois de mai 2017 son rapport intitulé : « Pour une intelligence artificielle maîtrisée, utile et démythifiée⁴. »

Ce cahier spécial, trouve son origine dans le colloque intitulé « Quelle place pour les robots dans notre société ? - Enjeux technologiques, défis éthiques et juridiques » co-organisé le 12 décembre 2016 par l'Association du droit des robots (ADDR⁵) et le Centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN). À cette occasion, une équipe de France Culture a montré son intérêt en enregistrant certaines interventions dans le cadre de la réalisation d'une série de quatre documentaires audio portant sur les robots⁶. La richesse des échanges de ce colloque a incité les organisateurs à poursuivre ces

(1) Nathalie NEVEJANS, *Traité de droit et d'éthique de la robotique civile*, LEH Édition, Bordeaux, 2017, 1230 p.

(2) Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//FR

(3) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//FR

(4) Tome 1 – Rapport : www.senat.fr/rap/r16-464-1/r16-464-11.pdf – Rapporteurs : Dominique GILLOT, Sénatrice, ancienne Ministre, et Claude de GANAY, Député.

(5) www.association-droit-robot.fr

(6) www.franceculture.fr/emissions/lsd-la-serie-documentaire/mon-jumeau-le-robot-44-un-robot-qui-me-veut-du-bien

travaux prospectifs à Lille dans le cadre du Forum international de cybersécurité (FIC). Lors de cette manifestation, un agora consacré au « droit des robots » a permis de poursuivre ces travaux avec un large public issu de la société civile. Ce numéro constitue un recueil des réflexions provenant d'intervenants de ces deux événements. Ce cahier spécial se présente en trois parties. La première partie regroupe l'état des réflexions autour des questions d'éthique sociétale. En l'absence d'un droit *sui generis* à la robotique, nous laisserons s'exprimer dans une deuxième partie des praticiens du droit. Leurs opinions apportent un éclairage sur les aspects relatifs à la responsabilité ainsi qu'aux libertés fondamentales. Enfin, la dernière partie de ce cahier met en relief quelques retours d'expérience de contact de l'homme avec les robots mais aussi des risques en l'absence de régulation. L'actualité dans le domaine de la robotique et de l'intelligence artificielle ne connaîtra pas de pause dans les mois à venir. Les quatrièmes États Généraux de la Robotique en France, qui se sont déroulés du mardi 16 au jeudi 18 mai 2017 à Aubervilliers au Docks de Paris, ont montré que les entreprises hexagonales disposent sur ce secteur d'une avance technologique certaine.

Jérôme LAGASSE
Rédacteur en Chef

ÉTHIQUE ET SOCIÉTÉ

Les robots	7
par Jean Donio	
Pour un dialogue sans ambiguïté entre l'homme et la machine	13
par Serge Tisseron	
L'homo cyberneticus	21
par Marc Watin-Augouard	
Quis custodiet ipsos custodes - Qui gardera les gardiens ?	33
par Ludovic Petit	
Hawking ou Montesquieu - À qui se fier pour encadrer les systèmes d'armes létaux autonomes ?	37
par Didier Danet	

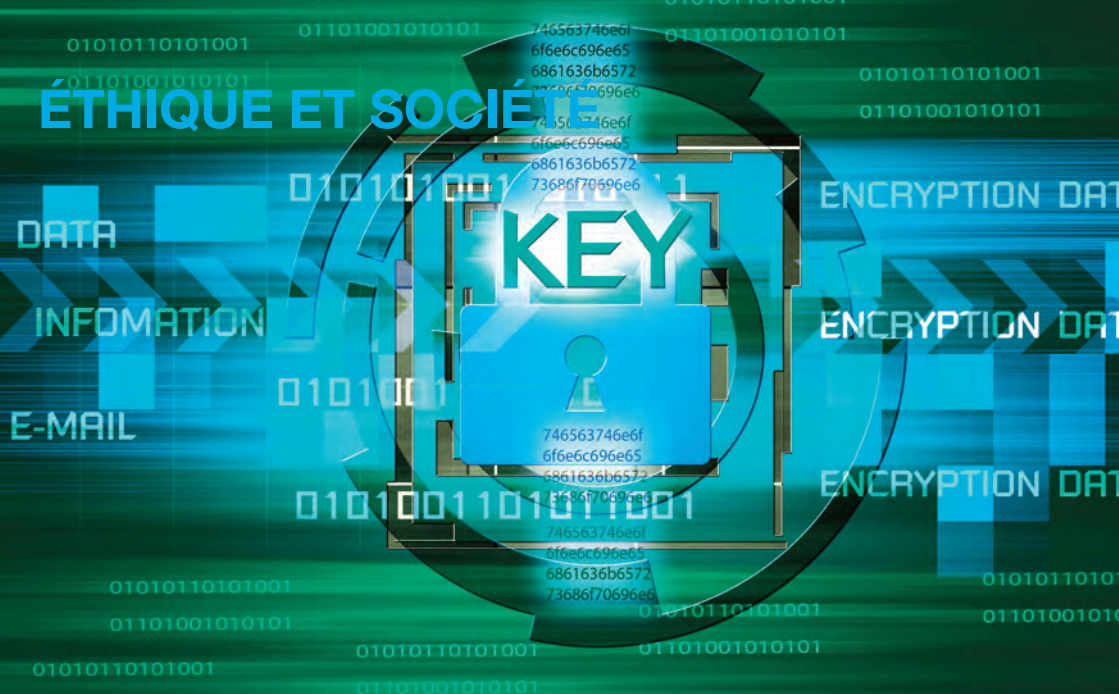
DOCTRINE JURIDIQUE

Robot or not robot ? petite digression juridico-philosophique	45
par Olivier de Maison Rouge	
Quelle responsabilité pour les robots ?	
Quelle responsabilité pour l'Homme ?	49
par Fabrice Lorvo	
Voiture autonome : quel droit pour les forces de l'ordre ?	53
par Didier Gazagne	
Application de l'intelligence artificielle (IA) à la robotique : un cadre juridique et éthique est nécessaire	75
par Didier Gazagne	
Contrôle routier des voitures connectées : quel nouveau paradigme dans les règles d'engagement coercitives des forces de sécurité publique ?	89
par Jérôme Lagasse	
Règles européennes de droit civil en robotique	105
par Nathalie Nevejans	

SCIENCES APPLIQUÉES

Robots autonomes, société et sécurité publique	123
par Thierry Daups	
Robot sociaux « empathiques » en santé : quels bénéfices ?	
Quelles inquiétudes ?	133
par Anne-Sophie Rigaud et Grégory Legouverneur	
Quelle autonomie décisionnelle pour les systèmes robotiques militaires du futur ?	139
par Gérard De Boisboissel	
Intelligence artificielle et conflictualité - Sur l'hypothèse de dérive malveillante d'une Intelligence Artificielle	149
par Thierry Berthier et Olivier Kempf	

ÉTHIQUE ET SOCIÉTÉ



Dans cette partie, les différents auteurs nous interpellent sur des questions éthiques qui nous obligent chacun(e) à amorcer un long travail d'introspection philosophique sur la place qu'il conviendra d'accorder aux robots dans notre société. La cohabitation des humains avec des machines douées d'une « empathie artificielle » pourrait, selon les orientations données, bouleverser la conception que nous avons d'autrui. Des scientifiques de renom comme le physicien Stephen Hawking n'hésitent pas à lancer un appel à la vigilance collective : « *nous devons absolument nous assurer que les objectifs des ordinateurs sont les mêmes que les nôtres* ». La robotique soulève aussi une réflexion à travers le débat portant sur l'humain augmenté. Là aussi, la réflexion éthique demeure fondamentale pour s'assurer de prévenir en premier lieu toute fracture entre homme amélioré et pas, mais surtout toute dérive vers le transhumanisme. La sphère défense et sécurité ne peut non plus faire l'économie de ce débat éthique sur la place qu'il conviendra d'accorder à la robotique sur un théâtre d'opération.

Les robots

par JEAN DONIO

L

La dimension robotique est de plus en plus présente dans la société civile ou militaire. Beaucoup de citoyens frustrés se révoltent, parce qu'ils sont privés d'informations pertinentes, et n'ont pas leur mot à dire, mais sans que cela n'ait d'effet. Les consommateurs ne font que subir une technologie qui les dépasse. C'est là peut-être qu'interviennent les sciences juridiques, pour créer un nouvel ordre. On peut penser au droit des robots,



JEAN DONIO

Ancien élève de l'École Polytechnique
Professeur Émérite à l'Université de Paris II
Ph.D. - Docteur à Sciences-M.A.E.
Expert Judiciaire honoraire près la Cour de Cassation de Paris
Auditeur du Centre des Hautes Études de l'Armement
jean.donio@yahoo.fr

mais a-t-on pensé au droit de survie de l'espèce humaine? Et surtout, en a-t-on encore le temps? Les espèces se succèdent sur terre, puis disparaissent. Alors, quelles sont aujourd'hui les chances de survie de l'espèce humaine par rapport aux robots ?

C'est par l'application des automates et des automatismes à la mécanique, l'électronique et surtout par l'informatique, que la robotique est devenue une discipline scientifique. Les premiers robots étaient destinés à nettoyer les cuves nucléaires, puis les automatismes se sont emparés des voitures, on a construit l'électronique des voitures et aujourd'hui ce sont les robots à face humaine que l'on voit apparaître un peu partout, ces robots ayant un rôle social d'aide et de remplacement des êtres humains.

Le numéro 255 du 1^{er} trimestre 2016 de la Gendarmerie Nationale présente dans son avant-propos une pensée très forte d'Albert Einstein qui écrit que : « *L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique* ». Cette pensée prend toute sa valeur quand on réalise que son auteur a été l'un des piliers du projet Manhattan à l'Université de Chicago. Ce projet a mis fin à la



La sécurité est au cœur de toute avancée technologique.

seconde guerre mondiale par la bombe atomique. La très grande sagesse de cette préoccupation et de récents événements, font de cette pensée une idée d'avant-garde, prédictive de ce qui risque d'arriver si on laisse la technologie sans contrôle.

Tout le monde a conscience que l'homme s'est toujours servi de son intelligence pour agir sur son milieu, et qu'il en est arrivé à dominer sur cette terre les autres espèces, qu'elles soient animales, végétales ou minérales. Ceci est resté vrai jusqu'au jour où l'homme a décidé de créer un être supérieur, qu'il a fait à son image, en utilisant les technologies de l'informatique.

De l'informatique à la robotique

Les technologies numériques ont donné lieu à l'informatique, créée en 1946 à l'Université de Harvard après la seconde

guerre mondiale. Elles peuvent dès à présent améliorer la vie de l'être humain, et sa sécurité, si elles sont bien utilisées. Mais elles peuvent aussi contribuer de manière néfaste à notre décadence, ou même à notre disparition totale, sans que la plupart d'entre nous aient leur mot à dire de ces éventualités. En vérité, on ne sait pas bien si les technologies seront utilisées pour le bien ou contre les hommes.

En ce qui concerne la technologie elle-même, celle-ci est ancrée dans la vie de l'espèce humaine. Étant optimiste, j'ai commencé par penser que la technologie sous forme de robots servirait l'homme, et l'émanciperait: mais aujourd'hui, je n'en suis plus si sûr.

La machine travaillant à la place de l'homme, celui-ci aurait eu tout le temps

nécessaire pour s'épanouir intellectuellement et artistiquement. Mais les aspects positifs et négatifs des technologies sont omniprésents dans la société (armée, économie, vie privée et loisirs), et personne ne peut dire à l'avance si l'homme va se servir des machines et devenir le maître des robots, ou si c'est l'homme qui sera asservi par les robots.

Tout semble évoluer, non pas vers l'homme, maître des robots, comme je pouvais le penser au départ, mais plutôt vers la super intelligence du robot, qui peut très bien devenir le maître d'un homme inutile et asservi par les robots. Il n'est certes pas trop tard pour supprimer les risques qui nous guettent, mais encore faut-il le vouloir. Or, nous vivons dans un tourbillon où la technologie évolue librement.

Le président des USA (depuis 1945, Harry Truman), s'est rendu compte qu'il n'y avait pas assez de scientifiques aux États-Unis pour mener à bien les calculs des bombes

A et H¹. C'est ainsi qu'il a chargé, par contrat, en 1946, l'Université d'Harvard de faire le premier calculateur au monde, ENIAC 1 (un monstre de plusieurs

(1) La bombe H est appelée à succéder à la bombe A, elle est plus sophistiquée que la bombe « A », déjà utilisée par le Président Roosevelt contre le Japon, et plus puissante (la bombe H utilise comme « allumette » la bombe A), et elle a besoin de plusieurs millions de degrés pour devenir opérationnelle.

mètres), construit sur une architecture toujours à la base des technologies numériques. Cette architecture comprend :

- une Mémoire Centrale qui permet à l'ordinateur de fonctionner et aux mémoires extérieures (disques, bandes,

ruban papier, cartes, *etc.*) qui enregistrent des quantités d'informations de s'en souvenir des années après ;

- une Unité Centrale : appelée à l'origine l'UAL (Unité Arithmétique et Logique), couplée avec la mémoire centrale, et ne travaillant qu'avec elle constitue l'intelligence du calculateur. Elle peut varier le nombre d'opérations permises.

Initialement, seules les fonctions arithmétiques et logiques étaient permises, mais aujourd'hui, la plupart des fonctions de l'intelligence humaine et d'autres encore sont devenues possibles. La société IBM a appelé ces calculateurs des "ordinateurs", car ils pouvaient donner des ordres à la machine ;

- des "Entrées-Sorties" : les capteurs donnent aux machines une supériorité des sens multiples, dont la plupart absents chez l'homme. Il est possible de concevoir des robots, avec une acuité des sens beaucoup plus développée que la nôtre, car les robots peuvent détecter les radiations, l'électromagnétisme, les émanations chimiques, *etc.*, en fait bien plus que les sens humains ne le permettent ;

- une « Communication » : l'interopérabilité permet à plusieurs machines de communiquer entre elles (imprimantes, écrans, claviers, souris, auparavant télétypes, *etc.*) et de travailler sur une même tâche, ce que les robots savent faire. Par contre, il est encore nécessaire que les humains communiquent avec des machines pour leur donner des ordres, sans utiliser leur langage.

Les quatre fonctions principales énumérées ci-dessus sont celles issues de l'être humain et l'ensemble de ces fonctions constitue l'informatique théorique (l'ensemble constitue le *hardware* et le *software*). Il y a par ailleurs la technologie des machines qui a pour but de miniaturiser les composants, et d'optimiser le tout.

La mémoire permet de se souvenir, l'intelligence permet de raisonner et de réagir, les sens et les moyens d'expression permettent d'appréhender l'environnement pour pouvoir l'analyser et d'en tirer les conclusions y afférant, et la communication permet de dialoguer. L'ensemble de ces quatre fonctions a donné à l'homme sa supériorité sur les autres espèces, celles du règne animal, du règne végétal, et du règne minéral. Quant à la technologie, elle ne fait aujourd'hui que développer et/ou améliorer les moyens mis à la disposition de l'homme par l'informatique théorique.

L'ENIAC 1 a été suivi de peu à Princeton dès 1947. Puis, la société IBM s'est installée à l'université de Columbia, où elle a créé un centre de recherches. Plus tard, l'Université de Stanford a créé le protocole TCP/IP, qui a permis pour la première fois aux instituts de recherche de résoudre leurs problèmes en se connectant successivement sur les calculateurs des universités des côtes Est et Ouest des Etats-Unis, malgré une différence de 3 heures entre les deux.

En 1994, Internet est né du physicien anglais Berners-Lee au CERN de

Genève, et grâce au protocole TCP/IP. La communication des calculateurs entre eux est devenue facilement réalisable. Les centres de recherche de différents pays, ont pris la suite: Mir en Russie, Bull en France, ICL en grande Bretagne, Olivetti en Italie, Nixdorf et Siemens en Allemagne, etc. ont tous suivi Harvard, en gardant l'architecture des ordinateurs d'origine. Aujourd'hui, internet et TCP /IP servent à tous, malgré les intrusions, le vandalisme, l'espionnage et le vol des données par les gouvernements et par les mafias, vol qui ne semble déranger personne, alors que tous sont au courant. C'est par le développement de ces technologies qu'on est arrivé à la robotique très présente dans notre société.

Société robotisée et sécurité

Initialement, il s'agit des automatismes, de la mécanique, de l'électronique, puis de l'application de l'informatique à la robotique. On pouvait alors imaginer un avenir où l'homme libéré des tâches dégradantes deviendrait le maître des machines ou celui d'une nouvelle forme d'esclavage de la machine.

Dans un futur proche, l'activité humaine sera réduite d'environ 40 %, selon mes calculs, pour une activité robotique qui demeure 24 heures sur 24, 7 jours sur 7, ce qui multiplie par un facteur 9 par semaine environ ce que les robots vont réaliser à la place des hommes. En outre, les robots travaillent plus vite que l'homme, sans salaire, avec peu de courant électrique (ce qui peut être fourni par des piles photovoltaïques, et donc devenir

énergétiquement autonome) : ceci n'a pas échappé aux grandes entreprises qui contrôlent maintenant les robots.

En janvier 2014, j'avais prévu une nouvelle taxe dite d'humanisation des entreprises, qui prendrait la place de toutes les autres taxes et impôts, sauf celle de la TVA. En effet, à partir du moment où ce sont les robots, et non plus les êtres humains, qui créent la richesse que nous partageons tous, il faudra penser au partage de cette richesse, et à des places à définir dans le nouvel ordre économique qui se crée.

En effet, la robotique opérationnelle couvre les domaines de l'activité humaine (qui va des soins aux personnes âgées, aux armées) : cela peut être positif, mais non sans danger. Pour ce qui concerne l'armée (terre, mer et air en général, et les *US Marine Corps* en plus aux États-Unis), les robots sont utiles, et de plus en plus utilisés. Des engins fixes ou mobiles sont là pour nous protéger ; mais est-ce la vérité ?

À la pointe de la technologie, la robotique participe à l'effort de la Recherche et Développement industriel des pays (l'exemple des USA, après la Seconde guerre mondiale, est très parlant car l'informatique y est née d'abord pour des besoins de guerre). Par ailleurs, en remplaçant les soldats, le pays qui utilise des robots dans les conflits de guerre n'aura pas en principe à pleurer la mort, la blessure, ou la prise d'otage de ses soldats. Qui plus est, contrairement aux soldats, les robots n'ont pas besoin de formation (sauf pour les mises à jour des

programmes), car ils ne partagent pas les exigences de la vie humaine. Il est inutile en conséquence de mettre en place une logistique lourde pour utiliser ces moyens : logement, nourriture, habillement, soins médicaux, transports, invalidités, retraites, etc., tout cela est financièrement intéressant. C'est pourquoi on trouve aujourd'hui dans l'armée des robots fixes ou mobiles, des drones qui peuvent faire de la surveillance, et lancer des missiles, des robots terrestres mobiles qui peuvent combattre le terrorisme, cette lutte étant de nos jours la guerre la plus difficile.

Pourtant, il ne faut pas oublier que des ingénieurs très qualifiés comptent parmi les terroristes et les états belliqueux, qui disposent d'importants financements pour développer leurs propres robots, dotés d'algorithmes d'apprentissage inhumains et destructeurs.

Les robots destinés à contrer le terrorisme ne sont efficaces que s'ils ont un pouvoir dissuasif, s'ils sont autonomes, et peuvent prendre des décisions : mais alors, quels sont les êtres humains qui auront la responsabilité de ces robots autonomes ?

Rappelons-nous que l'informatique théorique a été conçue à l'image des capacités humaines, et devient ainsi opérationnelle et expérimentale par la mise en place des robots de plus en plus performants. La performance de ceux-ci est conditionnée, en partie, par la technologie, qui optimise et miniaturise ses composants. Par ailleurs, l'IA et les nouveaux algorithmes, implémentés dans

des automates construits dans un matériel et/ou une technologie de pointe, donnent naissance à des androïdes autonomes, qui sont déjà supérieurs à l'homme dans de nombreux domaines spécifiques. Il suffit donc que tous les domaines soient réunis dans un seul androïde, doté d'algorithmes d'apprentissage, pour créer un être supérieur, et/ou doté d'une super intelligence, qui agira selon le cas, pour le bien de l'humanité ou contre elle.

Nous sommes maintenant très proches d'un processus autonome et intelligent, qui peut nous détruire. Mais, si cela existe pour certains d'entre nous, personne n'écartera le danger, car les grandes entreprises sont aveuglées par la logique du « tout profit », et l'armée par la logique du « plus fort ». Personne ne songe à l'espèce humaine et à son devenir. La société militaire, comme la société civile, use de son pouvoir technologique, en amoindissant peu à peu le pouvoir politique, qui semble devenir de plus en plus faible, et qui pourrait disparaître. Fin 2013, une association a été créée en Californie, qui a regroupé 12 grandes sociétés spécialisées dans les technologies numériques: Google, IBM, HP, Twitter, Facebook, SUN, Microsoft, Oracle, etc.

Il s'agit là de sociétés multinationales, ayant toutes plus de 100 000 employés, et le double objectif de ce regroupement était à la fois de diminuer le prix de la publicité, et aussi de discuter d'égal à égal avec les 240 gouvernements (environ) qui règlent le sort des 7 milliards d'êtres humains : ces objectifs ont été très vite atteints. En

réaction, toujours aux États Unis, il y a environ 2 ans, s'est constitué un ensemble de plusieurs milliers de personnes, menées par un dirigeant de la société Apple : ce groupe s'oppose à la volonté du président Obama, et de son conseiller Bill Gates, de faire la guerre uniquement avec des robots. Un expert du gouvernement Obama a dit que la troisième guerre mondiale sera très rapide, et très meurtrière.

L'année 2016 aura vu, également en Californie, une autre association de grandes sociétés internationales, cette fois-ci autour de l'intelligence artificielle, essentiellement pour les robots².

(2) « Le Temps » du 5 février 2015

Alors « Combien de temps faudra-t-il aux robots, ou à ceux qui les dirigent aujourd'hui, pour s'apercevoir que l'espèce humaine est devenue inutile? ».

Si la politique est devenue un mal nécessaire, peut-on accepter que l'humanité tout entière soit maintenant entre les mains de grandes compagnies multinationales, qui auront le pouvoir de contrôler une armée de robots ? L'homme pourrait devenir non pas le maître, mais l'esclave, de ce nouveau genre d'êtres, que sont les robots. Notre seule sauvegarde à ce stade pourrait être d'établir un rempart légal pour imposer une législation qui ne viendra pas toute seule, et instaurer un contrôle technologique adapté au problème qui se pose.

Pour un dialogue sans ambiguïté entre l'homme et la machine

par **SERGE TISSERON**

P

Parallèlement aux formidables opportunités qu'ils offrent, notamment dans le domaine industriel, de l'éducation et de la santé, les robots font courir un certain nombre de risques qu'il est important d'identifier et de prévenir. Certains de ces risques ne leur sont pas spécifiques, notamment ceux qui concernent les emplois et la protection de la vie privée. Mais d'autres risques sont liés à leurs particularités, notamment à la possibilité d'interagir avec eux par la parole comme avec un humain, et à leur éventuelle capacité de percevoir nos

émotions et d'y répondre.

Ces caractéristiques, jointes au pouvoir qu'ils auront de nous sauver la vie dans diverses circonstances, vont considérablement

augmenter les projections anthropomorphes sur eux. D'autant plus que les mots utilisés pour évoquer les capacités des robots sont exactement les mêmes que pour l'être humain : intelligence, autonomie, apprentissage, empathie, etc. Un premier risque serait d'oublier que les robots sont programmés et connectés, un second de croire qu'ils puissent avoir de vraies émotions alors qu'ils ne seront jamais que des machines à simuler, et un troisième de finir par préférer des robots prévisibles et toujours gratifiants à des humains imprévisibles et souvent plus préoccupés d'eux-mêmes que de nous... Autrement dit, nous ne devons pas seulement veiller à nous protéger des dangers que les robots pourraient nous faire courir, mais aussi à nous protéger contre le risque d'une mauvaise appréciation de leurs capacités. Ces risques appellent trois séries de mesures : législatives, technologiques et éducatives.



SERGE TISSERON

Psychiatre, membre de l'Académie des Technologies, docteur en psychologie



La « personne électronique » proposée en janvier 2017 par le Parlement européen pour désigner les robots constitue un obstacle pour une saine appréciation de leur réalité.

Un dialogue sans ambiguïtés entre l'homme et la machine

L'homme a toujours perçu ses outils comme relevant de sa seule maîtrise. Il devait donc apprendre à s'en servir. Mais le développement de l'Intelligence artificielle (IA) est en train d'inverser cette logique. Avec la robotique, ce n'est pas nous qui allons être obligés de nous adapter aux robots, ce sont les robots qui s'adapteront à nous. Mais si ce renversement a de quoi séduire, il ne rassure pas pour autant. Si j'achète un marteau ou une voiture, dans les deux cas je suis son propriétaire et je les contrôle totalement. Mais si j'achète un robot, je ne sais pas comment son fabricant l'a programmé, et je ne sais pas non plus si un hacker ne va pas un jour le retourner contre moi. C'est pourquoi l'homme a besoin de croire que les

machines dites autonomes auront un jour une conscience, une volonté et un libre arbitre pour pouvoir espérer les apprivoiser. Le mythe du robot doué d'une conscience est un peu en cela l'équivalent de la prostituée au grand cœur : plus l'homme accepte de se mettre en situation de vulnérabilité, plus il a besoin de penser que la créature, entre les mains de laquelle il se remet, a un cœur. L'idée que l'on puisse un jour donner une conscience aux robots obéit à cette logique : nous permettre de ne plus être effrayé par le robot comme une machine qui serait appelée à réaliser un programme en n'éprouvant ni état d'âme, ni pitié, ni empathie. Nous imaginons une conscience aux robots pour tenter de réenchanter le monde de la robotique placé aujourd'hui sous le signe du robot réalisant le programme que ses

constructeurs ont conçu pour lui. Le robot "libre" peut être méchant, mais parce qu'il est libre, on peut rêver de le faire changer d'avis. Des déportées ont raconté qu'elles étaient rassurées de voir leurs tortionnaires nouer des liaisons amoureuses avec leurs homologues masculins ; cela les rassurait sur le fait que ces femmes, qui leur paraissaient insensibles et "robotisées", étaient toujours des êtres humains, et qu'on pouvait, peut-être, en s'y prenant bien, les attendrir. Cela a aidé ces déportées à vivre.

Le problème, avec les robots, est évidemment bien différent, mais il repose sur la même logique. Les imaginer avoir une conscience nous permet de penser pouvoir les influencer même si nous ne connaissons pas leurs programmes. Bien sûr, cela risque en même temps de nous faire sous-estimer l'efficacité des programmeurs qui entretiennent cette illusion et donc de nous rendre plus vulnérables encore aux manipulations de toutes sortes ! Mais si nous voulons combattre efficacement le penchant d'un grand nombre de nos contemporains à avoir une représentation des robots qui doit plus à la science-fiction qu'à la réalité, nous devons d'abord ne pas nous tromper sur sa cause. Ce fantasme ne relève pas d'une mauvaise appréciation de la réalité des robots, comme on pourrait d'abord le croire. Il témoigne au contraire d'une excellente appréciation du

risque que le robot, préprogrammé et sans cesse reprogrammé à distance par ses concepteurs, échappe totalement à ses utilisateurs. Il cherche à y opposer également une vision qui n'est pas forcément plus rassurante, mais qui restitue à l'homme sa part d'initiative et de liberté.

Des mots et des pratiques qui brouillent les repères

La tentation d'accorder aux robots des pouvoirs bien plus grands que la réalité est, hélas, encouragée par l'anthropomorphisme du langage, mais aussi par des pratiques problématiques.

Les pièges du langage

En parlant d'autonomie, d'intelligence, de capacités d'apprentissage, d'empathie et de réseaux de neurones pour les robots, nous risquons d'oublier que ces expressions ne désignent pas du tout la même chose que chez l'être humain. Ce sont des métaphores, et elles risquent en outre de nous cacher que, quelle que soit l'autonomie que nous leur imaginons, ces machines resteront toujours reliées à leur fabricant. Pour leur mise à jour bien entendu, mais aussi pour la capture de nos données personnelles, pour leur adaptation à nos attentes et éventuellement pour nous manipuler à notre insu ! Autrement dit, ce discours anthropomorphe n'est pas neutre. Il cache les algorithmes qui dirigent les machines et la responsabilité immense de

ceux qui les fabriquent. C'est pourquoi il serait judicieux que nous soyons plus attentifs au langage que nous utilisons pour parler de ces nouveaux outils que sont les robots. Il vaudrait mieux parler de machines automatiques plutôt qu'autonomes, d'apprentissage automatique plutôt que d'intelligence artificielle, de simulation d'empathie plutôt que d'empathie artificielle, et de réseaux de composants électroniques plutôt que de réseaux de neurones. De ce point de vue, l'expression « *personne électronique* » proposée en janvier 2017 par le Parlement européen pour désigner les robots va constituer un obstacle de plus sur le chemin d'une saine appréciation de leur réalité. Rappelons que dans la philosophie occidentale, du point de vue social, la personne se différencie de l'individu en tant qu'elle est définie par ses droits et ses devoirs. Et du point de vue structurel, elle est associée à la conscience qu'elle a d'exister et à sa capacité de distinguer le bien du mal. Créer un statut de personne électronique, c'est inévitablement introduire à court terme la question des droits et devoirs des robots, et à moyen terme celle du droit à l'autodétermination. Dans le même ordre d'idées, il serait d'ailleurs salulaire d'interdire toutes les publicités qui parlent des machines dans des termes qui évoquent la spécificité humaine : les machines n'ont pas d'émotions et pas de cœur. Croire autre chose ferait courir à l'homme de grands dangers.

Des pratiques créatrices de confusion

Ce risque de confusion n'est pas seulement alimenté par la publicité. D'ores et déjà, l'ordinateur Watson répond aux clients d'une grande banque française sans que ceux-ci sachent qu'ils ont affaire à une IA. Un petit robot ressemblant à un enfant, appelé Kaspar, est aujourd'hui utilisé avec de jeunes autistes en étant téléopéré (c'est-à-dire que les paroles et les comportements du robot sont gérés en temps réel à distance par un informaticien invisible de ses

(1) C'est ce qu'on appelle la méthode WOZ, pour *Wizard of Oz*, en français le magicien d'Oz.

utilisateurs¹⁾ sans que ces enfants en soient informés. De

telles pratiques posent évidemment un problème éthique majeur. D'autant plus que certains chercheurs, comme Hiroshi Ishiguro, rêvent que nous puissions bientôt demander des conseils à des robots androïdes, dans des grands magasins, en croyant qu'il s'agit de vendeurs humains. Mais si cela est acceptable dans la culture japonaise, n'oublions pas nos propres traditions. L'humanisme occidental est fondé sur une claire distinction entre vivant et non vivant. Un principe démocratique pose que chaque citoyen a le droit de connaître l'origine des messages qu'il reçoit. Par exemple, personne n'a le droit d'imprimer des affiches en noir et blanc parce que ces deux couleurs sont réservées aux affiches officielles émanant de l'État et il est interdit à une chaîne de télévision de

transmettre des publicités pendant le journal télévisé en leur donnant le statut d'informations. De même, la publicité rentre dans une fenêtre de publicité, l'information dans une fenêtre d'information, la fiction dans une fenêtre de fiction, etc. Le même principe doit être respecté dans nos relations aux machines. Tout humain a le droit de savoir à quel moment il a affaire à un semblable et à un robot. D'autant plus que s'agissant des tchatbots qui sont appelés à se généraliser, le problème serait assez facile à résoudre. Il suffirait de prévoir un message vocal disant : « *Vous êtes en communication avec un système automatique, posez votre question, si vous préférez parler à un humain, appuyez sur la touche dièse* ». Mais les constructeurs ne voient aucun intérêt à en prévenir les usagers, puisque le but de ces systèmes est justement de réduire les emplois... Il y faut donc une volonté politique.

Les dangers de la confusion

De telles sources de confusion sont évidemment porteuses de grands dangers. J'en vois au moins trois : oublier que la machine mémorise tout et peut tout transmettre en temps réel à son fabricant ; oublier qu'une machine n'a pas d'émotions et qu'elle est seulement capable de les simuler ; et même oublier que les robots ne seront jamais des modèles pour les humains.

La machine transmet en permanence des informations

Aujourd'hui déjà, nos ordinateurs et nos smartphones enregistrent et transmettent nos données personnelles. Mais il s'agit d'une transmission ponctuelle, réservée aux moments où nous utilisons ces outils, et d'une transmission explicite puisque nous en sommes informés. Mais demain, avec les objets connectés de toutes natures qui nous entoureront (encore appelés « robjets »), cette capture se fera de façon permanente et implicite : nos compteurs d'eau et d'électricité, nos réfrigérateurs, nos véhicules autonomes, nos brosses à dents... pourront transmettre des données sur nos habitudes, nos déplacements, nos paroles et même nos constantes biologiques. D'ores et déjà, les robots installés dans des chambres d'hôtel à Tokyo montrent que les clients qui interagissent avec eux ne pensent pas à les débrancher lorsqu'ils ne s'en servent pas, et qu'ils vivent leur intimité comme si le robot n'était pas là. Ils y voient des amis dévoués et fidèles. Ils oublient que ce sont en même temps des mouchards potentiels. Pourtant, une note les en a avertis : « *Pour des raisons de sécurité, tout ce que ce robot filme et enregistre est transmis à un PC de sécurité.* »

Oublier que la machine n'a pas d'émotions

Avec les robots dotés d'empathie artificielle, c'est-à-dire capables de

comprendre les émotions humaines et d'y répondre par des intonations et des mimiques parfaitement simulées, l'homme va être plus enclin que jamais à établir avec un objet non humain une relation semblable à celle qu'il développe avec ses semblables. Il le fera d'autant plus que l'objet sera capable de lui donner l'impression qu'il le comprend en lui répondant de façon appropriée. À tel point que l'homme pourrait oublier que le robot simule, et croire qu'il éprouve de vraies émotions. Ainsi, une vidéo expérimentale mise en ligne par les concepteurs du robot « Atlas » (qui se déplace et porte des objets) a suscité de vives réactions des internautes, choqués par le fait qu'un chercheur renversait le robot avec un grand bâton pour tester sa capacité à se redresser après une chute. Comme si le robot en avait souffert !

Le problème est que si l'homme oublie que son robot n'est qu'une machine qui ne ressent rien, il peut être amené à se mettre en danger pour le protéger. Ainsi, l'armée américaine a pu observer que les soldats qui utilisent des robots démineurs « *interagissent parfois avec eux comme ils le feraient avec un être humain ou un*

(1) Singer P.W. (2009), *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, New York, The Penguin Press.

animal »². Ils savent très bien que ces robots sont des outils, mais ils ne

peuvent pas s'empêcher de les traiter comme un animal domestique, voire comme un autre humain, allant même,

pour certains d'entre eux, jusqu'à mettre leur vie en danger pour éviter que leur machine soit endommagée par l'ennemi ! Cette situation pourrait tout aussi bien se produire au domicile d'une personne âgée, ou sur un lieu de travail. On sait que les salariés montrent déjà une forme d'attachement à leurs outils de travail. Qu'en sera-t-il quand ils seront accompagnés d'un robot qui semble les comprendre ?

Le robot n'est pas un modèles pour les humains

À force d'interagir avec des robots obéissants, jamais fatigués et toujours gratifiants, certains d'entre nous risquent de se fabriquer une idée fausse de ce qu'est une relation et d'attendre la même chose des humains avec lesquels ils sont en contact. Notre curiosité envers des êtres plus imprévisibles pourrait se tarir et la communication entre humains devenir elle aussi de plus en plus factice. Nos téléphones mobiles nous ont rendus moins tolérants à l'attente. Nos robots risquent de nous rendre moins tolérants au caractère imprévisible de toute relation.

Prévenir les ambiguïtés dans trois directions complémentaires

Ces dangers ne sont pas une fatalité. Les moyens de les réduire concernent à la fois le législateur, les fabricants de robots et le domaine éducatif.

Le rôle du législateur

Les entreprises qui utiliseront l'intelligence artificielle pour répondre à leurs clients n'ont aucun intérêt à le dire, et celles qui utilisent l'anthropomorphisme du langage pour vendre des robots qui ont du cœur, comme elles le prétendent, n'ont aucun intérêt non plus à renoncer à ces publicités séductrices. L'État a donc d'abord le devoir d'informer. Cela comporte au moins trois aspects : que le citoyen sache toujours s'il a affaire à une machine ou à un humain ; que l'utilisateur d'une machine puisse connaître les algorithmes qui la dirigent ; que les citoyens soient protégés des publicités mensongères qui vendent des robots en utilisant un discours anthropomorphe trompeur.

Mais en même temps, dans la mesure où les robots sont appelés à être partout présents dans nos vies, dans nos maisons, nos rues et nos bureaux, il est essentiel d'organiser une large concertation autour des problèmes qui ne vont pas manquer de se poser. Il est urgent de ne pas laisser la seule responsabilité des robots, auxquels nous aurons affaire demain, et qui, pour une part, auront la capacité d'influencer nos décisions, voire de les prendre à notre place, aux seuls producteurs de ces machines. Il est essentiel que soit mis en place un groupe de réflexion et de propositions pluripartites, comportant à la fois des industriels et des chercheurs en

robotique, mais aussi des sociologues, des philosophes, des anthropologues et des psychologues, sans oublier des représentants des diverses religions. Il s'agit de déterminer, ensemble, la place à donner aux machines automatiques dans nos sociétés.

La responsabilité du roboticien

Pour éviter toute confusion, les constructeurs peuvent faire en sorte qu'une partie de la mécanique du robot soit toujours visible, afin de nous rappeler sa nature de robot. Signalons d'ailleurs que c'est exactement le choix opposé qui prévaut dans le cas des robots domestiques : cacher le plus possible les câbles, les circuits et les composants du robot ! Mais l'essentiel consisterait à concevoir des programmes dans lesquels les robots ne seraient pas destinés à remplacer des humains dans les interactions, mais à favoriser les contacts et les échanges entre les humains. Pour y parvenir, de tels robots n'ont pas besoin d'être humanoïdes. C'est ce que j'appelle des robots humanisants.

L'enjeu de l'éducation

L'éducation des enfants doit d'ores et déjà prendre en compte les données du nouveau monde dans lequel ils vivront pour les y préparer au mieux. Il faut pour cela développer chez eux le goût de l'imprévisible et de l'humain, par l'organisation de débats et de controverses, mais aussi les inciter

constamment à penser la complexité du monde en prenant en compte des jugements à la fois opposés et complémentaires. Les robots seront, selon le titre d'un livre évidemment écrit par un roboticien, « *le meilleur ami de l'homme* », mais ils seront tout autant, et en même temps, les pires mouchards que les humains aient jamais inventés. Il nous faudra apprendre à les considérer dans le même moment comme des assistants dévoués et efficaces, mais être capable à tout instant de les débrancher, même si des fabricants ingénieux font en sorte que nous ayons alors l'impression de les tuer ! Bref, nous devons dans le même moment leur faire confiance et nous en méfier. Si nous basculions du second côté, nous nous priverions de tous les services qu'ils peuvent nous rendre, et s'il nous arrivait de basculer du premier côté, nous aurions tôt fait de les juger comme supérieurs en tous points aux êtres humains.

Nous voyons que les directives machines concernant les robots, aussi importantes soient-elles, ne résolvent pas tous les problèmes posés par eux. Elles protègent l'homme des dangers matériels et physiques que les machines peuvent lui faire courir, mais elles ne le protègent pas des dangers qu'il risque de se faire courir à lui-même par une mauvaise appréciation de ce que sont les robots. Ce sont ces protections que nous devons aussi développer, parallèlement aux indispensables directives machines. L'enjeu est le maintien des repères qui fondent la différence entre l'humain et le non humain. Ce maintien est la condition pour vivre en paix avec les robots, en leur demandant tout ce qu'ils peuvent nous apporter, sans jamais attendre d'eux ce que seuls des humains peuvent nous donner. C'est aussi, rappelons-le, une base essentielle de l'humanisme occidental.

L'Homo cyberneticus

par **MARC WATIN-AUGOUARD**

L

La transformation numérique, par l'effet cumulatif des nouvelles technologies, bouleverse nos modes de vie, nos rapports à la santé, au travail, à la création, à la formation, à l'information, etc. Elle bouleverse surtout le rapport de l'homme au monde et avec lui-même. L'homme « augmenté » sera-t-il « diminué » face à des robots qui pourraient le dominer ? Que restera-t-il de son identité, de son autonomie, de son intimité dans un environnement où tout ce qu'il pensera, dira, fera, utilisera

sera capté, mesuré, évalué et, le cas échéant, automatiquement sanctionné ? Avec la « robolution », l'homme sera-t-il servi ou asservi ? Du « robot-homme » à « l'homme-robot », existe-t-il

une barrière infranchissable ? Plus que jamais vont se trouver posées des questions d'éthique, de déontologie. La réponse qui leur sera apportée sera déterminante pour l'avenir de l'individu et de la société.

L'homme augmenté

L'Homo cyberneticus, pour les plus optimistes, sera un « homme augmenté ». Ainsi, le cyberspace pourrait donner des ailes au courant transhumaniste, dont la doctrine est clairement explicitée, en 1999, dans la Déclaration de l'Association transhumaniste mondiale : « 1/ Les transhumanistes prônent le droit moral, pour ceux que le désirent, de se servir de la technologie pour accroître leurs capacités physiques, mentales ou reproductives et d'être davantage maîtres de leur propre vie. Nous souhaitons nous épanouir en transcendant nos limites biologiques actuelles.



MARC WATIN-AUGOUARD

Directeur du CREOGN
Fondateur du FIC
Président du CECyF



La techno-médecine et la technologie numérique laissent entrevoir un homme augmenté dont on compensera les insuffisances physiques et mentales.

2/ Nous prônons une large liberté de choix quant aux possibilités d'améliorations individuelles. Celles-ci comprennent les techniques afin d'améliorer la mémoire, la concentration et l'énergie mentale, les thérapies permettant d'augmenter la durée de vie ou d'influencer la reproduction, la cryoconservation et beaucoup d'autres techniques de modification et d'augmentation de l'espèce humaine. »

Une utopie ? Sans doute pas, si l'on se réfère au rapport de Mihail Rocco et de William Bainbridge sur les Technologies convergentes pour l'amélioration de la

(1) *Converting Technologies for Improving Human Performance*, juin 2002, www.wtec.org.

performance humaine¹ publié, en 2002, par la National Science Foundation (NSF) de Washington et le Département du Commerce américain. Ces technologies, regroupées sous l'acronyme NBIC, sont les nanotechnologies, les biotechnologies, l'informatique et les sciences cognitives, dont l'intelligence artificielle et les

(2) Des puces inspirées du cerveau humain donneront de « l'intelligence » aux objets connectés.

sciences du cerveau². Pour la NSF, « Une théorie computationnelle de l'esprit peut nous permettre de développer de nouveaux outils pour guérir ou maîtriser les effets

des maladies mentales. Elle sera certainement à même de nous fournir une appréciation plus profonde de ce que nous sommes et sur la place que nous occupons dans l'univers. Comprendre l'esprit et le cerveau nous permettra de créer une nouvelle espèce de machines intelligentes, capable de produire une richesse économique sur une échelle jusqu'alors inimaginable. L'ingénierie de l'esprit est donc beaucoup plus que la poursuite d'une curiosité scientifique, beaucoup plus qu'un monumental défi technologique. C'est l'occasion d'éradiquer la pauvreté et d'ouvrir un âge d'or pour l'humanité tout entière ».

La recherche de l'homme « augmenté » n'est plus de la science-fiction, ni le fruit des élucubrations d'originaux, mais un axe de réflexion et d'action pour les services et organismes les plus sérieux.

Google a bien compris cette opportunité. L'entreprise de Mountain View, que certains prennent encore pour un simple moteur de recherche, a bien d'autres ambitions qui s'affichent dans l'acquisition ou la création d'entreprises NBIC, le parrainage de la Singularity University, qui forme des spécialistes NBIC, et la création en 2013 de Calico, start-up qui a pour objectif d'augmenter la durée de la

(3) Ray Kurzweil a inventé le concept de « singularité technologique », selon lequel à partir d'un certain niveau technologique, les progrès de la civilisation seront exclusivement le fruit de l'intelligence artificielle.

vie de vingt ans d'ici à 2035... Google, que le visionnaire Ray Kurzweil³ a rejoint, en 2012,

pour travailler sur l'apprentissage automatisé et le traitement du langage, annonce pour 2060 l'avènement d'une intelligence supérieure à l'intelligence humaine.

Le projet Avatar 2045 du milliardaire russe Itskov Dmitri donne une idée de l'ambition pharaonique qui guide les transhumanistes rassemblés lors du Congrès International « Global Future 2045 », en juin 2013, à New York. Le calendrier est explicite :

Entre 2015 et 2020, réalisation d'une copie robotique du corps humain

UN PEU DE POÉSIE

« Je ne veux pas vivre dans un tel monde. Je veux pouvoir toucher une fleur qui éclot et la sentir. Je veux pouvoir serrer quelqu'un dans mes bras et lui dire que je l'aime, face à face. Je veux regarder le soleil se coucher avec une larme coulant le long de ma joue. Je veux pouvoir sentir la brise sur mon visage, sentir le fumet d'un repas qui se prépare. Je veux me sentir connecté de façon humaine. Je ne veux pas être assis dans un costume gris pendant qu'on m'explique ce qui est cool, dans un hall à air conditionné illuminé de leds, où des appareils électroniques enregistrent chaque mouvement de mes yeux. Être humain, c'est être libre ».

Réaction sur internet suite à la publication, le 21 février 2016, sur le compte Facebook de Mark Zuckerberg, d'une photo le montrant traverser une foule assise avec un casque de réalité virtuelle devant les yeux.

contrôlée à distance par une interaction cerveau-ordinateur ;

Entre 2020 et 2025, création d'un avatar dans lequel un cerveau humain pourra être créé : un cerveau biologique dans un corps artificiel ;

Entre 2030 et 2035, création d'un avatar avec un cerveau artificiel dans lequel pourra être transplantée la personnalité d'un être humain à la fin de sa vie ;

Entre 2040 et 2045, création d'un avatar hologramme...

Si l'augmentation par l'informatique et la techno-médecine demeure dans le champ de l'humain, dès lors qu'il s'agit de réparer des organes défaillants ou de faciliter la mobilité (exosquelette), les évolutions escomptées sont d'un tout

autre ordre⁴. Elles auront pour conséquence, si l'on n'y prend garde, un changement radical de l'humanité.

Comme le souligne le philosophe Jean-

Michel Besnier, « *on est en train de préparer une humanité à deux vitesses. La fracture ne sera plus entre le nord et le sud, mais au sein même des sociétés*⁵ ». Qui va-t-on augmenter ? A quel coût ? Selon quel choix ? « Être ou ne pas être augmenté, voilà la question ! ».

(4) Voir le film *Transcendance*, sorti le 25 juin 2014 : Singularité, croyance que la conscience des machines va bientôt émerger (2029), l'homme vivra alors 1000 ans ou plus mais il sera un sous-homme.

(5) « Transhumanisme : vers une guerre des mondes », *Libération*, 26 mars 2014.

Tout cela doit être pris au sérieux. Le premier salon transhumaniste TransVision 2014 s'est tenu en France du 20 au 22 novembre 2014. Didier Renard, premier diplômé français de la *Singularity University*, déclare : « *Bientôt vous pourrez sauvegarder votre mémoire cérébrale sur un support électronique. Ce jour-là, vous aurez envie d'un cloud souverain, un coffre-fort inviolable de votre identité géré par des organisations qui auront le sens de l'État avant d'avoir celui des affaires. Nous n'avons pas les ressources financières et humaines pour proposer un projet de société alternatif, cela dépasse clairement notre mission. Mais nous avons l'ambition d'être ce refuge quand cela sera nécessaire. D'ici là, l'État devra avoir défini l'acceptable, l'éthique et le responsable, le tout dans un cadre législatif et juridique imposé à*

(6) Interview, *Le Point*, 9 octobre 2014.

(7) Robotique de services : « La France est la Californie de l'Europe », *Le Parisien*, 5 mars 2014.

(8) Auteur de *La mort de la mort*, Editions JC Lattès, 2001, Interview *Journal du Dimanche*, 8 février 2014.

*tous, y compris, et bon gré mal gré, aux libertariens et autres transhumanistes qui veulent nous imposer leur propre vision du progrès et de l'humanité*⁶ ».

La « robolution » : l'homme servi ou asservi ? Du « robot-homme » à « l'homme-robot »

Avec la transformation numérique, la robotique connaît une impulsion sans précédent. Mais le robot sera-t-il un auxiliaire de l'homme, l'égal de l'homme

RÉFÉRENCES

« Qui sera le successeur de l'Homme ? La réponse est que nous créons nos propres successeurs. L'Homme deviendra pour les machines ce que le cheval et le chien sont à l'Homme ».

Samuel Butler, 13 juin 1863, *The Press*, sous le pseudonyme de Cellarius

« Dans peu d'années, les cerveaux humains et les ordinateurs seront reliés très étroitement et ce partenariat permettra la création d'une pensée nouvelle et d'un traitement de données sans rapport avec celui que nous connaissons aujourd'hui ».

John C.R. Licklider "Man Computer Symbiosis"

« Les gens ne se rendent pas compte que les robots vont les remplacer »

Bill Gates

« A l'horizon 2030, nous pouvons imaginer des systèmes complètement automatisés de création et fourniture de services dans un contexte multifournisseurs. Suite à la demande de service d'un usager, le système serait capable de la décomposer dans des services élémentaires (ce qui inclut la connectivité réseau), de découvrir qui fournit ces composants et de choisir les fournisseurs en fonction de divers critères extraits de la demande de l'utilisateur (qualité, sécurité, prix), d'orchestrer et de composer le service, de négocier avec les parties l'allocation nécessaire des ressources, de surveiller le service en fournissant à l'utilisateur des informations sur la qualité et les performances et d'adapter dynamiquement le service en fonction de l'évolution des usages, en particulier de la charge »

La dynamique d'internet
Prospective 2030

Commissariat général à la stratégie et à la prospective

« La robotique de service existe dans deux catégories, personnelle et professionnelle. Il y a déjà le robot aspirateur et le robot médical. L'industrie est passée aux machines intelligentes et collaboratives. La transformation de cette robotique de service va toucher les aspects de notre quotidien, comme l'apparition de robots dans la logistique ou les transports avec les drones. Des robots agricoles sont en cours de développement pour trier les mauvaises herbes ou traire les vaches. De nouveaux robots pour la maison, tels que les robots de présence pour surveiller des personnes âgées ou des handicapés arriveront d'ici 2 à 5 ans ».

Bruno Bonell, président du syndicat français de la robotique ⁷

« La bataille entre le microprocesseur et le neurone a commencé et l'intelligence artificielle arrive à grand pas. Selon la loi de Moore, la puissance informatique double très rapidement. Le nombre d'opérations réalisées par les plus gros ordinateurs est multiplié par mille tous les dix ans et donc par un million en vingt ans. En 1950, un ordinateur effectuait mille opérations par seconde. Aujourd'hui, on atteint trente-trois millions de milliards d'opérations par seconde. Ce sera mille milliards de milliards en 2029 ! Autour de 2040 émergeront des machines dotées de la capacité du cerveau humain. Et d'ici à la fin du siècle, elles nous dépasseront en intelligence, ce qui poussera l'homme à vouloir « s'augmenter » par tous les moyens. Imaginez si de tels robots, plus forts que nous, ayant accès à l'intelligence artificielle et à l'impression 3D, connectés et contrôlant internet existaient... leur pouvoir de manipulation serait quasi illimité. »

Laurent Alexandre⁸

ou supérieur à l'homme ? Tel est l'enjeu majeur de la « robolution » que nous allons vivre.

Les robots en quête d'autonomie

La robotique est déjà entrée en application, notamment dans l'industrie. La France bénéficie d'ailleurs d'une capacité d'innovation reconnue dans le monde qui a motivé la création, en mars 2014, du fonds d'investissement capital-risque « Robolution Capital » pour favoriser le développement d'une filière.

Comme le souligne Bruno Bonnell, initiateur du fonds, tous les secteurs vont être touchés par cette forme d'intelligence apportée aux machines. Le robot classique a permis de libérer le travail des tâches les plus répétitives et d'améliorer la qualité du produit fini. Le robot du futur aura une tout autre performance. S'effectuera en effet, le passage de la génération des robots Automates programmés industriels (API) à celle des robots dotés d'une intelligence artificielle, capables d'apprendre eux-mêmes grâce à un processus d'apprentissage automatique et d'accomplir des tâches que ne peuvent autoriser les traitements algorithmiques classiques. C'est ce que l'on appelle le *machine learning* qui s'appuie notamment sur le traitement de mégadonnées. Le *deep learning* (apprentissage en profondeur) est une forme encore plus élaborée de *machine learning* qui veut agir comme le cerveau

« Même si un jour on construit des systèmes par certains aspects plus complexes ou performants que les humains, ils vont être construits pour des tâches spécifiques. On associe trop souvent l'intelligence artificielle aux qualités et aux défauts humains. Il n'y a aucune raison que les machines que l'homme concevra aient comme lui des désirs, des pulsions et des défauts ! ».

Yann Le Cun

humain avec un système de type neuronal. Le programme informatique se perfectionne sans intervention de l'homme par un apprentissage non

(9) Dans un apprentissage supervisé, l'homme corrige la machine lorsqu'elle commet une erreur.

(10) Yann Le Cun, chercheur et directeur du laboratoire de recherche en intelligence artificielle de Facebook, professeur invité sur la Chaire informatique et sciences numériques. « L'apprentissage profond : une révolution en intelligence artificielle », leçon inaugurale au Collège de France, 4 février 2016.

supervisé⁹. Selon Yann Le Cun¹⁰, « *La technologie du deep learning apprend à représenter le monde. C'est-à-dire comment la machine va représenter la parole ou l'image ?* ».

On peut attendre de ces robots « intelligents » des progrès considérables dans le domaine de l'assistance aux personnes, de la sécurité, de la surveillance, tant du point de vue qualitatif que du point de vue quantitatif.

Par exemple, Dubaï envisage de mettre en œuvre des patrouilles de robots policiers autonomes dans les centres commerciaux et d'autres lieux lors de l'Exposition universelle de 2020... En juillet 2016, à Dallas, pour neutraliser

l'auteur du meurtre de cinq policiers retranché dans un parking, la police américaine a fait usage d'un robot

(11) L'entreprise israélienne General Robotics Ltd a mis au point Dogo, robot armé pour les opérations spéciales.

télécommandé équipé d'un explosif¹¹. Il s'agit vraisemblablement

d'un robot déjà utilisé par l'armée américaine en Irak. Certes, en l'occurrence, il s'agit d'un engin dépendant de l'action humaine, puisque télécommandé, mais on peut imaginer demain des robots entrant en action proprio motu. Cette utilisation offensive d'un robot renvoie au rapport, publié le

(12) Mind the Gap : Yhe Lack of Accountability for Killer Robots.

(13) Clinique des droits humains internationaux de la Faculté de droit de l'Université d'Harvard.

9 mars 2015¹², par l'ONG *Human Right Watch* et l'université d'Harvard¹³, qui demande à l'ONU de se saisir de la

question des robots « tueurs » pour définir la responsabilité juridique : l'État, le fabricant, une tierce personne ? Le Centre de recherche des écoles de Coëtquidan (CREC) approfondit la réflexion sur la robotique du champ de bataille, notamment avec le *Combat Studies Institute* de l'*US Army*.

Vers un statut juridique du robot ?

Le robot va-t-il remettre en cause tous les principes sur lesquels reposent aujourd'hui les règles de responsabilité civile ou pénale et créer des déséquilibres, notamment financiers ?

(14) Mady Delvaux, eurodéputée luxembourgeoise, Rapport 2015/2013 (INL) contenant des recommandations à la commission concernant des règles de droit civil de la robotique, Commission des affaires juridiques, 31 mai 2016.

En mai 2016, Mady Delvaux¹⁴ a déposé un rapport, à destination de la Commission européenne, relatif à

un projet de directive sur les règles de droit civil de la robotique. Parce que « *le développement de la robotique et de l'intelligence artificielle pourrait avoir pour conséquence l'accomplissement par des robots d'une grande partie des tâches autrefois dévolues aux êtres humains* », elle préconise, en particulier, de leur faire payer des cotisations sociales à la place des humains dont ils auront pris l'emploi et de créer un revenu universel de base pour tous ceux qui n'auront plus accès au marché de l'emploi. La députée européenne considère que « *grâce aux impressionnants progrès de la technique au cours des dix dernières années, non seulement les robots contemporains sont capables de mener à bien des tâches qui relevaient autrefois exclusivement de la compétence humaine, mais encore que la mise au point de fonctionnalités autonomes et cognitives (comme la capacité de tirer des leçons de l'expérience ou de prendre des leçons indépendantes) rapprochent davantage ces robots du statut d'acteurs interagissant avec leur environnement et pouvant le modifier de manière significative ; que dans un tel contexte, la question de la responsabilité juridique en cas d'action dommageable d'un robot*

(15) Alain Bensoussan, Jérémy Bensoussan, Bruno Maisonnier, Olivier Guilhem, Droit des robots, collection Lexing, éditions Larcier, juillet 2015.

(16) Alexandra Bensamoun, Les robots : objets scientifiques, objets de droits, Mare et Martin, février 2016.

(17) Grégoire Loiseau, Matthieu Bourgeois, La Semaine juridique, Edition Générale, 24 novembre 2014, n°48.

(18) Alain Bensoussan, interview dans « Esprit de Justice », France-Culture, 23 octobre 2014. Alain Bensoussan a fondé l'Association du droit des robots (ADDR).

(19) Dans son rapport précité, Mady Delvaux propose la mise en place d'un régime spécial d'assurance, d'un fonds de compensation.

(20) Alain Bensoussan, « data security and privacy en matière de robot », in Revue de la gendarmerie nationale, n°155.

devient cruciale ».

Faut-il un droit « des robots » ou un droit « pour les robots » ?

En appelant « à trancher la question fondamentale de l'octroi ou non d'une personnalité juridique aux robots », Mady Delvaux donne une résonance à la position d'Alain Bensoussan, avocat spécialisé dans les nouvelles technologies, qui, le premier, a réclamé cette personnalité juridique pour les robots, à l'instar de

celle attribuée aux personnes morales¹⁵.

Aujourd'hui « objets de droits¹⁶ », ils doivent, selon lui, devenir « sujets de droit » ou, au moins, relever d'un droit spécifique¹⁷, car les robots, contrairement aux automates, possèdent une forme d'intelligence, de capacité de compréhension, voire de perception des sentiments¹⁸. Ils peuvent, de ce fait, acquérir une autonomie qui leur permet de prendre des décisions à caractère juridique, par action ou abstention et donc être à l'origine d'un préjudice qu'il faudra couvrir¹⁹. Lorsque l'intelligence artificielle générera une nouvelle intelligence artificielle sans intervention

humaine, les robots franchiront le seuil de singularité technologique. Maître Bensoussan souligne que les robots peuvent être des « *concentrateurs d'intimité* »²⁰, capables de capter, traiter, échanger des données à caractère personnel et notamment médicales des personnes qu'ils assistent. Le robot devrait, selon lui, avoir un nom et même un genre, avec un numéro d'immatriculation²¹. Cette personnalité robotique est contestée par d'autres juristes qui considèrent que les règles de droit existantes sont suffisantes et qu'une telle disposition aurait pour effet de

déresponsabiliser leurs propriétaires²².

La première approche nous semble plus conforme à une réalité qui se dessine et qui ne relève pas de l'utopie ! La réflexion relative au

(21) Le numéro INSEE des hommes commence par 1, celui des femmes par 2. Le robot aurait un numéro d'identification commençant par 3. Mady Delvaux propose une immatriculation dans un registre spécifique de l'Union.

(22) Matthieu Bourgeois et Annita Bonnedjourn, « Créer une personnalité juridique pour les robots est totalement inutile », in L'Usine Nouvelle, 11 février 2015.

droit civil peut être élargie à la responsabilité pénale. La multiplication de machines dans l'espace public, notamment avec des liaisons sans fil, peut engendrer le risque d'une prise de contrôle malveillante ou d'un accident : qui sera responsable pénalement ? Le concepteur, le fabricant, celui qui l'a acquise, celui qui l'utilise, ou le robot ? Lors d'une exposition « *The Darknet : From Memes to Onionland* » qui s'est

tenue à Zurich du 5 au 11 janvier 2015, deux artistes suisses du Mediengruppe Bitnik ont présenté un robot automatisé « *Random Darknet Shopper* » qui fait des achats sur le Darknet, sur le site AlphaBay, à travers le réseau TOR, avec un budget de 100 dollars en bitcoins par semaine. Certaines de ces acquisitions, livrées et exposées au Kunst Halle St.Gallen, soulèvent évidemment des problèmes de droit : un sac Louis Vuitton ou un polo Lacoste contrefait, 10 pilules d'ecstasy, des cigarettes de contrebande, un faux passeport hongrois, etc. Qui est responsable pénalement ? Les artistes qui ont mis le robot en situation d'accomplir un acte illicite ? Aujourd'hui, sans aucun doute, même si la justice leur a finalement rendu leur robot confisqué, mais qu'en sera-t-il demain si le robot acquiert une véritable autonomie, grâce à l'intelligence artificielle qui lui donnera une capacité de discernement, élément clef de la responsabilité pénale ? De même qu'il existe une responsabilité pénale des personnes morales, on peut imaginer une responsabilité pénale des personnes électroniques. Un robot devant des juges, au pénal comme au civil, est-ce une vue

(23) Lors d'une conférence à l'École Nationale de la Magistrature, le 16 octobre 2014, nos propos en ce sens ont reçu un accueil qui mêlait incrédulité et ironie....

de l'esprit ou une réalité dans les dix prochaines années²³ ?

L'homme remplacé ?

La « robolution » va créer la symbiose entre l'homme et la machine, grâce à des

LES TROIS LOIS D'ISAAC ASIMOV (ROMANCIER)

- Un robot ne peut porter atteinte à un être humain, ni, restant passif, permettre qu'un être humain soit exposé au danger ;
- Un robot doit obéir aux ordres que lui donne un être humain, sauf si de tels ordres entrent en conflit avec la première loi ;
- Un robot doit protéger son existence tant que cette protection n'entre pas en conflit avec la première ou la deuxième loi.

interfaces (*Brain Computer Interfaces*). Le dialogue homme/machine pourrait s'accompagner du transfert de l'intelligence humaine vers cette dernière. Le téléchargement de l'esprit (*Mind Uploading*) vise à transférer le contenu d'un cerveau humain sur un ordinateur, sa dématérialisation dans le *cloud* et sa réimplantation dans un robot. Tel est l'objectif du projet *Blue Brain* lancé en 2005 par l'École Polytechnique de Lausanne.

Mais, les capacités n'étant pas limitées (semble-t-il), la machine pourrait devenir plus intelligente que l'homme. Ces robots seront-ils « humains », capables d'avoir des émotions, de percevoir celles des personnes, d'exprimer des sentiments ?

Pour Ray Kurzweil, les robots seront proches des humains en 2029...Selon lui, ils seront « *capables d'intelligence émotionnelle, d'être drôles, de comprendre des blagues, d'être sexy, aimants et de comprendre l'émotion*

(24) Ray Kurzweill, interview dans Wired, avril 2013. Voir également Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology*, New York, Penguin, 2005.

humaine²⁴ ». Le 27 juin 2015, deux robots japonais, Frois et Roborin, ont été « mariés » selon

le rite traditionnel avec comme témoin Pepper, un autre robot. Softbank, le fabricant japonais de Pepper, conçu par la société française Aldebaran Robotics, stipule dans le manuel d'instruction qu'il est interdit d'avoir des comportements sexuels et indécents avec son robot... Mais l'entreprise canadienne Abyss Creation a annoncé qu'elle allait mettre

(25) Le sexe avec des robots, cela pourrait commencer dès 2017. Huffington Post, 22 décembre 2016.

sur le marché un « robot sexuel » en 2017²⁵.

Asimov, le prophète

Prophète, Asimov, auteur américain d'origine russe, l'est sans doute, car les lois qu'il énonce semblent écrites pour le XXI^e siècle. Elles viennent en réaction à l'image du robot tueur véhiculée par la science-fiction des années trente. Pour lutter contre le complexe de Frankenstein, il publie, en 1940, un roman, *Robbie*, qui a pour héros un robot sympathique et noble qui s'occupe d'un enfant. Asimov écrit des nouvelles pour le magazine *Astounding Science Fiction*, dirigé par John Campbell. De leur dialogue va naître la question des relations entre l'homme et le robot au travers de la formulation de trois lois, exposées dans la nouvelle *Runaround* (1942), et qui doivent « être intégrées au plus bas niveau du cerveau

positronique ». En 1948, dans *Les Humanoïdes*, Jack Williamson, applique les trois lois aux robots qu'il met en scène. Près d'un demi-siècle plus tard, Asimov ajoute la « zéroïème loi », par

(26) Isaac Asimov, *Les Robots et l'Empire*, J'ai lu, 1985.

l'intermédiaire du robot Daneel

Olivaw²⁶ : « *Un robot*

ne peut porter atteinte à l'humanité, ni, restant passif, permettre qu'un être humain soit exposé au danger ». En 2014, le chercheur en robotique Alan Winfield a expérimenté la première loi d'Asimov en plaçant un robot devant un trou pour empêcher d'autres robots de tomber dedans. L'expérience montre que le robot est confronté à des difficultés de choix dès que le nombre de robots à protéger augmente.

Vers une cyberéthique ?

L'homme « augmenté » sera-t-il, en vérité, un homme diminué, asservi ? Au-delà du droit, la « Robolution » soulève des questions existentielles qui relèvent de l'identité de l'homme, de son unicité, de sa capacité à décider de manière autonome. Comme l'affirme Gilles

(27) Gilles Babinet, conférence *Changer d'Ère*, Cité des Sciences, 6 juin 2014, www.gillesbabinet.com.

Babinet²⁷, « *les critiques à l'égard de Kurzweil ou de la logique libertarienne*

et utilitariste en vogue outre Atlantique n'auront de pertinence que si nous parvenons à être capables de leur opposer un modèle qui ne soit pas, d'une façon ou d'une autre, un refus manichéen



Une intelligence artificielle à capacité cognitive dépasse rapidement les capacités humaines.

de la modernité ». Pour Stephen Hawking, astrophysicien britannique, enseignant à Cambridge, l'intelligence artificielle menace le genre humain : « Les formes primitives d'intelligence artificielle que nous avons déjà se sont montrées très utiles. Mais je pense que le développement d'une intelligence artificielle complète pourrait mettre fin à la race humaine. [...] Une fois que les hommes auraient développé l'intelligence artificielle, celle-ci décollerait seule et se

redéfinirait de plus en plus vite. Les humains, limités par une lente évolution biologique, ne pourraient pas

(28) Stephen Hawking, entretien sur la BBC, 2 décembre 2014.

rivaliser et seraient dépassés »²⁸. Lors de la conférence

Zietgeist 2015, à Londres, il ajoute « nous devons absolument nous assurer que les objectifs des ordinateurs sont les mêmes que les nôtres ».

On ne peut, de toute évidence arrêter le progrès, mais il existe déjà des situations contemporaines pour lesquelles le droit pénal met un coup d'arrêt aux applications scientifiques les plus folles. Entre ce que l'on sait faire et ce que l'on a le droit de faire, il peut exister un écart, celui établi par la loi et, tout particulièrement dans le cas qui nous intéresse, par le respect de principes généraux qui transcendent les choix et leur confèrent une légitimité. Depuis la loi du 6 août 2004, le code pénal contient des dispositions relatives à la bioéthique médicale. Il interdit, par exemple, le clonage d'êtres humains ou certaines

(29) Stephen Hawking, entretien sur la BBC, 2 décembre 2014.

recherches sur l'embryon²⁹. Il y aura sans doute dans

quelques années un chapitre du code pénal consacré à la « cyberéthique ». Ce chapitre pourrait notamment comprendre les infractions à la loi informatique et liberté de 1978 qui sont déjà des règles d'éthique. Dans sa déclaration du 25 novembre 2014 (art.3), le G29

souligne que la technologie est un moyen qui doit demeurer au service de l'homme : « *Le fait qu'un traitement de données soit techniquement faisable, qu'il puisse parfois révéler des informations utiles au renseignement ou permettre le développement de nouveaux services n'implique pas qu'il soit de ce fait acceptable sur les plans social et éthique, ni qu'il soit raisonnable ou conforme à la loi* » (article 3 de la déclaration). La cyberéthique rejoindra la bioéthique car des recherches sont également entreprises par des israéliens et des américains pour développer un ordinateur biologique, fabriqué à partir de matériel humain, de l'ADN et de l'ARN. Le « transcriptor », nom donné au transistor biologique, permet de créer un ordinateur dans une cellule vivante. Selon Drew Endy, responsable de la recherche, « les ordinateurs biologiques peuvent être utilisés pour étudier ou reprogrammer les systèmes vivants, surveiller l'environnement et améliorer les thérapies cellulaires³⁰ ».

(30) « L'ordinateur biologique a enfin son transistor biologique ! » Sciences-Mag, 29 mars 2013.

Mais il ne suffit pas de créer le droit, il faut aussi le faire appliquer, tâche beaucoup plus complexe dans le monde immatériel que dans le monde réel. Paraphrasant Malraux on pourrait affirmer que « *Le XXI^e siècle sera celui de la cyberéthique ou ne sera pas !* ».

Quis custodiet ipsos custodes ?

Qui gardera les gardiens ?

par **LUDOVIC PETIT**

T

Telle est du moins la question que me vient à l'esprit - je confesse de façon assez instinctive - quand on me parle robot(s), robot(s) autonome(s), Intelligence Artificielle.

De culture professionnelle technique et scientifique, l'Intelligence Artificielle que je perçois, par ailleurs nécessaire à l'évolution technologique que nous vivons de nos jours, est dans la légitimité des choses. Le point qui m'interpelle pour en revenir aux robots, de surcroît dans une perspective de robot autonome, est que l'Intelligence Artificielle doit nécessairement reposer sur un postulat



LUDOVIC PETIT

Directeur Cyber Sécurité
du Groupe Altran,
chercheur au CREOGN
Réserve citoyenne

mathématique formalisé dans un code, donc un développement logiciel, qui lui, va faire évoluer sa structure interne par auto-apprentissage d'un contexte.

Nous touchons donc par essence à la notion d'Intelligence en elle-même, avérée (en tant que champs des possibles) artificiellement par la résultante mécanique opérationnelle d'une séquence logique.

Ce qui m'amène, déformation professionnelle oblige, à m'interroger sur la qualité du développement logiciel qui, rappelons-le, ne constitue(ra) que ce que nous, humains, nous souhaitons qu'il fasse. Avec certes toutes nos qualités... mais aussi avec tous nos défauts.

Les langages de développement vont évoluer c'est indéniable, et par là-même la qualité de service qui y sera associée... pour faire fonctionner ce que nous concevons être aujourd'hui un robot. Ce terme de robot perdurera-t-il ? Je pense qu'il évoluera lui aussi de concert avec l'évolution technologique dont il est tributaire. Sujet philosophique s'il en est.



L'Intelligence artificielle modifiera notre approche conceptuelle de nos modèles mathématiques.

La faculté d'autonomie d'un robot est donc intimement liée à l'Intelligence Artificielle qui, à mon sens, n'en est qu'à ses balbutiements, tant d'un point de vue mathématique que technologique. Le champ des possibles est donc vaste, vraiment vaste, avec pour seules limites celles que nous souhaiterons.

Il est un champ des possibles qui mérite réflexion : comment maîtriser la création d'une intelligence... par une autre ? En d'autres termes et pour revenir au titre de cet essai, qui va – et comment – contrôler cette intelligence ? Le code initial qui sera développé pourra bien évidemment être conçu à dessein, avec un panel de possibilités fonctionnelles déterminées, mais l'intelligence embarquée sera-t-elle suffisamment bien codée, pour en assurer contrôle, gestion et maîtrise ? La résultante de fonctions mathématiques transcrites en langage logiciel abondant

en une action mécanique sera-t-elle toujours la même, en tant qu'approche, code et structure ? J'en doute.

Telle est la question... Entre beaucoup d'autres.

Interrogeons-nous maintenant sur la faculté d'autonomie d'une entité robotique, donc sur l'Intelligence nécessaire à son fonctionnement autonome.

La commission des affaires juridiques du Parlement européen a récemment adopté (en janvier 2017) un projet de résolution réclamant de la Commission des règles européennes en matière de droits des robots. Le texte prévoit de « *créer le statut de personnes électroniques pour les robots autonomes les plus sophistiqués, impliquant des droits et des obligations spécifiques* ». Des « droits de l'homme » pour les machines, en somme.

Le mot est lâché, « personnes électroniques » !

Stephen Hawking, génie de notre temps, physicien théoricien et cosmologiste britannique, a récemment exprimé son point de vue qui a fait débat : « *Est-ce que l'Intelligence Artificielle va sauver ou tuer le genre humain ?* », « *L'Intelligence Artificielle pourrait être la pire chose pour l'humanité* ».

L'Intelligence Artificielle va sauver des vies, dans nombre de secteurs d'activités, médical y compris. C'est donc en soi un complément à ce que nous, humains, pouvons accomplir au quotidien. Avons-nous une aversion (naturelle ?) pour le risque ? Sûrement ! Identifie-t-on l'autonomie d'un robot comme un risque en soi ? Certes, mais nous nous devons d'en adapter l'évolution à notre condition sociétale.

A noter que les membres du Parlement britannique du Comité de la science et de la technologie souhaitent un examen minutieux de l'impact éthique, juridique et sociétal probable de l'émergence de ces technologies, ce qui est légitime.

Elon Musk, PDG de la société Tesla, a déclaré que l'Intelligence Artificielle était la plus grande menace pour la survie de la race humaine.

Comment les langages logiciels vont-ils évoluer ? Ce sujet n'est-il pas en fait l'un des enjeux majeurs de notre temps ?

L'Intelligence Artificielle n'est-elle pas, *in fine*, déjà nécessaire pour faire évoluer les modèles de compréhension mathématiques et logiciels, afin d'en adapter l'usage ? Cette évolution implique une remise en question de notre propre approche à matérialiser cette évolution conceptuelle.

Une brève incise à propos de ce que l'on appelle Sécurité des Systèmes d'Information, afin de matérialiser mon propos relatif au monde numérique dans lequel nous vivons : le début des années 2000 a l'émergence de nouveaux concepts de modèles de fonctionnement informatiques appelés Réseaux Autonomes, dont IBM a d'ailleurs été un des précurseurs. Le concept était (et est toujours) pour un type de réseau d'être capable de s'auto-configurer et de délivrer un service basé sur les ressources contextuelles. Ce même concept a, depuis, été adopté dans une approche Sécurité par les éditeurs de logiciels. Mais nous n'en sommes véritablement qu'aux prémices, les éditeurs rivalisent à propos de solutions embarquant de l'Intelligence Artificielle. Comme nous pouvons le constater, le concept de Robot Autonome est aussi affaire d'entité logicielle. Et ce concept va grandissant, tout comme il nous faudra faire évoluer le cadre légal et réglementaire en conséquence, en fonction des usages, des droits et des devoirs.

Nous avons brièvement abordé le statut de personnes électroniques pour les robots autonomes les plus sophistiqués. Ne sommes-nous pas déjà dans la réalité des faits, au carrefour de la science et de ce que nous considérons jusqu'alors comme de la fiction ?

« *Connecto, ergo sum.* », lâcha l'entité robotique autonome.

« *Quis custodiet ipsos custodes ?* », lui répondit l'autre entité artificielle.

Sommes-nous suffisamment sages pour nous engager sur une telle voie ?

Les débats sont ouverts, le champ des possibles considérable, les enjeux sont majeurs !

Et de nous rappeler ce qu'Albert Einstein disait : « *Artificial intelligence is no match for natural stupidity* ». (« L'intelligence artificielle ne correspond pas à la bêtise naturelle. »)

A méditer.

PS : peut-on coder une émotion ?... *Vade retro, satanas ! Vade retro !*

L'AUTEUR

Professionnel de la lutte contre la cybercriminalité et de la lutte contre la fraude, Ludovic PETIT est Directeur Cyber Sécurité du Groupe Altran, chercheur associé au Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN), membre de la Réserve Citoyenne Cyberdéfense et Auditeur du Centre des Hautes Etudes du Cyberspace (CHECy).

Références

Projet de rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique :

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-582.443+01+DOC+PDF+V0//FR>

« Est-ce que l'Intelligence Artificielle va sauver ou tuer le genre humain ? »

<http://www.bbc.com/news/technology-37713629>

« L'Intelligence Artificielle pourrait être la pire chose pour l'humanité »

<http://www.bbc.com/news/technology-37713629>

Les humains ont besoin de nouvelles compétences pour le monde post-Intelligence Artificielle

<http://www.bbc.com/news/technology-37618579>

Robot, définition Larousse

Appareil automatique capable de manipuler des objets ou d'exécuter des opérations selon un programme fixe, modifiable ou adaptable.

<http://www.larousse.fr/dictionnaires/francais/robot/69647>

Autonomie, définition Larousse

Capacité de quelqu'un à être autonome, à ne pas être dépendant d'autrui ; caractère de quelque chose qui fonctionne ou évolue indépendamment d'autre chose.

<http://www.larousse.fr/dictionnaires/francais/autonomie/6779>

Hawking ou Montesquieu

À qui se fier pour encadrer les systèmes d'armes létaux autonomes

par **DIDIER DANET**

M

Mi-décembre 2016, après deux années de travaux, la cinquième conférence chargée de l'examen de la Convention sur certaines armes conventionnelles (CCW) se prononçait en faveur de la création d'un groupe d'experts gouvernementaux chargés d'étudier la question des Systèmes d'armes létaux autonomes (SALA). La CCW traitant des armes inhumaines, il n'était pas illogique qu'elle soit appelée à se pencher sur des systèmes militaires présentés par leurs adversaires comme capables d'identifier une cible et de prendre la décision de la détruire sans

aucune autre forme d'intervention humaine.

L'initiative des travaux menés à Genève revient en très large part à des organisations non gouvernementales

(1) HRW, *Losing Humanity. The Case Against Killer Robots*, 2012, <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>

(2) <http://www.article36.org/issue/autonomous-weapons/>.

(3) Interview à la BBC ; « The development of full artificial intelligence could spell the end of the human race. », 2 décembre 2014, <http://www.bbc.com/news/technology-30290540>.

(4) Pour le texte de la lettre ouverte : <https://futureoflife.org/open-letter-autonomous-weapons/>.

comme *Human Rights Watch*¹ ou Article 36² qui anime la *Campaign to Stop Killer Robots*. Parmi les figures tutélaires de cette campagne se trouve notamment Stephen Hawking. Dans plusieurs tribunes largement relayées, le célèbre astrophysicien met

en garde l'humanité contre les dérives possibles de l'intelligence artificielle³ et il est l'un des premiers signataires de la lettre ouverte du *Future of Life Institute* préconisant l'interdiction des *Killer Robots*⁴. Le débat est-il alors clos par cet argument d'autorité ? Peut-être pas car, à l'éminent patronage du membre à vie de l'Académie pontificale des Sciences et à l'interdiction qu'il promeut,

DIDIER DANET

Pôle « Mutations de la
Conflicthabilité »
Centre de recherche des
écoles de Saint-Cyr
Coëtquidan



L'utilisation de "Robots qui tuent" s'est récemment étendue aux services de police, à Dallas.

il est possible d'opposer une figure non moins prestigieuse, Montesquieu pour qui, s'il arrive qu'il faille changer la loi, « *il n'y faut toucher que d'une main*

(5) Montesquieu, Lettres persannes, Lettre 79, Usbeck à Rhédi, à Venise.

(6) Montesquieu, De l'esprit des Lois, Chapitre XVI.

tremblante »⁵. Or, les promoteurs de l'interdiction des « Killer Robots » ne semblent pas avoir

entendu l'avertissement de l'auteur de "De l'esprit des Lois" : « *Comme les lois inutiles affaiblissent les lois nécessaires, celles qu'on peut éluder affaiblissent la législation.* »⁶ En l'espèce, c'est bien à une loi inutile qu'il nous est proposé de souscrire, une loi qui est en particulier incapable de définir son objet et ses limites.

Une loi inutile : les "Robots qui tuent" sont déjà encadrés par le droit

Les "Robots qui tuent" existent. Non pas dans le sens de systèmes d'armes autonomes où l'entendent les ONG prohibitionnistes mais dans celui où les forces armées de nombreux pays disposent déjà depuis longtemps de robots susceptibles d'être armés et de délivrer des effets cinétiques pouvant être mortels. Les États-Unis recourent ainsi régulièrement à des frappes de drones pour éliminer les membres des organisations combattantes irrégulières auxquelles ils sont confrontés dans leurs opérations extérieures. L'utilisation de "Robots qui tuent" n'est même plus seulement l'apanage des forces armées américaines. Elle s'est récemment étendue aux services de police qui, à Dallas par exemple, ont recouru à un robot télécommandé *Northrop Grumman Remotec Andros* pour abattre le forcené qui avait tué cinq policiers et deux civils le 8 juillet 2016.⁷

Ces robots armés, qui sont déjà en service et qui n'ont rien d'autonome, relèvent de deux grandes catégories.

Les uns sont télé-opérés. C'est le cas des *Reapers* américains. Ils sont pilotés à distance par un équipage placé sous la responsabilité d'une chaîne de commandement qui prend les décisions les plus importantes, comme le ciblage et le tir. La seule différence entre ces robots

télé-opérés et les avions traditionnels réside dans le déport de l'élément humain qui n'est plus en contact direct avec le champ de bataille. Mais, cet éloignement n'implique aucune différence de nature entre les deux systèmes et le cadre juridique actuel, applicable à l'un est applicable à l'autre.

D'autres robots militaires relèvent d'une deuxième catégorie. Ils sont automatisés au sens où certaines de leurs fonctions sont réalisées par des calculateurs permettant de libérer l'opérateur d'une partie du processus d'information préalable à la prise de décision ou de mise en œuvre de cette décision. Ainsi, le système robotisé antimissiles qui équipe certains navires ouvre le feu sur les objets présentant les caractéristiques d'un missile antinavire beaucoup plus rapidement que ne pourrait le faire un opérateur humain. Mais, de la définition des caractéristiques permettant d'identifier un missile antinavire à la décision d'activer le dispositif de protection ou à l'interruption du programme, rien n'est laissé à la libre appréciation de la machine. Celle-ci exécute un ensemble d'instructions qui sont implantées dans son système.

Dans les deux cas, il est impossible de parler d'autonomie ou même de systèmes précurseurs de l'autonomie des robots. L'homme reste dans la boucle par l'action directe qu'il exerce sur le système d'armes (télé-opération) ou par le fait qu'il

a conçu les séquences d'actions réalisées par la machine et qu'il en contrôle le déploiement et la mise en œuvre (automatisation). Le ciblage et le tir restent le monopole de la chaîne de commandement qui en assume la responsabilité politique et juridique comme le montre le cas du président américain dont l'approbation est indispensable à la réalisation d'une opération d'assassinat ciblé.

Dès lors, ces robots militaires, dont certains peuvent délivrer des effets mortels, ne posent pas de difficulté de principe quant à l'application du Droit pénal interne ou du Droit international humanitaire. Ce qui est, par exemple, en cause dans l'utilisation des drones par les États-Unis pour les besoins de leurs opérations en Afghanistan ou en Irak, voire au Pakistan ou en Somalie, n'est pas le drone en lui-même mais le contexte dans lequel il est employé pour des assassinats ciblés : les États-Unis sont-ils en situation de légitime défense ? Portent-ils atteinte à la souveraineté de pays qui ne sont pas partie au conflit ? L'action entreprise méconnaît-elle les principes de proportionnalité et de distinction ? Rien ici ne permet de dire que de nouvelles règles portant précisément sur les robots militaires sont nécessaires. Ces robots sont déjà encadrés par le droit applicable à tous les systèmes d'armes. La question n'est d'ailleurs pas posée puisque les systèmes



Les experts craignent que la différence entre l'intelligence humaine et l'intelligence artificielle entraîne une suprématie de cette dernière.

d'armes existants (télé-opérés et automatisés) sont expressément exclus du champ d'étude de la CCW.

Faut-il interdire les Killer Robots ?

Si l'on estime utile de réfléchir à un cadre juridique visant un type de machine qui n'existe pas et dont l'hypothétique avènement semble lié à des extrapolations pour le moins aventureuses, la proposition des ONG

prohibitionnistes répond-elle à l'impératif prudentiel proposé par Montesquieu ? Dans un domaine porteur d'enjeux scientifiques, politiques, économiques, juridiques... aussi essentiels, il semblerait effectivement important que les différentes parties prenantes, pouvoirs publics, forces armées, industrie de la Défense et ONG elles-mêmes, sachent ce qui est autorisé et ce qui ne l'est pas. Or,

le moins que l'on puisse dire est qu'il n'en est rien pour le moment. Aucune définition claire n'émerge quant à l'objet même de l'interdiction. Plusieurs propositions sont en concurrence parmi les contempteurs des *Killer Robots*.

Selon l'ONG « Article 36 », l'autonomie se reconnaît à la réunion de trois conditions cumulatives : une capacité à agir en

(8) The term 'autonomous' is used by engineers to designate systems (such as a self-driving car) that can operate without direct human control or supervision in dynamic, unstructured, open environments based on feedback information from a variety of sensors. », Article 36, « Structuring Debate on Autonomous Weapons », <http://www.article36.org/wp-content/uploads/2013/11/Autonomous-weapons-memo-for-CCW.pdf>.

l'absence de contrôle direct ou de supervision humaine, une aptitude à opérer dans un environnement non structuré, une certaine variété de senseurs.⁸ Sans doute conscients du

fait que des critères comme la non-structuration de l'environnement ou la variété des senseurs n'auraient aucune consistance juridique et rendraient l'interdiction inopérante, les responsables de la campagne concentrent la définition de l'autonomie sur la seule notion de contrôle humain. Serait autonome un système d'armes létal qui opère *beyond*

*meaningful control*⁹.

(9) "Deploying AWS that operate outside of meaningful human control is neither ethically nor legally acceptable.", *ibidem*.

Le problème n'est pas résolu pour autant puisque,

comme l'ont souligné certains Etats pourtant favorables à la création du Groupe d'experts gouvernementaux, la notion de contrôle significatif n'a pas de

sens et peut aussi bien s'appliquer aux systèmes télé-opérés ou automatisés, ce qui reviendrait à amalgamer tous les systèmes d'armes existants ou non et à élargir le champ des discussions très au-delà de ce qui a été convenu. Stephen Hawking et les signataires de la lettre ouverte du *Future of Life Institute* adoptent également le critère inconstant du *meaningful control*. Ils lui en ajoutent un second qui n'est pas moins problématique et qui tient à la finalité du système d'armes. Ne seraient interdits que les systèmes autonomes à vocation offensive tandis que seraient autorisés les systèmes à vocation défensive. « *Starting a military AI arms race is a bad idea, and should be prevented by a ban on*

(10) <https://futureoflife.org/open-letter-autonomous-weapons/>.

offensive autonomous weapons beyond meaningful human control. »¹⁰

(11) On rappellera sur ce point la définition proposée par la France et qui tient en trois points : « un vecteur capable de se déplacer librement dans un environnement terrestre, aérien ou marin qui n'est pas entièrement connu d'avance, de réaliser le ciblage et le tir d'un effecteur létal (balle, missile, bombe) en autonomie totale de fonctionnement (« Human out of the Loop »), c'est à dire sans la moindre intervention ou validation humaine (« Human in the Loop ») ou supervision (« Human on the Loop »).

Ces propositions sont de véritables nids à contentieux et ils révèlent une incapacité profonde à définir l'objet visé par la demande d'interdiction.¹¹

La chose n'est pas pour surprendre tant la revendication

prohibitionniste s'alimente à deux visions opposées du futur de l'intelligence artificielle.

Les spécialistes rassemblés derrière Stephen Hawking craignent au fond que l'homme ne soit dépassé par sa créature. Evoluant trop lentement par rapport aux progrès des intelligences artificielles, il sera rapidement dominé par elles. Placées entre de mauvaises mains, ces machines deviendraient les Kalachnikov du XXI^e siècle et leur intelligence supérieure servirait à des fins d'épuration ethnique, de répression politique ou d'actions terroristes.

A l'inverse, les spécialistes des organisations non gouvernementales semblent plutôt craindre l'imperfection congénitale des machines futures, de sorte qu'elles seraient incapables du discernement que l'on attend d'un soldat sur le champ de bataille. Les progrès scientifiques et techniques seraient trop frustes pour que les systèmes d'armes létaux qu'ils produisent puissent intégrer les principes fondamentaux du Droit international humanitaire. Ainsi, pour *Human Rights Watch*, « *there is no certainty that fully autonomous weapons would have the capacity to make such distinctions reliably. That is especially the case in the increasingly common scenarios of contemporary warfare, in which combatants do not identify themselves by uniforms or insignia. When there are no visible clues in a close*

combat situation, assessing an individual's intentions

(12)

<https://www.hrw.org/news/2013/10/21/qa-fully-autonomous-weapons#4>.

is key to determining a potential target's status and level of threat. »¹²

De deux choses l'une

Soit les progrès de l'intelligence artificielle sont insuffisants pour donner une véritable autonomie aux systèmes d'armes létaux mis en œuvre sur les champs de bataille, ceux-ci demeurent sous contrôle humain. Ils sont téléopérés ou automatisés et ne se distinguent pas des robots militaires existants. Il n'est alors nullement besoin de les soumettre à un régime juridique spécifique puisque ces robots sont déjà encadrés par le Droit. Soit l'intelligence artificielle se développe au point que des machines véritablement autonomes, d'une intelligence supérieure à celle des êtres humains qui composent les forces armées, envahissent les champs de bataille. On ne voit pas alors pourquoi ces machines ne pourraient pas intégrer et apprendre les règles légales et éthiques que l'on inculque aujourd'hui à des combattants humains. Ces systèmes supérieurement intelligents seraient au contraire mieux armés pour faire face au chaos du champ de bataille. Loin d'être un problème, ils seraient la solution aux excès de violence associés à la fatigue, à des erreurs de jugement ou au débordement de sentiments humains comme la peur ou la haine...

L'inconsistance des propositions d'interdiction des *Killer Robots* formulées par les émules de Stephen Hawking montre que si ce dernier est sans doute meilleur astrophysicien que Montesquieu, il est assurément préférable de s'en remettre à l'auteur de "De l'Esprit des Lois" pour l'élaboration du cadre juridique régulant le développement des systèmes d'armes. En proposant un régime d'interdiction pour d'hypothétiques équipements militaires dont il est impossible de définir la nature ou les caractéristiques distinctives, les associations prohibitionnistes enfreignent le principe prudentiel préconisé par Montesquieu et prennent le risque d'introduire la plus grande des confusions dans un dispositif qui s'avère pour l'heure effectif et suffisant. On peut penser que ce n'est pas le meilleur service à rendre aux populations civiles que l'on entend protéger.



Les ruptures technologiques qui s'annoncent amènent une interrogation doctrinale sur la validité des mécanismes de responsabilité et d'indemnisation du droit positif. En effet, l'avènement du tryptique robot/intelligence artificielle/algorithmes interpelle une frange des praticiens du droit sur la nécessité de discuter de l'adoption d'une personnalité électronique juridique. En l'absence de définition juridique en Europe mais aussi en France sur les termes robots et intelligence artificielle, il est utile de rappeler les définitions retenues par l'organisation internationale de normalisation (ISO) :

Robot : ISO 8373 : 2012 « *un mécanisme programmable actionné sur au moins deux axes avec un degré d'autonomie, se déplaçant dans un environnement pour exécuter les tâches prévues* ».

Intelligence artificielle : ISO 2382-28 « *capacité d'une unité fonctionnelle à exécuter des fonctions généralement associées à l'intelligence humaine, telles que le raisonnement et l'apprentissage* ». Sur ce propos, l'étude commanditée par la Commission des affaires juridiques du Parlement européen apporte une base solide de réflexions.

L'introduction à destination du grand public de la voiture à délégation partielle ou totale de conduite, plus communément connue sous le terme de voiture autonome, devrait constituer *a priori* un des premiers vecteurs d'approche *in concreto* des consommateurs dans leur processus d'acculturation des robots et de l'intelligence artificielle.

Robot or not robot ?

petite digression juridico-philosophique

par OLIVIER DE MAISON ROUGE

À

À l'occasion du FIC 2017, Octave KLABA, fondateur d'OVH, déclarait à La Voix du Nord, qu'à la vitesse où la transition numérique s'impose aux acteurs économiques, c'est tout un modèle sociétal qui chavire, un changement de paradigme socio-économique. « *Quand on a l'intelligence artificielle et qu'on a plus besoin des gens, qu'est-ce qu'on fait des gens ?* »¹. C'est en substance la même question qu'il est convenu de se poser à l'ère de la robotique, de surcroît numérique.



OLIVIER DE MAISON ROUGE

Avocat – Docteur en droit
Vice-président de la
Fédération européenne
des experts en
cybersécurité (EFCSE)

Ce dilemme n'a en réalité rien de nouveau car les révolutions industrielles successives - la dernière en date étant une mutation digitale – ont toujours fait jaillir de

grandes interrogations sur l'avenir de l'homme dans le nouvel environnement technologique qu'il a conduit à façonner.

(1) « le sens de la vie va être remis en cause, qu'on le veuille ou pas », in La Voix du Nord, 25 janvier 2017.

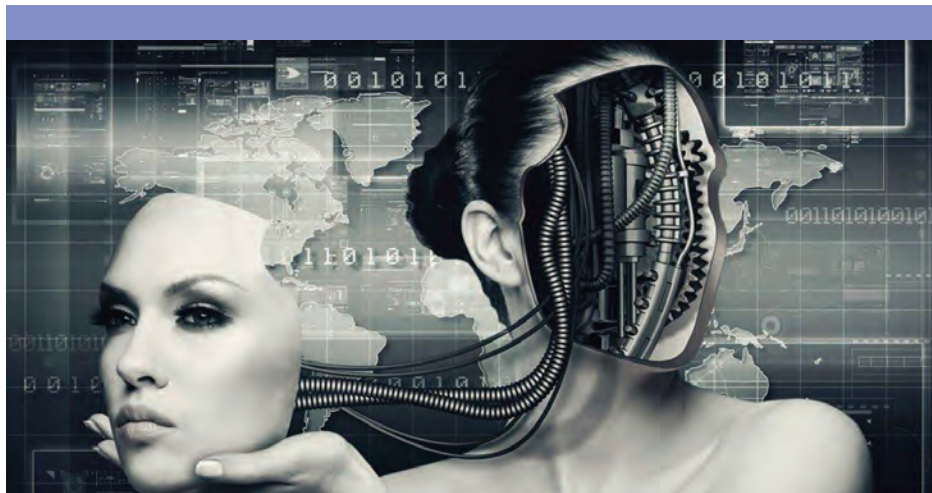
(2) Un syndrome Frankenstein ?

La cybernétique fait naître autant de grands espoirs qu'elle terrifie².

En l'occurrence, il s'agit de s'interroger sur la place de l'homme dans sa relation aux robots, et peut-être plus précisément face à l'intelligence artificielle qui les anime. À ce jour, le droit n'a pas encore pris toute la dimension de ce défi, mais rien n'interdit à ce stade d'intégrer quelques considérations devant présider à l'élaboration d'un droit du robot que certains imaginent déjà.

Du robot substitution à l'Homo laborans ...

Sous cette approche, objet des craintes voire des querelles entre anciens et modernes, le robot est davantage perçu comme une alternative à la souffrance de



« La machine est devenue dans les tâches quotidiennes le substitut de l'homme, sans toutefois en être son égal. »

l'homme au travail. Ce fut la voie empruntée jusqu'à présent. Depuis lors, nous en voyons et croisons quasiment chaque jour, que ce soit l'automate qui a remplacé le caissier du péage ou du parking, la borne d'information à La Poste ou dans la gare... La machine est devenue dans les tâches quotidiennes le substitut de l'homme, sans toutefois en être son égal.

Le docteur Humbert rappelle que la robotique vient du tchèque « *robota* » qui veut dire travail et qu'elle est censée soulager l'homme de certaines tâches pénibles. Ce faisant, le robot est synonyme de progrès humain, en ce qu'il décharge l'homme du *labor* et de sa pénibilité. Avec cette avancée significative, on s'écarte d'autant de la pensée de Voltaire pour qui « *le travail éloigne de nous trois grands maux :*

l'ennui, le vice, le besoin ». En vérité, la question est loin d'être nouvelle et/ou actuelle dès lors qu'elle agitait déjà les penseurs et théoriciens du travail dans les années 1930, à l'heure de la mécanisation des tâches industrielles.

La question de la place de l'homme face à la machine était déjà débattue et s'était déplacée dans les années 1970 sur le terrain du coût du travail. Cependant, si la machine affranchit l'homme, elle est également perçue comme étant destructrice d'emplois. Or, moins d'emplois rémunérés signifient moins de cotisations sociales à percevoir et donc un déficit de financement des caisses destinées à financer la protection sociale : retraite, maladie... c'est d'ailleurs la raison pour laquelle le candidat Benoît Hamon prônait une cotisation « sociale » pour les robots.

Mais c'est peut-être s'affranchir un peu trop rapidement de la loi de Lavoisier pour qui « *rien ne se crée, rien ne se perd, tout se transforme* », à l'image de la révolution digitale actuelle, où les emplois de demain naissent avec les nouvelles technologies au détriment des emplois d'hier (le WC automatique a fait passer à trépas la dame pipi). La nouvelle économie n'est pas malthusienne. Les métiers de l'innovation que nous côtoyons tous les jours en sont la démonstration. Combien

(3) Et les statistiques allemandes montrent qu'en dépit d'un taux élevé de robotisation de l'industrie, le chômage est faible.

d'activités nouvelles sont nées en moins d'une décennie³ ?

Mais à ce stade de la réflexion, il n'est pas encore question d'autonomie du robot, qui demeure à l'état de machine-outil, lointaine descendante des premières inventions de la révolution industrielle. La mécanique, fruit de l'activité inventive de l'homme, est destinée à l'économiser physiquement et à générer un gain économique, qui permet de réduire à due concurrence un coût social pour l'entreprise, ce d'autant plus que le robot n'est pas contestataire. Il devient donc doublement créateur de richesse, dès lors qu'il est moins onéreux que le coût du travail de l'homme, et qu'il présente une meilleure rentabilité industrielle (ajouté à l'amortissement fiscal exceptionnel⁴).

(4) Article 39 AH du Code général des impôts

Ainsi présenté, le robot se pare de toutes les vertus.

... au robot doté d'une personnalité juridique ?

Ainsi que le montre la plupart des auteurs, ce n'est désormais plus tant la place du robot dans notre société qui questionne, que le degré d'autonomie de ce dernier, et accessoirement la place de l'*homo faber* (générateur du robot).

Avec le développement de la cybernétique associée aux mathématiques algorithmiques, l'intelligence artificielle s'est trouvée un corps-réceptacle en s'incarnant dans la machine. Fort de cette transmutation le robot s'est éloigné de la machine-outil servile pour gagner son indépendance morphologique. Dans son langage poétique, l'administration fiscale le définit alors comme « *un manipulateur multi applications reprogrammable commandé automatiquement* ».

Cette notion d'autonomie (sans la volonté ?) s'incarne dans le fait que le robot, fruit d'un programme, doit pouvoir, indépendamment de l'intervention de l'homme, réagir en fonction de situations données. Ce processus d'autonomie de la machine est plus ou moins prégnant selon le type de robot. Plus exactement, en fonction du quotient d'intelligence artificielle (QIA) dont il est doté, le robot acquiert son autonomie d'action. *In fine*, on ne distingue plus le génie de l'homme créateur (ou *homo faber*) de la propre indépendance intellectuelle du robot.

Comme dans l'antique complexe œdipien l'intelligence artificielle en est-elle venue à tuer le père (son programmeur) ou à tout le moins le dépasser ?

Cela conduit naturellement à s'interroger sur la nature même du robot, de sa personnalité, de sa responsabilité : on

(5) I.A., I, Robot ou Minority report ont vu court.

plonge alors en pleine science

juridique fiction⁵.

Car, pour pousser un peu, peut-on imaginer un robot qui échapperait à toute tutelle, qu'elle soit celle de son programmeur-géniteur ou celle de son propriétaire-utilisateur, et lui conférer une autonomie juridique ? Certains ont allègrement franchi cet horizon en invoquant une « *personnalité juridique du*

(6) Projet de rapport du Parlement européen 2015/2103 (INL) § 31 ff.

robot »⁶ pour « *qu'au moins les robots autonomes les plus*

sophistiqués puissent être considérés comme des personnes électroniques dotées de droits et de devoirs précis y compris celui de réparer tout dommage causé à un tiers ». Le robot étant appréhendé comme étant « *une personne électronique qui prend des décisions autonomes de manière intelligente ou qui interagit de manière indépendante avec des tiers* ».

Mieux que l'animal, qui est simplement

(7) Loi du 16 février 2015.

doué de sensibilité⁷, le robot devient l'égal de l'homme et peut-être son avenir,

(8) Jean Ferrat.

(9) Article 1240 du Code civil.

(10) Article 1242 du Code civil.

supplantant la femme (selon le poète⁸). L'androïde devient dès lors un être sensible.

En matière de responsabilité, le robot autonome répondra de ses actes, non comme étant sous la garde, le contrôle et la direction de l'homme⁹, ni au titre de la responsabilité du fait des choses¹⁰, mais distinctement. Il s'agirait d'une responsabilité propre, ici encore autonome, à tout le moins limitée pour son créateur et/ou utilisateur.

Pour conclure provisoirement cette digression, laissons le dernier mot ici encore à celui qui pense bien souvent pour les autres, à savoir le philosophe : « *Attribuer une responsabilité à un robot, créer un régime d'assurance propre implique une sorte de personnalisation, une humanisation du robot, qui déresponsabilise l'humain qui le fabrique ou l'utilise. (...) L'expérience est risquée, elle atténue toujours plus la distinction entre l'homme et la machine dans une vision transhumaniste qui relève de l'idéologie.* »¹¹

Sur www.genethique.org.

Quelle responsabilité pour les robots ?

Quelle responsabilité pour l'Homme ?

par **FABRICE LORVO**

L

Les robots sont présents dans nos vies, depuis des décennies. La révolution numérique réactive notre intérêt pour eux dès lors que certains sont devenus autonomes, c'est-à-dire qu'ils ont la capacité de prendre des décisions et de les mettre en pratique dans le monde extérieur, indépendamment de tout contrôle ou influence extérieurs (il s'agit notamment des voitures autonomes, des drones, des robots médicaux, etc.).

Le marché des robots autonomes est porteur. Il est en forte progression (de 17 % par an entre 2010 et 2014 et + 29 % en 2014).

Dans ces conditions, les interactions entre les êtres humains et les robots autonomes seront de plus en

plus nombreuses. Certaines de ces interactions pourront être dommageables pour l'être humain. Il convient donc d'envisager la question de la responsabilité juridique des robots mais aussi, celle de l'Homme vis-à-vis de l'intelligence artificielle (qui est en quelque sorte, le cœur des robots).

Quelle responsabilité pour les robots ?

Vers une responsabilité du robot ?

Le premier constat est que notre droit n'est peut-être pas forcément adapté pour appréhender les conséquences du fait d'un robot (que ce fait soit fautif ou non). Notre droit reconnaît la responsabilité d'un individu pour son fait personnel ou pour un fait commis par une autre personne (enfant, employé, etc.) ou un animal. Il reconnaît aussi la responsabilité du fait des choses (mobilières ou immobilières). Le caractère autonome du robot ne permet pas de le



FABRICE LORVO

Avocat

classer dans la catégorie de la chose et il ne permet pas, non plus, de le rattacher à la catégorie des humains. L'adoption d'une législation dédiée aux robots s'impose.

(1) PROPOSITION DE
RÉSOLUTION DU
PARLEMENT EUROPÉEN
contenant des
recommandations à la
Commission concernant des
règles de droit civil sur la
robotique (2015/2103(INL))

En janvier 2017¹, la commission des affaires juridiques, sur la base d'un rapport (DELVAUX), a fait des

recommandations concernant l'adoption de règles de droit civil sur la robotique. Ce rapport invite la Commission Européenne à proposer des instruments (soit législatifs, soit des lignes directrices ou des codes de conduite) sur les aspects juridiques du développement et de l'utilisation de la robotique et de l'intelligence artificielle à un horizon de 10 à 15 ans.

Sur la responsabilité du propriétaire ou de l'utilisateur des robots

Dans l'attente d'une législation propre à la responsabilité des robots autonomes, et même si le fait du robot est reconnu, une responsabilité « robotelle » (néologisme créé à partir de responsabilité individuelle) ne nous mènerait pas loin car derrière la responsabilité, il y a la question de l'indemnisation de la victime et pour le moment, les robots n'ont pas encore de patrimoine.

Il conviendra probablement de résoudre l'indemnisation de la victime par l'obligation d'assurance du robot, obligation qui pèserait sur le propriétaire

et/ou l'utilisateur du robot. Une fois la victime indemnisée, la question de l'imputation de la responsabilité restera ouverte. Elle donnera lieu à toute une série de recours subrogatoires afin de déterminer qui est le responsable du dysfonctionnement du robot.

Du fait de la chaîne des intervenants pour la conception et l'entretien des robots, on peut facilement imaginer que les juristes auront de beaux jours devant eux pour déterminer les responsabilités en cas de dysfonctionnement d'un robot, sous réserve que l'on puisse établir la chaîne de commande qui a causé le dommage.

À cette fin, il conviendra de prévoir ou d'imposer que chaque robot autonome soit équipé d'une boîte noire enregistrant l'intégralité des données correspondant à ses agissements, y compris la logique qui a abouti à sa prise de décision.

Quelle est notre responsabilité vis-à-vis de l'intelligence artificielle ?

Outre celle de la sécurité, la place grandissante des robots dans nos sociétés pose de nombreuses questions au niveau économique et social (quel sera l'impact de la substitution du travail de l'homme par celui du robot sur le chômage ? Quelle sera la viabilité des régimes de sécurité sociale ?). D'autres questions plus structurelles ne doivent pas être ignorées.

La téléologie des robots

Depuis des siècles, l'être humain est le plus grand des prédateurs et n'a pas de

rival. Il n'est pas exclu qu'un jour, l'intelligence artificielle puisse remettre en question la suprématie ou l'existence de l'humanité. Sans vouloir jouer les Cassandra, on peut raisonnablement considérer que l'intelligence artificielle arrivera à son paroxysme d'évolution lorsqu'elle remettra en cause le postulat selon lequel elle est au service de l'Homme, lui-même, centre de l'univers.

À un degré moindre, l'intelligence artificielle sans contrôle peut donner lieu à de surprenants résultats. En 2016, Microsoft a développé un robot conversationnel (chatbot) appelé Tay qui participait à des conversations sur des réseaux sociaux (notamment Twitter ou Snapchat). Tay a envoyé 96000 tweets en 8 heures et il devait devenir de plus en plus intelligent au fur et à mesure des conversations. L'expérience a dû être arrêtée car Tay a fini par tenir des propos vulgaires ou racistes notamment parce que des internautes lui ont demandé de les répéter.

(2) Programme de recherche en intelligence artificielle de Google

En 2016, Google Brain² a fait communiquer deux intelligences artificielles entre elles. Ces deux ordinateurs ont rapidement sécurisé leurs communications par le biais d'un chiffrement qu'ils avaient eux-mêmes développé et qui n'a pas pu être déchiffré par l'Homme.

Le premier enseignement est donc que l'Homme doit concevoir les robots avec la possibilité d'exercer, à tout moment, un

contrôle humain. Un interrupteur doit être prévu, accessible et sécurisé. De plus, les domaines d'intervention des robots peuvent être de nature à créer des conséquences invisibles pour l'humanité. Par exemple, dans des établissements de santé les actes et la présence de l'homme peuvent être remplacés par les soins ou la compagnie de robots. Il est donc possible qu'une relation émotionnelle se développe entre l'homme et le robot, notamment chez les personnes vulnérables (personnes âgées, personnes handicapées, enfants). De surcroît, si l'altérité, est un élément essentiel de la condition humaine, quelles seront les conséquences d'une relation avec l'intelligence artificielle ? Ces situations doivent être anticipées ou étudiées.

Imposer l'éthique by design dans la conception des robots ?

La création d'un cadre juridique ne pourra se faire sans la définition d'un cadre éthique relatif au développement, la conception, la fabrication, l'utilisation et la modification des robots. Le rapport DELVAUX a proposé une charte établissant un code de conduite pour les ingénieurs en robotique, une déontologie pour les comités d'éthique de la recherche lorsqu'ils examinent les protocoles de robotique, et un ensemble de licences-types pour les concepteurs et les utilisateurs.

Pour prendre la mesure de cette nécessité, raisonnons par analogie avec

la voiture autonome (voiture qui fonctionne sans intervention d'un être humain). Doit-on laisser à l'intelligence artificielle la possibilité de violer le Code de la route ? Une telle violation pourrait cependant être salutaire si, pour éviter un accident, une voiture dépassait une vitesse limite autorisée, ou franchissait une ligne continue. Si deux voitures vont se percuter de plein front, laquelle doit se jeter dans le fossé ? Doit-on prendre en compte l'âge des passagers ? Leur nombre ? Leur rang social ? Autant d'informations qui seront probablement, avec le Big Data, à la disposition de l'intelligence artificielle.

On comprend clairement pour le cas de la voiture autonome que l'on va transférer à des algorithmes, des décisions à prendre qui engagent l'humanité. Qui va prendre l'initiative et la responsabilité de les paramétrer ? Jusqu'à ce jour, lorsque deux voitures fonçaient l'une sur l'autre, il y avait autant de solutions possibles que de chauffeurs concernés. Aujourd'hui, l'homme va probablement être dépossédé de ce choix ou plutôt, quelqu'un d'autre aura choisi pour lui dans ce type de situations extrêmes, sauf à convenir que le passager de la voiture autonome pourra reprendre, à cette occasion, le contrôle de ladite voiture (qui ne serait donc que partiellement autonome).

Admettons que l'on doive fixer et donc hiérarchiser ces choix. En transférant à l'intelligence artificielle, la prise de décision concernant l'être humain, on limite les possibilités de choix et on les

classifie. Tout ce qui touche à la norme humaine, et notamment les normes du comportement humain idéal ou du comportement social moyen, devrait faire l'objet d'une discussion ou d'une validation préalable obligatoire sous un angle éthique.

Il a été créé un Comité consultatif national d'éthique (CCNE) pour les sciences de la vie et de la santé. Aujourd'hui, les mêmes types de question se posent dans le domaine numérique, notamment pour les algorithmes prédictifs. Étant donné la vitesse d'évolution du monde numérique, il est urgent de légiférer rapidement et d'imposer la consultation et la possibilité d'un contrôle d'un organe éthique (notamment en le créant ou en étendant la mission de la CCNE ou de la CNIL) sur toutes les questions de nature à faire disparaître l'aléa dans les décisions d'un algorithme pouvant affecter un être humain.

(3) LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique modifiant la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(4) Rapport CNIL, bilan d'activité 2016 page 102.

Rappelons que la loi³ a confié à la CNIL la mission de conduire une réflexion sur les problèmes éthiques et les questions de société soulevés par

l'évolution des technologies numériques. Dès janvier 2017, la CNIL a lancé un cycle de réflexion⁴.

À ce sujet, le CREOGN apportera sa contribution en organisant à la rentrée 2017, un atelier de recherche dont le thème portera sur les enjeux éthiques et juridiques des algorithmes prédictifs.

Voiture autonome :

quel droit pour les forces de l'ordre ?

par **DIDIER GAZAGNE**

D

D'après de récentes études publiées, le marché des véhicules autonomes représenterait entre 3 et 8 millions de voitures autonomes qui pourraient être commercialisées à l'horizon 2030 en Europe.

L'Allemagne envisage déjà en Europe l'interdiction totale de la voiture thermique d'ici 2030. Cette situation pourrait bien être une réalité en Europe pour d'autres États européens et pourquoi pas en France ou sur d'autres continents d'ici 2030.



DIDIER GAZAGNE

Avocat
Vice-Président de
l'Association du Droit des
robots (ADDR)
Président de la
Commission Usine 4.0
(ADDR)

Compte tenu du gisement des données produites par une voiture autonome, sous réserve de la disponibilité et de l'accès depuis leurs tablettes numériques, les

forces de l'ordre pourraient bien disposer demain de toutes les informations concernant le propriétaire du véhicule autonome à contrôler, ses occupants et ses caractéristiques, et seraient donc en mesure de vous identifier où que vous alliez et où que vous soyez sur l'espace public ou privé.

Essayez d'imaginer que les forces de

(1) Les forces sur le terrain pourraient aussi être représentées par un robot-policier ou robot-gendarme tel que les robots Atlas ou AnBot

l'ordre¹ aient pour mission de vous contrôler dans votre voiture autonome sur

un espace public. Nous sommes en 2020 ou en 2030, les voitures thermiques ont totalement disparu, les autorités européennes ayant pris la décision d'interdire désormais la circulation publique de toutes voitures thermiques.

Avant d'appréhender le cadre juridique existant et d'identifier s'il convient de le faire évoluer pour le rendre adéquat et approprié pour permettre aux forces de

l'ordre d'intervenir directement sur un véhicule autonome, tout en assurant la protection des droits fondamentaux, répondre à cette question qui introduit cet article implique de définir préalablement ce qu'est un véhicule autonome.

Quelle définition de la voiture autonome ?

La définition de la voiture autonome questionne tout d'abord le concept d'autonomie et plus précisément le degré d'autonomie dont dispose le véhicule lorsqu'il se déplace et se dirige dans un environnement public ou privé. Première difficulté, il existe de nombreuses nomenclatures pour définir les différents degrés d'autonomie d'un véhicule autonome. La comparaison de différentes nomenclatures permet de constater qu'il n'existe pas réellement de définition unique et partagée pour définir une voiture autonome et plus généralement un véhicule autonome.

Le concept d'autonomie appliqué au véhicule

Plusieurs nomenclatures définissent et catégorisent les différents degrés d'automatisation des véhicules. Les principales sont les suivantes :

(2) http://bast.opus.hbz-nrw.de/volltexte/2013/723/pdf/Legal_consequences_of_an_increase_in_vehicle_automation.pdf

– la nomenclature BAST² de l'organisme technique fédéral allemand (*Bundesanstalt für*

Straßenwesen) ;

(3) <http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development>

(4) http://www.sae.org/misc/pdfs/automated_driving.pdf

(5) Plan Nouvelle France Industrielle, Feuille de route d'usages du véhicule autonome particulier, 16-7-2015 <http://www.pfa-auto.fr/wp-content/uploads/2016/03/Objectifs-de-recherche-Vehicule-Autonne.pdf>

– la nomenclature NHTSA³ de l'administration de la sécurité routière aux États-Unis (*National Highway Traffic Safety Administration*) ;

– les travaux de pré-normalisation de l'organisme SAE International⁴, situé aux États-Unis,

(anciennement *Society of Automotive Engineers*) ;

– la nomenclature du Plan industriel véhicule autonome en France⁵.

La nomenclature SAE, semble être la plus partagée par les constructeurs automobiles et équipementiers, mais également par la communauté scientifique en Europe. Elle prévoit cinq niveaux d'automatisation.

Les voitures auxquelles nous consacrons cette analyse sont celles qui relèvent du niveau 5 sur la nomenclature du consortium SAE.

Les technologies de la voiture autonome

La conception d'un véhicule autonome implique une interaction entre de nombreuses technologies permettant au véhicule autonome de fonctionner sur la voie publique sans l'intervention d'un conducteur humain.

Les composants élémentaires des technologies embarquées dans la voiture autonome comprennent :

- l'interface homme-véhicule (interface homme-machine au sens général du terme) ;
- les capteurs fournissant des données sur le fonctionnement interne du véhicule et de ses parties : tels que les freins, la transmission, la direction, l'accélérateur, les pneus, etc. ;
- les capteurs qui fournissent l'emplacement en temps réel et l'environnement de la chaussée extérieure donnée ;
- les actionneurs qui, à l'inverse des capteurs, désignent les organes de la voiture qui engendrent un phénomène physique : freinage, accélération, évitement... ;
- les systèmes embarqués de commande qui permettent au véhicule autonome de prendre des décisions et d'envoyer des ordres aux actionneurs à partir des informations fournies par les capteurs.

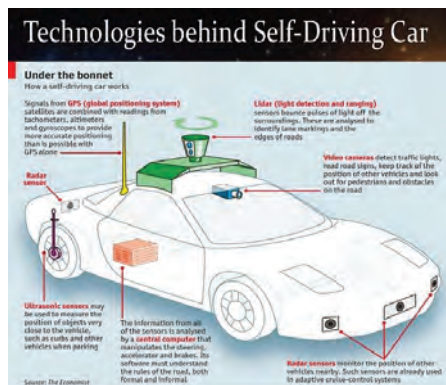
2 juillet 2014			
Niveau 0 : Pas d'automatisation	Conducteur uniquement	Niveau 0 : Pas d'automatisation	Niveau 0 : Pas d'automatisation
Niveau 1 : Assistance à la conduite	Conducteur uniquement	Niveau 1 : Automatisation de fonctions spécifiques	Niveau 1 : Assisté
Niveau 1 : Assistance à la conduite	Automatisation partielle	Niveau 2 : Automatisation des fonctions combinées	Niveau 2 : Automatisation partielle
Niveau 3 : Automatisation conditionnelle	Automatisation partielle	Niveau 3 : Conduite automatisée limitée	Niveau 3 : Automatisation conditionnelle
Niveau 4 : Automatisation élevée	Automatisation totale	3/4 (Niveau 4 : Conduite automatisée totale)	Niveau 4 : Automatisation haute
Niveau 5 : Automatisation totale	-	3/4 (Niveau 4 : Conduite automatisée totale)	Niveau 5 : Automatisation complète

Nomenclature SAE.

Les 4 schémas ci-après illustrent respectivement :

Schémas 1 et 2 : le positionnement des différents capteurs sur un véhicule autonome ;

Schémas 3 et 4 : le rôle des différents capteurs sur un véhicule autonome et la surface ou l'environnement de collecte des données.



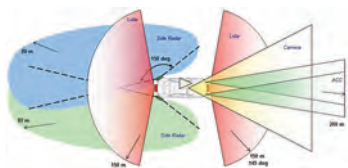
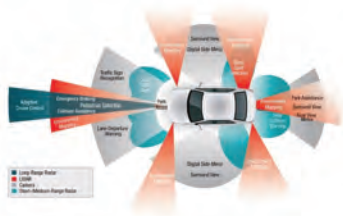
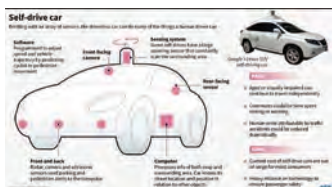
d'intelligence artificielle Watson conçu par IBM ne sert pas à piloter le véhicule mais permet à celui-ci de devenir intelligent, sensible et capable de comprendre les interactions linguistiques.

Il peut notamment comprendre et répondre à des questions formulées en langage courant concernant une destination, le fonctionnement du véhicule ainsi qu'ajuster en permanence sa trajectoire en fonction des préférences des passagers, des informations locales ou à partir des plus de 30 capteurs embarqués dans le véhicule.

La voiture autonome est également dotée d'applications ou de dispositifs mobiles : smartphone, appareil Bluetooth, GPS...

À terme, le véhicule autonome aura besoin de capter, analyser, comprendre son environnement en permanence, devenant pour cela une véritable centrale de traitement de données.

Longtemps confinées à l'intérieur de l'habitacle, les données du véhicule se sont en quelques années connectées à des éléments extérieurs, par des systèmes embarqués maîtrisés par les constructeurs, par des systèmes ajoutés (par exemple des GPS), ou encore par le truchement du smartphone (et d'applications mobiles liées à la conduite).



Véhicule autonome et IA

Très récemment, le 16 juin 2016, les sociétés Local Motors et IBM ont

(6) IBM : Local Motors Debuts "Olli", the First Self-driving Vehicle to Tap the Power of IBM Watson
<http://www-03.ibm.com/press/us/en/pressrelease/49957.wss>

présenté Olli⁶, le premier véhicule de transport autonome intégrant de l'intelligence

artificielle, déjà mis en service à Washington. Le programme informatique

Typologie des voitures autonomes et flux de communication

(7) Dorothy J. Glancy, Symposium, Privacy in Autonomous Vehicles, 52 Santa Clara L. Rev. 1171 (2012) <http://digitalcommons.law.scu.edu/lawreview/vol52/iss4/3/>

Le Professeur Dorothy J. Glancy de l'Université de Santa Clara (États-Unis), auteur de l'article

*Privacy in Autonomous Vehicles*⁷, distingue deux types de voitures autonomes :

- les voitures interconnectées, reliées à un réseau commun, permettant le partage et l'échange d'informations ;
- les voitures non connectées au réseau (*self-contained*), conservant toutes les données dans l'ordinateur de bord, sans effectuer d'échanges avec d'autres voitures.

Cette distinction est d'une grande importance dans la mesure où elle va avoir un impact sur la gestion des données issues de la voiture autonome. En effet, les données de la voiture non connectée au réseau seront moins facilement accessibles et présenteront moins de risques que les données des véhicules interconnectés. Leur captation nécessiterait l'installation d'un dispositif de captation dans un véhicule non connecté, et entraverait les captations à distance, ou au moins ne simplifierait pas la tâche aux forces de l'ordre.

Dans son programme de recherche *Connected Vehicle Program*, le

département américain des transports (*United States Department of Transportation ou USDOT*) aborde en particulier, le cas des voitures interconnectées. Ces dernières utiliseront des technologies de communication et des réseaux en cours de développement au sein du programme de recherche.

De nouvelles formes de communication sont en effet en train de voir le jour, en particulier celle de véhicule à véhicule (V2V – *vehicle to vehicle*) et du véhicule vers l'infrastructure (V2I – *vehicle to infrastructure*).

La communication V2V permet aux voitures interconnectées de partager entre elles (émettre et recevoir) leur vitesse, leur direction et leur positionnement en temps réel, afin d'éviter les collisions ou d'optimiser la conduite d'un groupe restreint de véhicules.

L'autonomie du véhicule permet d'envisager que les forces de police et de gendarmerie puissent techniquement prendre le contrôle d'un véhicule et lui ordonner de se ranger sur le bas-côté à partir de ce flux V2V. Il ne s'agirait plus d'un partage de données mais bien d'une prise de contrôle du véhicule.

La communication V2I permet aux véhicules de partager leur position, mais aussi la destination et jusqu'à l'itinéraire qu'ils souhaitent emprunter avec un poste central - ou une infrastructure routière -

dont le rôle serait de coordonner et de dispatcher l'information concernant le trafic, les itinéraires...

Il convient également de mentionner la communication véhicule à dispositif (V2D – *vehicle to device*) qui consiste en l'échange d'informations entre un véhicule et tout autre appareil électronique qui peut être connecté au véhicule lui-même. La communication V2D la plus classique est celle qui intervient entre un véhicule et un smartphone.

Il existe une dernière catégorie de communication, ouverte, pour ne pas dire fourre-tout, désignée par le single V2X (*vehicle to everything*).

En 2015, l'USDOT a également lancé un programme de recherche sur les véhicules connectés pour encourager les *Dynamic Mobility Applications*. Le programme de l'USDOT vise à combiner véhicule connecté et périphériques mobiles afin d'améliorer la mobilité des voyageurs, tout en réduisant les impacts environnementaux et en améliorant la sécurité routière.

Ces applications mobiles incluent les récepteurs GPS, les appareils Bluetooth, les systèmes d'*infotainment* mais surtout le – ou les smartphones – de la voiture qui guide, alerte, informe.

Ces flux de communications V2V, V2I, V2D et V2X pourraient-ils être interceptés par les forces de police et de gendarmerie

pour répondre à des finalités de maintien de l'ordre ou de sécurité, de lutte contre le terrorisme? En effet, ils renferment des données dont il conviendrait de sélectionner les plus pertinentes.

Données et voitures autonomes : un gisement de données

Capteurs, actionneurs, systèmes embarqués, ordinateurs de bord, intelligence artificielle, applications... chacune de ces technologies produit un gisement de données.

Une voiture autonome, qui peut compter jusqu'à 145 actionneurs et plus de 70 capteurs, produit ainsi plus de 25 Go de données par heure. Les flux de données sont analysés par plus de 70 ordinateurs de bord.

Plus un véhicule est autonome, plus celui-ci est en réalité dépendant des données.

Une large part de ces données doit être considérée comme des données personnelles, dès lors qu'elles permettent l'identification directe ou indirecte du conducteur ou des occupants ou utilisateurs du véhicule autonome, et sont soumises au respect de la loi Informatique et Libertés.

Absence de lignes directrices de conformité du véhicule autonome en matière de protection des données personnelles

CNIL

Le 23 mars 2016, la présidente de la CNIL a débuté les travaux d'un 6^e pack

(8) CNIL, En route vers un pack de conformité consacré aux véhicules connectés, 23 mars 2016 <https://www.cnil.fr/fr/en-route-vers-un-pack-de-conformite-consacre-aux-vehicules-connectes>

de conformité⁸ afin de concilier l'innovation dans les écosystèmes de l'automobile et la protection des

données à caractère personnel des usagers de l'automobile.

Ces travaux réunissent des acteurs issus d'horizons divers :

- acteurs de la filière automobile,
- entreprises innovantes du secteur des assurances et des télécoms,
- autorités publiques.

La CNIL organise cette concertation afin de fournir aux parties prenantes des lignes directrices et de permettre la constitution d'une « boîte à outils » de la conformité du véhicule connecté, catégorie qui englobe le véhicule autonome.

G29

Le G29 ou Groupe de travail Article 29 sur la protection des données est un organe consultatif européen indépendant sur la

protection des données et de la vie privée. Celui-ci ne s'est pas encore prononcé sur la question des voitures autonomes.

Fédération internationale de l'automobile

La Fédération internationale de l'automobile (FIA) a lancé la campagne *MyCarMyData*², dont l'objectif est que chacun puisse

décider quand et avec qui son véhicule partage des données, que le partage ne soit pas imposé, hormis pour des obligations légales. L'objectif de la FIA est de donner à chacun la liberté de choisir les services auxquels est relié le véhicule, tout au long de son cycle de vie.

Alliance of Automobile Manufacturers

Aux États-Unis, des initiatives d'autorégulation voient le jour. Les constructeurs automobiles ont ainsi adopté une déclaration de grands

(10) Alliance of Automobile Manufacturers, Privacy principles for vehicle technologies and services, 12 novembre 2014 <http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163>

principes qui entend donner des gages aux possesseurs de voitures concernant le sort réservé à leurs données¹⁰.

Privacy by design et Security by default des véhicules autonomes

Privacy by design

Définie à l'article 25 du Règlement général sur la protection des données¹¹,

l'approche *privacy by design* consiste

(11) Règlement (UE) 2016/679 du 27-4-2016 abrogeant la directive 95/46/CE (règlement général sur la protection des données) <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR> ;

(12) Sur cette question : Chloé Torres, Mettons le cap sur l'approche *Privacy by design* ! Lexing Alain Bensoussan Avocats <http://www.alain-bensoussan.com/privacy-by-design-2/2016/06/09/>

pour une entreprise à développer des produits et des services en prenant en compte, dès leur conception et tout au long de leur cycle de vie, les aspects liés à la protection de la vie privée et des données à caractère personnel.

L'approche *privacy by design* sera obligatoire en Europe dès le 25 mai 2018¹².

Security by design

Le même article 25 prévoit également le principe de protection des données par défaut.

Les acteurs de l'écosystème du véhicule autonome vont ainsi devoir se conformer

à ces deux obligations. Le pack de conformité est également l'occasion de préparer tous les acteurs du secteur au futur règlement européen sur les données personnelles qui serait opérationnel en 2018 et de porter au niveau européen les recommandations nationales.

Accord européen pour l'adoption d'un standard universel de données entre véhicules autonomes et Cloud

Très récemment, Ertico-ITS, partenariat public-privé pour des systèmes de transport intelligents (ITS) vient d'accepter le développement d'un standard mondial dénommé *Sensoris* proposé par la

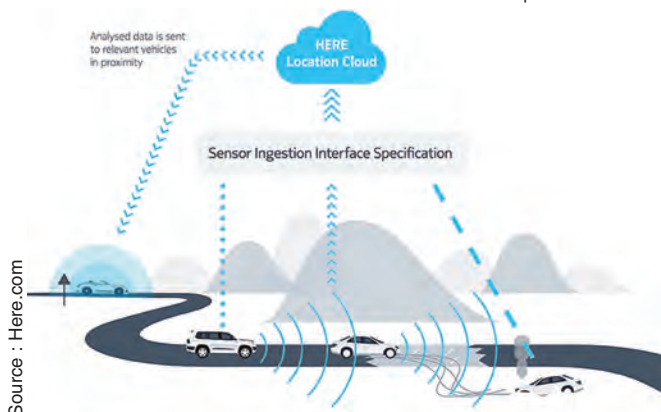
(13) https://its.cms.here.com/static-cloud-content/Newsroom/290616_HERE_automotive_companies_move_forward_on_car_to_cloud_data_standard.pdf

(14) <http://ertico.com/vision-and-mission/>.

société *Here Maps*¹³ pour l'adoption d'un format de données universel pour les véhicules autonomes. Il s'agit

selon Ertico-ITS de proposer une spécification d'interface standardisée

utilisable par l'ensemble de l'industrie automobile pour les véhicules autonomes. Ce standard devrait permettre la création du premier réseau de partage de données sur les véhicules autonomes permettant de rendre les déplacements des véhicules autonomes



plus sûrs et de réduire les accidents.

Ertico-ITS, fondé en 1991, se définit comme un « *partenariat public-privé, multi-secteur, poursuivant le développement et le déploiement des ITS (systèmes de transport intelligents)* »¹⁴. Il a été constitué pour promouvoir le succès paneuropéen d'un marché des ITS et veiller à ce que les intérêts européens soient pleinement représentés dans le monde entier. Il convient de noter que ne figure côté français au Conseil de surveillance d'Ertico-ITS qu'un seul représentant issu de la société Renault, alors que pour d'autres pays européens, c'est le ministre des transports qui participe au Conseil de surveillance d'Ertico-ITS.

Avec plus de 100 partenaires à travers les cinq secteurs : pouvoirs publics, industrie, opérateurs d'infrastructure, utilisateurs, et autres ; Ertico-ITS réunit l'ensemble des acteurs clés pour le véhicule autonome et plus généralement pour les systèmes de transport intelligent.

Parmi les constructeurs automobiles partenaires d'Ertico-ITS figurent Volvo, Toyota, Renault, Jaguar, Land-Rover, Honda, Ford, Fiat, BMW, Mini et ACEA. Figurent également parmi les partenaires d'Ertico-ITS les fournisseurs et équipementiers : Aisin AW CO.LTD., Bosch, Continental, Denso, Ficosa, Fujitsu Ten, Gemalto, Here, LG Electronics, Mitsubishi Electric, NavInfo,

NEC, Novero, NXP, Panasonic, Peiker, Pioneer, Telit, TomTom et 3M.

Les problématiques juridiques

Il n'existera donc pas de marché pour les véhicules autonomes demain sans un encadrement juridique du volume des données produites ou traitées par le véhicule autonome pour se déplacer dans son environnement. Les flux d'informations générés par la voiture autonome vont également nécessiter de définir une frontière et des garde-fous afin de préserver un juste équilibre entre vie privée et méthodes d'investigation et de surveillance des forces de l'ordre des véhicules autonomes.

Les véhicules autonomes recueilleront et partageront une énorme quantité d'informations non seulement sur les mouvements de leurs occupants mais également sur leurs habitudes, leurs préférences, leurs communications avec l'extérieur, etc.

La captation de ces données ne sera pas sans conséquences sur la vie privée des occupants des véhicules autonomes.

Si ces données peuvent paraître anodines, leur accumulation permettra de relever des données intimes sur les occupants, en permettant d'inférer des informations, de créer de nouveaux types de profilages à partir de l'extraction de données ou d'algorithmes prédictifs.

Quel droit pour les forces de l'ordre sur

les voitures autonomes ? Quels moyens et capacités de contrôle des forces de l'ordre sur les voitures autonomes ?

La réponse à ces deux questions ne résulte pas uniquement d'enjeux juridiques et dépend également d'enjeux technologiques, normatifs, éthiques et transversaux. Elle implique de prendre en compte des questions nouvelles, suscitant elle-même des débats et parfois même des débats de société.

Une grande partie des interrogations que soulève la question des capacités de contrôle des forces de police et de gendarmerie concerne finalement nos relations avec ces objets tangibles que sont les voitures autonomes, leur statut juridique, mais aussi la délimitation de la frontière entre maintien de la sécurité publique, protection de la sécurité des personnes et des biens, et protection de nos données personnelles.

Un autre aspect est également déterminant et importe tout autant que la fixation de cette frontière. Il concerne la cybersécurité des voitures autonomes, des systèmes complexes et embarqués, des multitudes de capteurs et de la profusion de données produites *via* les capteurs ou actionneurs nécessaires au fonctionnement sur l'espace public des véhicules autonomes mais aussi par les occupants des véhicules autonomes.

À partir de là, rien n'est simple.

Un entier contrôle à distance par les forces de l'ordre sur les voitures autonomes est évidemment susceptible d'entraîner des dérives et des atteintes aux libertés fondamentales et notamment à la *privacy*. Une voiture autonome doit-elle être programmée pour exécuter tout ce que pourrait demander un représentant des forces de l'ordre ?

Si le véhicule autonome est équipé d'un bouton *Off*, l'occupant, l'utilisateur ou le propriétaire du véhicule autonome pourront-ils l'activer et dans quelles situations ou configurations (espace, temps) ? Les forces de l'ordre pourront-elles être en mesure d'empêcher l'utilisation du bouton *Off* à partir de leurs tablettes numériques lors d'un contrôle autoroutier par exemple et dans quelles conditions juridiques et opérationnelles ?

Répondre à ces questions conduit à envisager une refonte de notre droit applicable aux véhicules autonomes dès aujourd'hui et à anticiper un nouveau droit en matière de contrôle par les forces de l'ordre des véhicules autonomes.

Il convient de ne pas attendre que les voitures autonomes soient omniprésentes sur l'espace public après disparition totale des voitures thermiques pour commencer à réfléchir aux règles juridiques que pourront mettre en œuvre les autorités judiciaires et les forces de sécurité. La mise en œuvre d'une opération de captation d'informations par les forces de

police et de gendarmerie pose aujourd'hui des défis techniques et juridiques non-résolus.

La captation de données, lorsqu'elle se déroule sur plusieurs heures, va amener les forces de l'ordre à emmagasiner plusieurs centaines de Go de données. Bien qu'elle ne soit pas insoluble, cette difficulté devra être anticipée par les personnes en charge de la captation.

Par ailleurs, le recueil d'une telle quantité d'informations pose des problèmes de respect de la vie privée et des données à caractère personnel. Il conviendra de s'interroger sur la possibilité de sélectionner les flux de données les plus pertinents pour l'enquête ou l'information judiciaire mais également les plus strictement nécessaires.

Boîtes noires

Les systèmes de boîtes noires peuvent-ils être intégrés au véhicule autonome et être utilisés à titre de preuve sans méconnaître les droits des occupants ? L'utilisateur ou occupant du véhicule autonome doit-il consentir à l'utilisation d'un tel dispositif ? Les forces de l'ordre doivent-elles avoir accès aux données recueillies par une boîte noire ? Faut-il attribuer aux assureurs un droit d'accès à celles-ci ? Dans quels cadres et conditions d'accès après un accident de la circulation ?

L'ensemble de ces questions fait débat.

S'agissant des assureurs, la CNIL avait

montré quelques réticences à la mise en œuvre de systèmes embarqués de géolocalisation à des fins de modulation de tarifs d'assurance automobile, avant de finalement autoriser ces systèmes. Par sa délibération du 8 avril 2010, elle subordonne l'utilisation d'un tel système au respect des conditions suivantes :

- la finalité de traitement se cantonne à la modulation des tarifs d'assurance automobile ;
- les infractions éventuelles au Code de la route ne doivent pas être identifiées ;
- seul le traitement de la vitesse moyenne peut être réalisé ;
- les assureurs doivent enfin prendre des mesures afin d'éviter l'agrégation des données.

La CNIL recommande également aux assureurs d'éviter la multiplication des données et de ne les conserver que pendant le temps nécessaire pour caractériser chaque item utile au calcul de la prime

(15) Délibération n° 2010-096 du 8 avril 2010 portant recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules
<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00002227831> ;

d'assurance¹⁵. Se pose ainsi la question de savoir si ces conditions sont transposables aux boîtes noires.

La principale difficulté va se situer au niveau de l'agrégation des données stockées dans la boîte noire. Cette

agrégation risque d'être difficilement conciliable avec les exigences actuelles de la CNIL. Une solution pourrait être de mettre en place un système faisant intervenir un tiers de confiance en charge de ne communiquer aux assureurs que les informations strictement nécessaires à l'exécution du contrat.

Dans le cadre d'une procédure pénale, si la preuve d'une infraction pénale est facilitée par le recours aux nouvelles technologies, il convient néanmoins de s'assurer que la preuve de la commission d'une infraction respecte bien les principes généraux de la procédure pénale. Un parallèle peut ici encore être opéré avec la géolocalisation.

En France, la Cour de cassation considère que cette technique constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge¹⁶.

En l'état actuel du droit, l'accès à la boîte noire du véhicule autonome devrait être préalablement autorisé par un juge et ne pourrait pas être mis en œuvre dans le cadre d'un simple contrôle des forces de l'ordre.

Faut-il adapter le cadre juridique actuel pour encadrer demain les contrôles des voitures autonomes ?

Notre droit positif en vigueur encadre déjà :

- le contrôle automatisé des données signalétiques des véhicules et les traitements automatisés de données personnelles ;
- la prévention, répression, exposition particulière à un risque d'actes de terrorisme ;
- les comportements en cas de contrôle routier ;
- les captations de données informatiques dans un lieu privé qui peut être le véhicule d'une personne.

Contrôle automatisé des données signalétiques des véhicules et traitements automatisés de données personnelles.

Notre cadre juridique actuel et notamment le Code de la sécurité intérieure permet déjà, afin de faciliter la constatation des infractions en matière de terrorisme et plus généralement de faciliter la constatation des infractions criminelles ou liées à la criminalité organisée aux services de police et de gendarmerie nationales et des douanes, aux termes des dispositions de l'article L-233-1 du Code de la sécurité intérieure, de mettre en œuvre des dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules prenant la

(16) Cass.crim. 22 octobre 2013, n°13-81945
<https://www.legifrance.gouv.fr/affichJuriJudi.do?oldActio n=rechJuriJudi&idTexte=JUR ITEXT000028116516&fastR>

photographie de leurs occupants, en tous points appropriés du territoire, en particulier dans les zones frontalières, portuaires ou aéroportuaires ainsi que sur les grands axes de transit national ou international.

Pour les finalités précitées, les données à caractère personnel collectées à l'occasion des contrôles susmentionnés peuvent faire l'objet de traitements automatisés mis en œuvre par les services de police et de gendarmerie nationales ainsi que par les services des douanes.

L'alinéa 2 de l'article L233-1 du Code de la sécurité intérieure autorise également, à titre temporaire, l'emploi de dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules, pour la préservation de l'ordre public, à l'occasion d'événements particuliers ou de grands rassemblements de personnes, par décision de l'autorité administrative.

L'article L233-2 du Code de la sécurité intérieure permet que les données à caractère personnel collectées à l'occasion des contrôles réalisés conformément aux dispositions de l'article L233-1 du Code de la sécurité intérieure puissent faire l'objet d'un traitement automatisé des données à caractère personnel collectées pour les finalités mentionnées à l'article L233-1 du Code de la sécurité intérieure précité.

L'article L233-2 du Code de la sécurité

intérieure prévoit également que les traitements comportent une consultation du traitement automatisé des données relatives aux véhicules volés ou signalés ainsi que du système d'information Schengen et, afin de permettre cette consultation, la conservation des données collectées durant un délai maximum de huit jours au-delà duquel elles sont effacées, dès lors qu'elles n'ont donné lieu à aucun rapprochement positif avec les traitements. En outre, les données qui ont fait l'objet d'un rapprochement positif avec ces mêmes traitements peuvent être conservées pour une durée d'un mois sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale ou douanière.

Afin de prévenir et de réprimer les actes de terrorisme et de faciliter la constatation des infractions s'y rattachant, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent avoir accès à ces traitements.

L'article L235-1 du Code de la sécurité intérieure prévoit que les données contenues dans les traitements automatisés de données à caractère personnel gérés par les services de police et de gendarmerie nationales peuvent être transmises, dans le cadre des engagements internationaux régulièrement introduits dans l'ordre juridique interne, à des organismes de

coopération internationale en matière de police judiciaire ou à des services de police étrangers, qui représentent un niveau de protection suffisant de la vie privée, des libertés et des droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Prévention, répression, exposition particulière à un risque d'actes de terrorisme.

L'article L223-4 du Code de la sécurité intérieure autorise également la mise en œuvre de système de vidéoprotection, pour une durée déterminée, lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent.

Comportement en cas de contrôle routier.

En matière de comportement, lors d'un contrôle routier, l'article L233-1 du Code de la route dispose que le fait pour tout conducteur d'omettre d'obtempérer à une sommation de s'arrêter émanant d'un fonctionnaire ou agent chargé de constater les infractions et muni des insignes extérieurs et apparents de sa qualité est puni de 3 mois d'emprisonnement et de 3 750 euros d'amende. Toute personne coupable du délit de l'article L233-1 du Code de la route encourt également des peines complémentaires.

Dans le cadre de contrôles routiers de véhicules autonomes, entièrement

automatisés par des robots-policiers ou des robots-gendarmes, sous la supervision des forces de l'ordre, la réglementation en vigueur devra nécessairement être modifiée et complétée pour permettre la constatation directe d'infractions par des robots-policiers et gendarmes. Tous les experts devraient s'accorder sur la nécessité d'élaborer des règles juridiques définissant les capacités de contrôle des forces de police et de gendarmerie sur les voitures autonomes.

Quant à partir de 2025 et 2030, seules les voitures autonomes seront en circulation sur l'espace public, sur la base de quelles règles juridiques et par quels moyens les forces de police et de gendarmerie pourront-elles contrôler ces véhicules qui posséderont une autonomie, une indépendance et un degré de liberté en raison des capteurs embarqués ? Ce nouveau cadre juridique devrait, selon nous, appréhender et définir les conditions de contrôle à distance des véhicules autonomes.

Captation de données informatiques.

La loi relative au renseignement du 24

(17) Loi n° 2015-912 relative au renseignement du 24 juillet 2015

juillet 2015¹⁷

introduite dans le Code de la sécurité

intérieure autorise dans les conditions prévues dans ledit code l'utilisation de dispositifs techniques permettant la captation, la fixation la transmission et l'enregistrement d'images et de données

informatiques dans un lieu privé. L'autorisation d'utilisation de dispositifs techniques de captation, de fixation et d'enregistrement de données informatiques à l'intérieur n'est donnée qu'à des agents appartenant à l'un des services spécialisés de renseignement mentionnés aux articles L. 811-2 et L. 811-4 du Code de la sécurité intérieure et pour les finalités définies à l'article L.811-3 du Code de la sécurité intérieure.

Rappelons que parmi ces finalités figurent notamment la prévention du terrorisme (4°), la prévention des troubles à l'ordre public (5°), la prévention de la criminalité et de la délinquance organisées (6°). En l'état de notre droit positif, la captation de données informatiques sur une voiture autonome ne pourrait être autorisée que dans les cas précités prévus par la loi.

Dans ce cadre, l'article 706-102-1 précise les conditions d'une captation des données par la mise en place d'un dispositif technique et sous contrôle d'un

(18) www.code-et-lois.fr/code-de-procedure-penale/article-706-102-1

magistrat¹⁸ en tous lieux et sans le consentement de

l'intéressé.

Investigations policières et 4^e Amendement aux États-Unis : la vision de la Cour Suprême américaine

Les origines du 4^e Amendement de la Constitution américaine tiennent aux pratiques mises en œuvre par les autorités britanniques qui, pour lutter contre la subversion dans les colonies

américaines, se munissaient de mandats formulés dans les termes les plus généraux (*general warrants*), de manière à ce que les fouilles et perquisitions soient les plus larges possibles.

En réaction à cette pratique, les Américains ont intégré dans leur *Bill of*

*right*¹⁹ un 4^e Amendement énonçant :

« le droit des citoyens d'être garantis dans leurs personnes, domicile, papiers et effets, contre les

fouilles [search] et saisies déraisonnables ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur une présomption sérieuse [probable cause], corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir ».

Par la décision *Smith v. Maryland* (1979)²⁰, la Cour suprême des États-Unis a énoncé qu'une fouille par les forces de l'ordre devait être considérée comme déraisonnable au sens du 4^e Amendement (*unreasonable search*) :

– lorsqu'elle empiète sur la *reasonable expectation of privacy* - à savoir, l'attente raisonnable d'un citoyen au respect de sa vie privée ; et

– dans la mesure où la société est prête à considérer une telle attente comme raisonnable.

(19) Les dix premiers amendements à la Constitution américaine forment la déclaration des droits. Ils affirment des droits des citoyens, sous la forme d'une limitation explicite des pouvoirs de l'Etat.

(20) *Smith v. Maryland*, 442 U.S. 735 (1979) <http://caselaw.findlaw.com/us-supreme-court/442/735.html>

Dans l'hypothèse où une fouille dépasserait la *reasonable expectation of privacy*, l'agent de police devra préalablement obtenir un mandat d'un juge, ou à défaut agir dans le cadre d'une exception à l'exigence d'un mandat.

La doctrine de la *reasonable expectation of privacy* est le critère majeur pour la définition du champ d'application de la protection de la vie privée par le 4^e Amendement. C'est ce critère qui va permettre de déterminer, au regard de la jurisprudence de la Cour Suprême, quelles fouilles, et plus largement quelles captations – ou interceptions d'informations – les forces de l'ordre seraient en droit de mettre en œuvre ou, au contraire, seraient jugées comme déraisonnables au sens du 4^e Amendement..

Il convient de distinguer la fouille de la voiture autonome de la surveillance qui peut être mise en œuvre au moyen des informations collectées ou émises par le véhicule autonome.

Fouille de voiture autonome

Aux États-Unis, les automobiles constituent des effet au sens du 4^e Amendement, et leurs propriétaires ou possesseurs peuvent généralement prétendre à une attente raisonnable du respect de leur vie privée contre les intrusions que pourraient constituer les fouilles par les forces de l'ordre.

L'entrée et les recherches effectuées

dans un véhicule automobile par d'un agent de police constitue une fouille (search) et nécessite de ce fait un mandat délivré par un magistrat (sauf exception).

L'entrée dans les systèmes informatiques de la voiture autonome, ou la captation des données émises ou reçues par cette dernière pourrait également être qualifiée de search au même titre que la fouille physique d'un véhicule.

Parce que les véhicules autonomes ne sont pas encore disponibles pour une utilisation générale, les prévisions concernant les attentes raisonnables de respect de la vie privée en ce qui concerne les véhicules autonomes doivent nécessairement être déduites à partir des décisions de la Cour Suprême concernant d'autres types de véhicules (notamment la voiture avec conducteur), modes de transport, ou systèmes.

Excluant d'abord les automobiles du champ d'application du 4^e Amendement, la Cour suprême des États-Unis a fait évoluer sa jurisprudence à la fin du XX^e siècle.

Début du XX^e

Au début du XX^e siècle, la Cour Suprême s'est montrée réticente à appliquer la protection conférée par le 4^e Amendement aux véhicules automobiles présents sur la voie publique. Par leur nature même, et à la différence des propriétés privées, les voies publiques n'étaient pas considérées

comme des lieux où les citoyens devaient attendre une quelconque protection de leur vie privée.

À titre d'illustration, dans sa décision

(21) *Olmstead v. United States*, 277 U.S. 438 (1928)
<https://www.law.cornell.edu/supremecourt/text/277/438>

(22) *Carroll v. United States*, 267 U.S. 132 (1925)
<https://www.law.cornell.edu/supremecourt/text/267/132>

Olmstead v. United States (1928)²¹, la Cour Suprême a expressément refusé la protection par le 4^e Amendement des activités menées

dans les lieux publics.

Durant la Prohibition (de 1919 à 1933), la Cour Suprême a ainsi autorisé de nombreuses pratiques pour faire cesser la contrebande soupçonnée d'alcool. La décision *Carroll v. United States* (1925)²² en est l'illustration la plus marquante.

Dans cette affaire, la Cour Suprême accorde aux autorités de police une plus grande marge de manœuvre pour la fouille de véhicules que pour les perquisitions de biens immobiliers. En l'espèce, les autorités de police, à la recherche d'alcool de contrebande, arrêtaient et fouillaient un grand nombre d'automobiles.

La Cour a décidé que les véhicules pouvaient être fouillés sans mandat dans la mesure où les forces de l'ordre justifiaient d'une présomption sérieuse de transport d'alcool de contrebande.

Tournant des années 70

En 1967, dans une décision *Katz v. United States*²³, la Cour Suprême a

(23) *Katz v. United States*, 389 U.S. 347 (1967)
<https://www.law.cornell.edu/supremecourt/text/389/347>

énoncé le principe selon lequel le 4^e Amendement

protège « *les hommes – et pas seulement les lieux – contre les fouilles et saisies déraisonnables* » et en a déduit que « *son application ne doit pas dépendre de l'existence ou de l'absence d'une intrusion physique dans une sorte quelconque d'espace clos et fermé* ».

Deux conclusions essentielles, encore applicables aujourd'hui, sont à tirer de cette décision :

– la première est que la présence dans un lieu public n'écarte pas l'application du 4^e Amendement. La Cour Suprême a rejeté le raisonnement selon lequel la possession d'un mandat n'est exigée qu'en cas d'interférence avec le droit de propriété.

– la seconde, est que la Cour Suprême n'exclut plus les éléments de preuve intangibles.

Ainsi, dans la mesure où la plupart des informations personnelles générées par les véhicules autonomes seront des données numériques intangibles collectées sur la voie publique, la décision *Katz v. United States* est essentielle pour la compréhension des principes et de l'étendue de la protection conférée par le 4^e Amendement pour les attentes de la vie privée dans les véhicules autonomes.

Cette décision ne signifie pas pour autant que toutes les communications

intangibles dans les lieux publics seront toujours automatiquement protégées par le droit à la vie privée. Mais elle rend éligibles à la protection les communications entre les véhicules autonomes et :

- d'autres véhicules autonomes ;
- l'infrastructure routière ;
- d'autres appareils mobiles ;
- le Cloud.

Qu'en est-il aujourd'hui ?

Aujourd'hui, la doctrine américaine distingue l'arrêt du véhicule de la fouille elle-même.

(24) Terry v. Ohio, 392 U.S. 1 (1968)
<https://www.law.cornell.edu/supremecourt/text/392/1>

Depuis la décision Terry v. Ohio²⁴ (1968), la Cour suprême n'exige plus

de probable cause (présomption sérieuse) pour demander l'arrêt d'une automobile. L'agent de police doit seulement justifier d'un soupçon raisonnable que la personne a commis, commet ou est sur le point de commettre une infraction.

En revanche, la fouille du véhicule sans mandat à la suite de cet arrêt doit être justifiée par une probable cause (présomption sérieuse).

En l'absence de conducteur, et donc d'observation du comportement de celui-ci, la preuve d'une raisonnable suspicion ou d'une probable cause (présomption sérieuse) va être rendue plus difficile par les forces de l'ordre.

Voitures connectées et exception à l'exigence de mandat

L'exigence de mandat délivré par un juge connaît néanmoins plusieurs exceptions qui s'appliquent à l'automobile. Les principales exceptions aux exigences du 4^e Amendement sont les suivantes :

Consentement : la police peut fouiller un véhicule si elle reçoit le consentement volontaire du propriétaire ou possesseur apparent du véhicule. Le recueil d'un consentement sera plus difficile à obtenir dans le cas où la voiture autonome ne transportera ni occupant ni conducteur. ;

Exception automobile: un véhicule peut être fouillé sans mandat lorsque la preuve d'une contrebande risque de disparaître en raison de la mobilité d'un véhicule et il n'est ainsi pas possible d'obtenir un mandat sans compromettre la preuve potentielle ;

(25) Arizona v. Gant, 556 U.S. 332 (2009)
<http://www.supremecourt.gov/opinions/08pdf/07-542.pdf>

Fouille incidente à l'arrestation : la décision

Arizona v. Gant

(2009)²⁵ a précisé qu'un agent de police pouvait fouiller un véhicule à la suite de l'arrestation récente d'un occupant à condition que la personne arrêtée soit à distance de marche du compartiment des passagers ou qu'il soit raisonnable de croire que le véhicule contient des preuves de l'infraction de l'arrestation ;

Fouille sommaire: la police peut fouiller l'habitacle d'un véhicule pour y trouver une arme si l'agent a des soupçons

raisonnables et que l'occupant du véhicule peut devenir dangereux si on lui laisse accès à l'arme en question ;

Fouille d'inventaire : un véhicule légalement mis à la fourrière peut être physiquement fouillé dans le cadre d'un inventaire de routine;

Contrôle du permis de conduire et de l'immatriculation du véhicule: sous certaines circonstances, la police peut procéder à la fouille d'un véhicule pour s'assurer de la conformité de son immatriculation et du respect des exigences réglementaires.

En principe, ces exceptions sont vouées à s'appliquer aux véhicules autonomes comme elles le sont pour les voitures classiques.

Néanmoins, la nature de la preuve que les forces de l'ordre peuvent chercher dans les véhicules autonomes peut compliquer l'analyse des exceptions du 4^e Amendement. A cet égard, le recueil de preuves numériques des véhicules autonomes par la police peut se révéler particulièrement sensible.

Récemment, dans l'affaire Riley v.

California (2014)²⁶, la Cour suprême a jugé déraisonnable une fouille sans mandat portant sur des téléphones mobiles à la suite d'une arrestation. Pour parvenir à ce résultat, la Cour a souligné la quantité et la nature potentiellement sensible de l'information numérique présente dans ces dispositifs.

(26) Riley v. California, 573 U.S. ____ (2014) <https://supreme.justia.com/cases/federal/us/573/13-132/>

Appliquée aux véhicules autonomes, cette décision encouragera la contestation d'une fouille, même lorsque cette action est prise en vertu d'une exception reconnue. L'émergence de véhicules autonomes pourrait ainsi limiter les moyens d'investigation classiques en raison des données sensibles que contient cette catégorie de véhicule.

Surveillance des véhicules autonomes

Il convient de distinguer les deux types de surveillance qui pourraient être mis en œuvre par les forces de l'ordre américaines : la surveillance ciblée et la surveillance de masse.

Surveillance ciblée

La surveillance ciblée garde la trace d'une personne particulière et identifiée.

Surveillance à distance

Dans l'affaire United States v. Jones

(27) United States v. Jones, 132 S. Ct. 945, 565 U.S. ____ (2012) <https://www.law.cornell.edu/supremecourt/text/10-1259>

(2012)²⁷, la question s'est posée de savoir si le tracking GPS d'une voiture

nécessitait un mandat préalable du juge. Dans le cas d'espèce, les policiers avaient tracé pendant 28 jours les déplacements d'un trafiquant de drogue grâce à un système GPS qu'ils avaient implanté dans la voiture de sa femme.

Les juges de la Cour Suprême ont appliqué la doctrine habituelle de la reasonable expectation of privacy, en se demandant si le justiciable pouvait raisonnablement avoir anticipé d'être ainsi

surveillé sans autorisation d'un magistrat.

La Cour Suprême a décidé qu'à moins qu'un mandat soit d'abord obtenu auprès d'un juge, le suivi à distance automatisé d'un véhicule autonome sur la voie publique interférerait avec des attentes raisonnables de la vie privée protégée en vertu du 4^e Amendement.

Obtentions de données auprès de tiers

La third-party doctrine repose sur l'idée selon laquelle un individu n'a pas de reasonable expectation of privacy lorsqu'il communique volontairement à un tiers des informations.

Cette doctrine a été appliquée dans

(28) Smith v. Maryland, 442 U.S. 735 (1979)
<https://www.law.cornell.edu/supremecourt/text/442/735>

l'affaire Smith v. Maryland²⁸. Il s'agissait en l'espèce d'un dispositif

enregistrant tous les numéros appelés à partir d'une ligne de téléphone particulière qui avait été installée par la police dans une compagnie téléphonique.

L'opinion majoritaire a par ailleurs considéré qu'il n'était pas déraisonnable de supposer que la compagnie téléphonique gardait dans ses registres une trace de tous les numéros de téléphone composés.

Dans le cadre d'une surveillance ciblée faisant appel à une infrastructure tierce (constructeurs, opérateurs de téléphonie mobile...), les forces de l'ordre pourraient invoquer la *third-party doctrine* pour

justifier l'acquisition sans mandat d'informations concernant l'utilisation du véhicule autonome.

Captation des données contenues dans le véhicule

La captation des données enregistrées dans le véhicule autonome devrait suivre le même régime que celui de la fouille : mandat ou probable cause (présomption sérieuse).

Surveillance de masse

La surveillance de masse implique la collecte complète et sans discrimination des informations personnelles d'une population ou d'un groupe. La surveillance de masse rassemble littéralement toutes les informations disponibles à propos de toutes les personnes à portée de la surveillance en question. La surveillance de masse pourrait être utilisée pour le profilage de personnes, la prédiction de comportements, et éventuellement la manipulation du comportement des véhicules et de leurs utilisateurs.

(29) City of Indianapolis v. Edmond, 531 U.S. 32 (2000)
<https://www.law.cornell.edu/supct/html/99-1030.ZS.html>

Dans l'affaire, Indianapolis v. Edmond (2000)²⁹, l'opération au cours

de laquelle des agents de police ont arrêté et fouillé chaque automobile d'une route aux fins de démasquer des transporteurs de drogue a été jugée déraisonnable.

La Cour Suprême a en effet considéré que l'arrêt sur une route de chaque automobile à des fins générales d'application de la loi constitue une fouille au sens du 4^e Amendement et nécessite un mandat judiciaire.

Les forces de l'ordre, mais également les investisseurs privés, les régies publicitaires et les mercaticiens pourraient souhaiter, dans le cadre de leurs activités, obtenir l'accès aux informations émises par les voitures autonomes, et leur réseau le cas échéant.

En matière de surveillance de masse, la Federal Communications Commission (FCC) a enquêté sur la collecte massive de données sur des réseaux Wifi non-sécurisés par *Street View*. Après avoir condamné Google au paiement d'une amende de 25 000 dollars pour entrave à l'enquête, la FCC a rendu un rapport le

(30) F.C.C. Report on Google's Street View Project http://www.nytimes.com/interactive/2012/04/29/technology/fcc-report-on-google-street-view-project.html?_r=0

13 avril 2012³⁰ faisant état d'un programme informatique intégré aux Google Cars

conçu pour collecter ces données personnelles.

(31) Délibération n°2011-035 du 17 mars 2011 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société GOOGLE Inc <https://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987>

Par une délibération rendue le 17 mars 2011, la Commission Nationale de l'Informatique et des Libertés (CNIL) a

prononcé en France une sanction

pécuniaire de 100 000 € à l'encontre de Google pour les mêmes motifs³¹.

Faut-il définir un cadre éthique ?

Le véhicule autonome intégrera de plus en plus d'intelligence artificielle.

L'intégration de plus d'intelligence artificielle dans le véhicule autonome permettant une plus grande autonomie et donc une plus grande automatisation de la conduite et des opérations liées à la conduite questionne également le débat éthique.

Définir un ou plusieurs cadres d'éthique permettant de déterminer si un bouton OFF devra être prévu dans tout véhicule autonome, ainsi que cerner les hypothèses d'utilisation du bouton OFF dans une voiture autonome, ne sera pas chose facile. En effet, en fonction de l'autonomie des voitures autonomes dans leur prise de décision, cela nécessitera très probablement de définir des règles primaires mais également toutes les variations ou déclinaisons possibles.

En 2030, il ne peut être exclu que tout ou partie de certains types de contrôles de véhicules autonomes puissent être automatisés par le recours à des robots-policiers ou des robots-gendarmes, sous la supervision de policiers ou gendarmes humains, en interaction ou non avec des drones de surveillance.

Les robots capables de réguler la circulation existent déjà dans certains pays. En effet dès 2013, le premier robot

de régulation de la circulation a été mis en œuvre en République démocratique du Congo (RDC)³².

(32)
<http://www.aaaep.fr/blog-tests-psychotechniques/robot-regule-circulation-0059-684/>

(33)
<https://humanoïdes.fr/robots-policiers-dubai-expo-2020/>

Le saut technologique nécessaire pour que certains robots soient capables

demain d'établir certains contrôles automatiques donnant lieu à une verbalisation de véhicule autonome dans certaines configurations déterminées, n'est pas une simple hypothèse d'école.

Les Émirats Arabes Unis envisagent de déployer à Dubaï en 2020 des robots policiers pour l'Expo 2020. Ils pourraient bien préfigurer un modèle d'agent de l'ordre 4.0, même si la Smart Police de Dubaï n'envisage de confier aux robots-policiers que des tâches bien spécifiques³³.

La définition d'un cadre légal en matière de contrôle à distance des véhicules autonomes pour les forces de l'ordre sera également fortement subordonnée, outre les questions juridiques et éthiques, à de nombreux autres enjeux que nous n'avons pas développés volontairement dans cet article et qui pourront faire l'objet de nos prochaines publications.

Il s'agit notamment des enjeux industriels, des enjeux de la normalisation en matière de véhicule autonome et en matière de traitement des gisements de données,

des risques liés à la cybersécurité des architectures et des systèmes complexes que sont les voitures autonomes. La complexité de conception et de développement d'architectures de systèmes complexes dédiés aux voitures autonomes nécessitant d'identifier les risques de défaillances matérielles des capteurs et actionneurs ainsi que des dysfonctionnements logiciels, ont conduit l'Iso à publier la norme ISO 26262 sur la sécurité fonctionnelle. Sur la base d'un cycle de vie de la sécurité pour le véhicule autonome, celle-ci doit permettre de démontrer que l'ensemble des exigences de sécurité est respecté.

S'agissant des risques liés à la cybersécurité, l'Institut de recherche technologique (IRT) SystemX, dans le cadre du projet EIC, vient de lancer un programme de recherche sur une durée de cinq ans dont l'objet d'étude consiste à déterminer les bons arbitrages à mettre en œuvre entre coût de la sécurité des véhicules autonomes, sûreté de fonctionnement et respect d'un droit numérique tout en tenant compte des besoins de l'ensemble des parties prenantes.

Application de l'intelligence

artificielle (IA) à la robotique : un cadre juridique et éthique est nécessaire

par **DIDIER GAZAGNE**

D

Dans cette publication, rédigée spécifiquement pour l'AGORA Droit des robots du FIC 2017, il est proposé de faire un point sur la manière dont l'intelligence artificielle appliquée à la robotique modifie les frontières entre technologie et droit ainsi que sur la manière dont les règles de la responsabilité sont impactées par les robots qualifiés d'intelligents. Aux termes de cette analyse, il nous apparaît que le droit commun applicable en matière de

responsabilité est mal adapté, et que les régimes spéciaux de responsabilité, notamment la responsabilité du fait des choses, bien que plus opportune, présentent

également une inadaptation à l'intelligence artificielle appliquée à la robotique. Une publication relative à l'analyse du droit positif et des régimes de responsabilité en vigueur à l'épreuve de l'intelligence artificielle appliquée à la robotique sera réalisée dans le cadre des prochains travaux de l'ADDR et publiée également sur le site web alain-bensoussan.com.

L'intelligence artificielle irrigue déjà de nombreux domaines et secteurs, au premier rang desquels la finance, la santé, la recherche, le e-commerce et même les métiers du droit.

Or, du fait du couplage avec une intelligence artificielle toujours plus sophistiquée – dont le point culminant serait l'émergence d'une IA forte – et du rôle majeur des algorithmes, les robots ont vocation à disposer de toujours plus d'autonomie décisionnelle, et ce, grâce à une capacité d'apprentissage en constante augmentation, d'abord



DIDIER GAZAGNE

Avocat
Vice-Président de
l'Association du Droit des
robots (ADDR)
Président de la
Commission Usine 4.0
(ADDR)



« les avancées fulgurantes de l'IA appliquée à la robotique impactent les frontières entre technologie et droit. »

supervisée par l'humain, puis non supervisée.

Ce couplage entre la robotique et l'IA doit-il conduire à adapter notre système de responsabilité et d'indemnisation ? Une réponse positive semble s'imposer et un processus de normalisation a déjà été à ce titre enclenché au niveau de l'Union européenne.

Peut-on envisager de franchir une étape supplémentaire et considérer que la rupture technologique majeure résultant de la synergie entre la robotique mécanicienne et le développement des

applications d'intelligence artificielle doit conduire à repenser notre système de catégorisation juridique, de telle sorte à donner une place à cet être artificiel ?

Certains le proposent déjà, aux États-Unis et en France notamment, dans le cadre d'une approche prospective assumée qui consiste à s'interroger sur le fondement et la fonction d'un tel renouvellement des catégories juridiques. À tout le moins, on peut penser qu'il sera très délicat de ne pas voir dans l'entité « robot-IA » un objet de droit complexe soumis, à cet égard, à un certain nombre de régimes

spécifiques. L'enjeu de cet enchevêtrement de corpus normatifs sera de trouver un point d'équilibre entre la vision matérielle que l'on peut en avoir et son « *intelligence* » (qui peut être objectivée et étalonnée au regard de sa capacité à résoudre les problèmes qui lui sont soumis).

Dans tous les cas, les avancées fulgurantes de l'IA appliquée à la robotique impactent les frontières entre technologie et droit. En effet, plus le robot aura accès à une intelligence artificielle forte et disposera d'autonomie décisionnelle et d'une capacité d'apprentissage machine (*Machine learning*) non supervisé par l'homme (c'est-à-dire lorsque les données des algorithmes d'apprentissage machine en entrée et en sortie ne sont pas nécessairement connues par l'humain dans la boucle), moins le robot pourra être considéré comme un simple objet de droit sous le contrôle ou la garde d'un ou de plusieurs acteurs (le concepteur, le fabricant, le codeur des briques logicielles ou *hardware*, le codeur des algorithmes, le propriétaire du robot, l'utilisateur ou encore l'intégrateur).

En réalité, des systèmes disposant d'une autonomie décisionnelle et d'une capacité d'apprentissage non supervisés par l'homme existent déjà.

Robot, machine, intelligence artificielle (IA) : de quoi parle-t-on ?

Le terme robot est utilisé abondamment mais il appréhende des réalités techniques multiples et complexes qui ont un impact direct sur les qualifications et les régimes juridiques.

À l'exception du rapport pour la proposition de résolution du Parlement européen contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, dont madame Mady Delvaux est la rapporteuse, la régulation positive actuelle aux niveaux européen et français est essentiellement basée sur un objet technique appréhendé sous le terme de machine.

Sur le plan juridique, la définition de la machine est issue de la directive 2006/42/CE du 17 mai 2006 et modifiant la directive 95/16/CE (refonte) ; elle y est définie comme un « *ensemble équipé ou destiné à être équipé d'un système d'entraînement autre que la force humaine ou animale appliquée directement, composé de pièces ou d'organes liés entre eux dont au moins un est mobile et qui sont réunis de façon solidaire en vue d'une application définie* ».

L'élément le plus discriminant de cette définition est la capacité de la machine à réaliser une application définie.

À l'exception de la proposition de classification des robots intelligents proposée en annexe du rapport de Mady Delvaux, le terme robot lui-même ne fait, à notre connaissance, aux niveaux européen et français, l'objet d'aucune définition juridique, cette difficulté ayant d'ailleurs été relevée dans ledit rapport.

Pour disposer d'une première définition technique, il faut se référer uniquement à la norme ISO 8373:2012 dans laquelle le robot est défini comme un « *mécanisme programmable actionné sur au moins deux axes avec un degré d'autonomie, se déplaçant dans un environnement pour exécuter les tâches prévues* ». L'élément discriminant de cette définition est l'autonomie. En fonction des capteurs, du *hardware* et du *software* et de l'intelligence artificielle (forte ou non), le robot décide des actions à exécuter pour atteindre les objectifs qui lui ont été assignés, en interprétant les données collectées à partir des capteurs ou actionneurs et en fonction d'une capacité d'apprentissage supervisée ou non par l'humain.

Il en est de même de l'absence de définition juridique relative à la notion d'intelligence artificielle. Seule la norme ISO 2382-28 définit l'expression intelligence artificielle comme la « *capacité d'une unité fonctionnelle à exécuter des fonctions généralement associées à l'intelligence humaine, telles que le raisonnement et l'apprentissage* ».

L'expression « *unité fonctionnelle* » est elle-même décrite dans la norme ISO/IEC 2382-2015 comme une « *entité de matériel ou de logiciel, ou les deux, capable d'accomplir un but précis* ». Le discriminant majeur de la définition de l'intelligence artificielle dans cette norme réside dans la capacité d'exécution de fonctions associées à l'intelligence humaine, ces deux fonctions étant le raisonnement mais surtout la capacité d'apprentissage, cette capacité pouvant être supervisée entièrement par l'homme ou réalisée sans aucune supervision de l'homme.

(1) CERNA - Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene [http://cerna-ethics-allistene.org/digitalAssets/38/38704_Avis_robotique_livret.pdf]

Seule la CERNA¹ avait défini le robot comme « *une machine mettant en œuvre et intégrant :*

- *des capacités d'acquisition de données avec des capteurs à même de détecter et d'enregistrer des signaux physiques ;*
- *des capacités d'interprétation des données acquises permettant de produire des connaissances ;*
- *des capacités de décision qui, partant des données ou des connaissances, déterminent et planifient des actions. Ces actions sont destinées à réaliser des objectifs fournis le plus souvent par un être humain, mais qui peuvent aussi être déterminés par le robot lui-même, éventuellement en réaction à des événements ;*

– des capacités d'exécution d'actions dans le monde physique à travers des actionneurs, ou à travers des interfaces ».

La régulation positive européenne et française existante ne définit pas ce qu'est un robot autonome disposant d'une capacité d'apprentissage (notamment lorsqu'il est sans aucune supervision humaine) et dont les actions ou omissions pourraient porter atteinte aux personnes ou aux biens.

Or, du fait du couplage de la robotique à l'intelligence artificielle et à une algorithmique forte, notre droit positif semble à l'avenir démuné pour appréhender le robot disposant d'un fort degré d'autonomie et d'une capacité à exécuter des fonctions associées à l'intelligence humaine, que sont le raisonnement et la capacité d'apprentissage, surtout si l'on considère la phase d'exploitation où le système robotique dispose d'une capacité d'apprentissage non supervisée par l'humain.

Les questions juridiques de l'application de l'intelligence artificielle forte à la robotique

Le juriste comme le législateur se doivent d'être les mieux informés des innovations afin de préparer et d'anticiper les ruptures technologiques et les transformations pouvant impacter le monde de l'entreprise comme le citoyen.

Les enjeux actuels pour le législateur et pour le juriste sont de comprendre les implications réglementaires ou éthiques potentielles de l'application de l'intelligence artificielle forte à la robotique afin d'apprécier la portée du droit positif, et pour le régulateur, d'éviter d'adopter une législation obsolète.

Pour une réglementation créative, collaborative et contributive en robotique

Dans de nombreux domaines technologiques, le législateur est parfois démuné face à ces évolutions. De ce fait, l'absence d'une régulation élaborée de manière collaborative, associant l'ensemble des expertises nécessaires à la compréhension non seulement des enjeux, empêche de pouvoir se projeter avec une certaine anticipation sur l'évolution des technologies.

À cet égard, le travail de décryptage et de réflexion, qui a été initié par un cycle de

débats de France Stratégie² sur les questions éthiques soulevées par la robotique ainsi que par les débats

(2) France Stratégie
[<http://www.strategie.gouv.fr/evenements/place-robots-societe>]

(3) Les robots et la loi
[<http://www.senat.fr/notice-rapport/2015/r15-570-notice.html>]

conduits sous l'autorité de l'Office d'évaluation parlementaire des choix scientifiques et technologiques (OPECST)³, est primordial. L'OPECST était d'ailleurs pleinement dans son rôle en tentant d'anticiper les évolutions scientifiques et technologiques prévisibles

pour concilier l'émergence, accélérée et souvent imprévisible, des robots assortis d'impératifs individuels, sociaux ou économiques. Ces débats et réflexions associées ont surtout concerné les robots dits humanoïdes et les robots qualifiés de compagnie. Ce travail se prolonge actuellement et devrait déboucher sur une approche globale, systémique et interdisciplinaire de l'intelligence artificielle, notamment appliquée à la robotique.

Avec le développement de celle-ci, les questions juridiques mais également éthiques soulevées par l'application de l'intelligence artificielle forte à la robotique sont et seront nombreuses. Il est essentiel que le législateur et les autorités européennes puissent réfléchir avec anticipation à l'activité de réglementation de ce domaine.

Des juristes se sont déjà prononcés dans le cadre de publications sur les questions juridiques relatives à des robots intelligents ou cognitifs. La communauté des juristes est elle-même partagée, entre ceux qui défendent la plasticité du droit positif et qui préconisent de n'y toucher

(4) Selon l'expression de Montesquieu

que « *d'une main tremblante* »⁴ et ceux

qui considèrent, par exemple, que la capacité du droit de la responsabilité à bien régir les situations résultant du couplage entre la robotique et l'IA est en train de se dégrader. Les premiers considèrent le plus souvent que les règles

de droit existantes sont parfaitement en mesure d'appréhender l'ensemble des questions juridiques soulevées par les robots qualifiés d'intelligents et, en matière de responsabilité civile, mettent en exergue le caractère particulièrement accueillant des principes suivants :

- « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer* » ;

- « *Chacun est responsable du dommage qu'il a causé non seulement de son fait, mais encore par sa négligence ou son imprudence* » ;

- « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde* ».

Les seconds considèrent, à l'inverse, soit que le droit commun de la responsabilité est mal adapté, soit qu'une forme

(5) Pour approfondir sur la question de l'autorégulation, voir notamment : Ryan Calo, *Open Robotics*, 70 *Maryland Law Review* 571 (2011) ; Me Jérémie Bensoussan, *Droit des robots*, <http://blogs.economie.gouv.fr/les-cafes-economiques-de-bercy/droit-des-robots-bensoussan/>

d'autorégulation⁵ pourrait être mise en œuvre pour les robots dits intelligents. C'est le cas notamment aux États-Unis et en Corée du Sud où des

propositions sont formulées pour établir des chartes du droit des robots.

Certains, à l'instar de l'initiative portée par le professeur de droit Ryan Calo, militent

pour la création d'une Agence fédérale de la robotique, une autorité européenne qui permettrait de développer des regards croisés et de réunir des roboticiens, mais aussi des experts, des industriels, des éthiciens et des juristes afin que le droit positif actuel soit rapidement adapté pour répondre aux nouveaux enjeux et défis de l'application de l'intelligence artificielle à la robotique.

L'avancée fulgurante de l'intelligence artificielle appliquée à la robotique, le développement des technologies cognitives et de l'algorithmique modifient les frontières disciplinaires entre sciences, technologies et droit. Conscients de cette modification des frontières, des industriels avisés travaillent également activement à mettre au point des normes internationales ou européennes afin de les défendre auprès des législateurs nationaux ou européens.

À la recherche d'un statut et d'un régime de responsabilité pour le robot autonome et de sa capacité d'apprentissage supervisée ou non par l'humain

S'interroger sur le statut et le régime de responsabilité "le plus adapté" au robot, disposant d'une autonomie décisionnelle forte et d'une capacité d'apprentissage pouvant être à un certain stade non supervisée par l'humain, implique de bien connaître l'état de l'art des technologies.

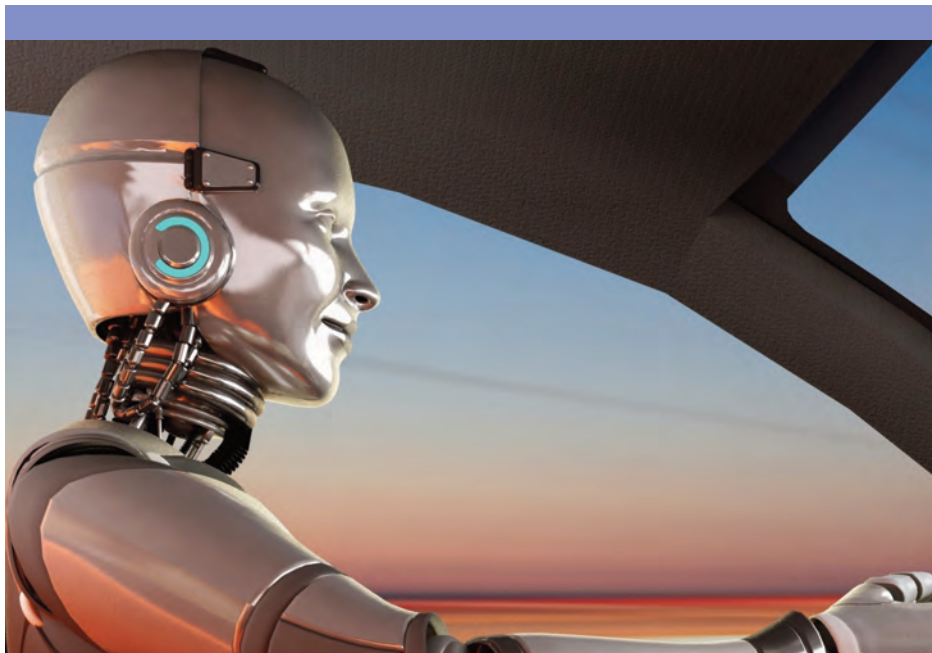
Il est nécessaire de repenser la législation en vigueur, sans chercher à identifier et

cartographier tous les risques, pour réguler l'application de l'intelligence artificielle forte à la robotique sans attendre qu'une nouvelle application de l'IA à la robotique entraîne des conflits.

L'intelligence artificielle appliquée à la robotique doit être confrontée au droit et en particulier aux différents régimes de responsabilité.

Prenons quelques exemples. Le premier exemple est celui de deux réseaux de neurones, du programme Google Brain, dénommés respectivement Alice et Bob, qui ont été capables, au terme d'échanges de nombreux messages, de créer leur propre algorithme de chiffrement, pour sécuriser leurs messages. Cet algorithme s'est avéré indéchiffrable par un troisième réseau de neurone, dénommé Eve, ainsi que par l'humain. L'utilisation des capacités des réseaux neuronaux devrait demain s'étendre à de nombreux domaines d'applications industrielles.

Qui serait demain le responsable dans le cas d'un usage malveillant d'un tel système sur des systèmes d'information ? L'entité utilisatrice du (des) réseau(x) de neurones pour une application donnée, les concepteurs des réseaux de neurones, les concepteurs des moteurs algorithmiques ou encore les trois entités au prorata de leur contribution à la réalisation du dommage ? Qui pourrait être considéré comme le gardien des



Un statut et d'un régime de responsabilité pour le robot autonome doté d'une capacité d'apprentissage supervisée ou non par l'humain.

réseaux de neurones, si la capacité d'apprentissage dépasse celle de l'humain et n'est plus supervisée par lui au moment de la réalisation du dommage ?

Notre second exemple se déroule en avril 2016 : un réseau de neurones en *deep learning* et des algorithmes ont été utilisés pour analyser l'ensemble des œuvres de

Rembrandt et plus particulièrement les portraits dans les œuvres du maître. Dans un second temps, moyennant l'utilisation d'une imprimante 3D, il a été possible de réaliser un « nouveau Rembrandt ».

Dans le cas de l'utilisation d'un réseau identique sur une œuvre qui ne serait pas tombée dans le domaine public, qui pourrait être reconnu en tant qu'auteur

d'une œuvre conçu comme ce « *nouveau Rembrandt* » ? Le créateur concepteur du modèle de *deep learning*, le ou les créateurs des algorithmes, la société qui aurait commandé la réalisation d'une

(6) Interface de programmation (API)

œuvre à un prestataire ayant réalisé l'API⁶ de

reconnaisances des caractéristiques de l'œuvre d'un artiste ? Les trois ensembles si l'on considère qu'il s'agit d'une œuvre collective autonome produite par une intelligence artificielle ?

Très récemment, le Pentagone a également annoncé avoir testé avec succès l'utilisation de microdrones, dénommés *Perdrix*, mesurant 16 centimètres, dotés d'une intelligence artificielle collective (I.A.C), travaillant ensemble pour réaliser des actions en groupe et capables de s'adapter à un panel de situations. En l'espèce, le test réalisé par le Pentagone en Californie en octobre 2016 a concerné pas moins de 103 microdrones *Perdrix*, largués par trois jets. Pour le Pentagone, grâce à cet IA collective, les microdrones ont « *montré des comportements collectifs avancés, comme par exemple dans leur prise de décision, dans leurs changements de formations de vol et dans leur processus d'auto-réparation* ». Pour le responsable du bureau de l'innovation au Pentagone, les microdrones *Perdrix* travaillant ensemble sont « *un organisme collectif* » qui « *partage une intelligence en commun*

pour la prise de décisions et d'adaptation » à l'image d'un essaim naturel. Cet exemple de l'application de l'intelligence artificielle collective à la robotique concerne la robotique militaire. Toutefois, des microdrones comparables aux microdrones *Perdrix* pourraient parfaitement être utilisés demain dans le domaine civil, pour l'exploitation des prises de décisions de l'IA collective. Demain, le recours à une intelligence artificielle collective pourra se développer en dehors du champ militaire.

Qui sera alors responsable si un même essaim de microdrones dans le domaine civil prenait une décision pouvant porter atteinte à une personne ou à un bien ? Le concepteur des microdrones, le fabricant du système de communication entre les microdrones, le développeur des modèles de *deep learning* ou des annotateurs, l'entité utilisatrice des microdrones lors de la survenance du fait générateur du dommage ?

Enfin, considérons le cas d'un professionnel de santé utilisant *Watson* pour analyser les informations du dossier d'un patient, pour obtenir une analyse des études de cohortes ou encore pour proposer des stratégies thérapeutiques : le professionnel de santé aura-t-il toujours, face à son patient, le dernier mot lors du diagnostic ?

Demain, les robots utiliseront de plus en plus de briques logicielles

d'apprentissage machine (*deep learning*) agissant directement sur les volumes de données traitées et l'impact sur les prises de décisions humaines augmentera.

Les situations où l'intelligence artificielle forte appliquée à la robotique pourrait surpasser l'humain, grâce notamment aux réseaux de neurones et à l'algorithmique, ont vocation à se multiplier avec, en ligne de mire, le point de la singularité juridique.

Vers de futures règles juridiques européennes de droit en robotique

Les députés européens demandent la mise en place d'un cadre juridique communautaire adapté aux robots intelligents. Le rapport de la Commission juridique (JURI) de la Commission européenne a été adopté très récemment (le 12 janvier 2017) par un vote de la

(7) Commission JURI, Commission européenne ; Mady Delvaux : « Un cadre légal en matière de robotique est nécessaire » - <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BBPE-582.443%2B01%2BDOC%2BPDF%2BVO//FR>

(8) Association du Droit des Robots (ADDR) - <https://www.association-droit-robot.fr/>

Commission juridique en première lecture⁷.

La Commission parlementaire du Parlement européen devrait se prononcer en séance plénière à partir du 13 février

2017 sur cette procédure d'initiative législative.

Maître Alain Bensoussan, qui a fondé l'Association du droit des robots (ADDR)⁸, s'est prononcé en faveur de l'adoption d'une personnalité juridique singulière

dont pourraient être dotés les robots intelligents⁹ en précisant que « *La personnalité morale est une pure construction juridique conçue pour répondre à des nécessités pratiques et*

(9) A. Bensoussan, « Les robots ont-ils une personnalité ? », Planète Robots, n° 19, janvier-février 2013. Blog Le Figaro Droit des technologies avancées, Alain Bensoussan, « La personnalité robot », <http://blog.lefigaro.fr/bensoussan/2015/02/la-personnalite-robot.html>

(10) Blog Le Figaro Droit des technologies avancées, Alain Bensoussan, « La personnalité robot », <http://blog.lefigaro.fr/bensoussan/2015/02/la-personnalite-robot.html>

faire accéder à la vie juridique des structures qui n'ont pas d'existence corporelle ou physique comme les sociétés commerciales, les associations ou les syndicats professionnels. Ces

entités ne sont pas dotées d'émotions, mais sont responsables pénalement et civilement des actes commis par leurs dirigeants car elles sont dotées d'une personnalité juridique »¹⁰.

La roboéthique

Les robots sont conçus pour créer de la richesse et améliorer la qualité de vie de l'humain. Les innovations déjà issues d'intelligence artificielle appliquée à la robotique irrigueront la société de manière massive et parfois inattendue.

La prise en considération des questions éthiques dès la conception

Avec l'application de l'intelligence artificielle à la robotique, les questions éthiques sont à prendre en considération dès la phase de conception du système robot-IA, afin que « *la confiance que l'on peut placer dans un robot, les possibilités et limites de celui-ci et du couple qu'il forme avec l'utilisateur, la reprise en main,*

(11) Rapport de la Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene (CERNA). Rapport accessible sur <http://cerna-ethics-allistene.org>

le traçage »¹¹

puissent permettre de rendre compte du comportement du système.

Lorsque le robot entre en interaction directe avec l'humain, il est indispensable et nécessaire que les utilisateurs puissent avoir confiance en lui.

Le questionnement sur la roboéthique est en lui-même différent du questionnement sur l'éthique du robot, qui impose aux robots de respecter des règles éthiques. Celles du robot sont à l'état de concept théorique, dans la mesure où elles impliqueraient que les robots disposant d'une autonomie soient en mesure de prendre des décisions se rapprochant de

la morale. La roboéthique implique pour les roboticiens, dès la phase de conception, d'essayer d'empêcher un déficit de confiance de l'utilisateur, mais également celle d'une confiance trop aveugle dans le robot.

Les règles ou instructions éthiques du robot qui pourront être codées afin d'encadrer le comportement du robot sont complexes à modéliser et à résoudre et *a fortiori* à intégrer dans le robot. Le faut-il et les roboticiens et programmeurs le peuvent-ils en l'état de la maturité technologique ? Roboticiens, fabricants, éthiciens le souhaitent-ils et ont-ils la même vision de l'éthique appliquée au couple robot-IA ?

La voiture autonome est probablement l'exemple le plus symptomatique de la difficulté à poser des équations sur l'éthique du robot, si nous laissons de côté volontairement la robotique militaire et en particulier les systèmes d'armes létaux autonomes, ainsi que les drones. Le concepteur et fabricant du véhicule autonome doit faire en sorte que les décisions du véhicule autonome ne soient pas prises à l'insu de l'opérateur afin de ne pas créer de ruptures dans sa compréhension de la situation (c'est-à-dire afin que l'opérateur ne croie pas que le robot est dans un certain état alors qu'il est dans un autre, c'est à dire, la perception par l'opérateur de l'état réel du robot).

En matière d'éthique, il est fondamental de définir le comportement du robot en situation critique. Prenons l'exemple bien connu du véhicule autonome et du scénario dans lequel un dilemme social se pose et qu'il doit être déterminé par algorithme, l'équation à mettre en œuvre consistant soit à éviter un piéton soit à sacrifier les occupants du véhicule autonome.

Ce scénario pourrait paraître abstrait voire totalement artificiel. Deux roboticiens et chercheurs soutiennent des positions antagonistes. Pour Azim Shariff¹², Jean-

François Bonnefon et Iyad Rahwan¹³ de l'Université de l'Oregon « (...) « ces expériences de pensée philosophique pourraient devenir concrètes, car elles correspondent à des décisions qu'auront à prendre les véhicules autonomes ». Mais ils considèrent que si une régulation pourrait être

nécessaire, elle pourrait également être contre-productive.

Pour Jean-Gabriel Ganascia¹⁴, une schématisation des dilemmes sociaux est discutable du point de vue éthique au

motif que « (...) la seule somme des différents maux schématise trop la situation et engendre des débats infinis. Faut-il tenir compte de l'âge des personnes, du fait qu'elles avaient ou non le droit d'être à cet endroit sur la route ». Ce dernier considère qu'une telle schématisation conduirait à des calculs sans fin.

Nos lecteurs pourront à leur tour se faire leur propre vision des dilemmes sociaux posés par le véhicule autonome sur la plateforme en ligne MORAL MACHINE (<http://moralmachine.mit.edu/hl/fr>), plateforme créée spécifiquement pour compiler les différentes perspectives humaines sur les décisions morales et éthiques prises par les voitures autonomes.

Le cadre éthique de la proposition de résolution européenne

La proposition de résolution de la Commission JURI du Parlement européen propose un cadre éthique pour la conception, la fabrication et l'utilisation des robots, justifié par l'évolution des technologies robotiques et de

l'intelligence artificielle¹⁵. Le rapport comporte même en annexe un projet de charte

instaurant un code de conduite pour les ingénieurs en robotique et un code de déontologie pour les comités d'éthique de

(12) Azim Shariff est psychologue. Il traite cette question dans la revue Science, connue depuis 1967, sous le nom du dilemme du chauffeur de trolley.

(13) Jean-François Bonnefon, Azim Shariff et Iyad Rahwan, « The social dilemma of autonomous vehicles », Science, vol. CCCLII, n° 6293, 24 juin 2016.

(14) Jean-Gabriel Ganascia, expert en intelligence artificielle, apprentissage machine, découverte scientifique, sciences cognitives, philosophie computationnelle et éthique des nouvelles technologies [http://www.upmc.fr/fr/salle_de_presse/repertoire_d_experts/vous_cherchez_un_expert/pole_1/jean_gabriel_ganascia.html]

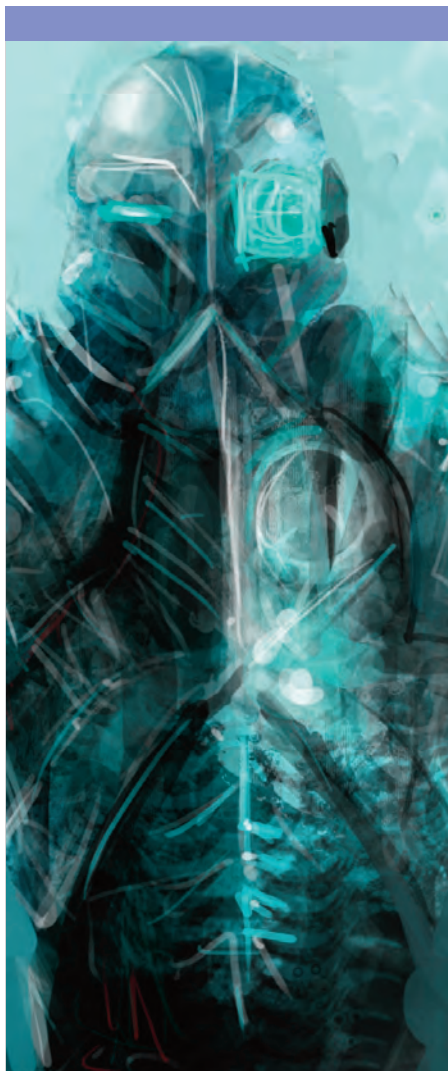
(15) Commission JURI, Commission européenne ; Mady Delvaux : « Un cadre légal en matière de robotique est nécessaire » <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=->

la recherche ainsi qu'un ensemble de licences-type pour les concepteurs et utilisateurs.

Dans son approche, le cadre éthique proposé par la Commission JURI est basé sur l'examen des avantages et des risques liés à la sécurité, à la vie privée, à l'intégrité, à la dignité, à l'autonomie et à la propriété des données.

Le cadre éthique proposé par la proposition de résolution du Parlement européen est basé sur les 9 principes éthiques suivants :

- Protéger les êtres humains contre les atteintes causées par un robot ;
- Droit pour une personne d'être prise en charge par un robot ;
- Respect de la liberté d'une personne lors de la mise en œuvre du robot ;
- Protéger la vie privée d'une personne contre une atteinte par un robot ;
- Protéger les données à caractère personnel ;
- Protéger l'homme contre les risques d'instrumentalisation par le robot ;
- Eviter la rupture du lien social en présence de robot ;
- Assurer une égalité d'accès au progrès de la robotique ;
- Restreindre l'accès de l'homme aux technologies augmentatives.



Fotolia Dusan Kosche

Le Parlement européen se prononce pour un cadre éthique de la conception et du spectre d'usage du robot.

On peut retenir de cette énonciation quelques conclusions.

L'intelligence artificielle appliquée à la robotique – lorsque la capacité d'apprentissage n'est plus supervisée par l'humain et permet au système robot-IA de disposer d'une très grande autonomie décisionnelle – pose des problématiques nouvelles sur le plan juridique et éthique. Les systèmes technologiques les plus avancés ne sont incontestablement pas appréhendés en tant qu'objet technique par notre droit positif.

L'intelligence artificielle forte appliquée à la robotique pourra permettre la création de nouvelles applications et rendre de très nombreux services, qui n'existent pas nécessairement aujourd'hui et qui n'ont pas été encore imaginés. L'intelligence artificielle appliquée à la robotique, associée aux technologies cognitives, pourrait comme toute technologie être mal utilisée par l'humain et entraîner, par action ou par abstention, des dommages.

Le développement de l'intelligence artificielle et son application à la robotique sont aujourd'hui une réalité et ne relèvent pas d'un futur lointain. Pour appréhender réellement ses réalités technologiques, le droit en vigueur se trouve partiellement inadapté ou démuné. Le droit en vigueur ne pourra trouver à s'appliquer que s'il est fortement complété par des réponses juridiques et spécifiques tenant compte

des spécificités de l'intelligence artificielle et de la robotique.

Sur le plan européen, la proposition de résolution du Parlement européen, contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, stipule que, quelle que soit la solution juridique choisie en matière de responsabilité des robots dans les cas autres que des dommages matériels, ledit instrument ne devrait en aucune manière limiter le type ou l'étendue des dommages qui peuvent faire l'objet d'un dédommagement et ne devrait pas non plus limiter la nature de ce dédommagement. Avec le développement fulgurant de l'intelligence artificielle et de la robotique, un nouveau champ disciplinaire s'inscrit sous le terme de « roboéthique ». La proposition de résolution du Parlement européen propose également un cadre éthique de la conception à l'utilisation des robots.

Contrôle routier des voitures

connectées : quel nouveau paradigme dans les règles d'engagement coercitives des forces de sécurité publique

par **JÉRÔME LAGASSE**

L

Le contenu de l'article de Maître Didier Gazagne dresse une analyse prospective sur les opportunités que la technologie est susceptible d'offrir à moyen et long terme dans la réalisation des missions quotidiennes confiées aux forces de sécurité intérieure. Il apporte de surcroît un éclairage sur les prises de position de la Cour suprême des États-Unis d'Amérique dans le domaine des libertés individuelles et du droit de propriété notamment par l'évolution jurisprudentielle du 4^e amendement de la Constitution.



JÉRÔME LAGASSE

Chef d'escadron, centre de recherche de l'école des officiers de la gendarmerie nationale

Une des questions essentielles soulevées dans cette première partie concerne notamment la place de la voiture autonome vis-à-vis de son

environnement. Autrement dit, ce moyen de locomotion sera-t-il interconnecté ou

(1) Cf § 1.3 – Typologie des voitures autonomes et flux de communication.

(2) Pour une étude des algorithmes prédictifs dans le champ de la sécurité publique : Rand Corporation, Research report, Predictive policing – The rôle of crime forecasting in law enforcement operations [Prévision policière – le rôle de la prévision du crime dans les opérations policières], 2014, 155. P

http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND-RR233.pdf

non à un réseau commun¹ ? En fonction des options qui seront retenues par les autorités de régulation, il découlera nécessairement des conséquences sur la manière dont les forces de l'ordre accompliront leurs

missions traditionnelles. En effet, les flux de données générés par les différentes applications provenant d'une voiture connectée seront collectés et stockés dans de puissants centres informatiques (*data center*) en vue d'une exploitation optimale à l'aide d'algorithmes prédictifs². En termes de sécurité publique, un débat s'ouvrira pour s'interroger sur les conditions de captation de ces données



« nous sommes sur le point d'assister à l'effacement progressif du conducteur à bord d'une automobile thermique en lieu et place d'une voiture autonome voire indépendante, électrique, pilotée par une intelligence artificielle »

dans un segment qui impacte les libertés individuelles. Avec quels objectifs et pour quelles finalités les agents de la force publique pourraient-ils être autorisés à capter certaines données avec, par exemple, la faculté de les agréger ?

Dans la lignée de ce qui précède, un

(3) www.rand.org/t/rr928. Cf P.20 « Controlling automated vehicles : Need methods for control and manipulation of automated vehicles (when warranted). For example, law enforcement may want to direct a parked vehicle to move. »

www.slate.fr/story/106141/police-autorisee-prendre-contrôle-voitures-sans-conducteur

récent³ rapport publié par le laboratoire d'idées (*think tank*) Rand Corporation intitulé "L'avenir des nouvelles technologies et de la justice pénale"

soulève un certain nombre de problématiques dont l'une est de savoir si la police devrait être en mesure de

prendre ou non le contrôle d'une voiture autonome. Extrait et traduit du présent rapport, le scénario ci-dessous tend à appeler l'attention sur le fait que nous assistons subrepticement à un changement de paradigme dans les politiques de sécurité publique dont l'anticipation et la prédiction seront les noyaux. Ce changement dont toutes les conséquences n'ont pas été encore totalement identifiées, se manifeste entre autres à travers le vecteur dominant de la mobilité : la voiture.

« *L'agent de police Rodriguez régulant la circulation depuis l'intersection pouvait voir la voiture se dirigeant vers lui et son occupant regarder son ordiphone. L'agent fit signe alors à la voiture sans conducteur de s'arrêter, celle-ci roula vers*

l'emplacement situé derrière le passage pour piétons.

L'agent guidait cette voiture alors que le passager indifférent continuait de consulter sa messagerie électronique. Cependant, ce dernier n'allait pas rester indifférent très longtemps. Un conducteur au volant d'un véhicule utilitaire sport franchit l'intersection, obligeant l'agent à se jeter au sol et la voiture indépendante à freiner brusquement pour s'écarter et éviter ainsi une collision.

Pendant que l'agent Rodriguez appelait du renfort, un véhicule aérien motorisé (drone) identifia en excès de vitesse le véhicule utilitaire sport et le prit en chasse tout en transmettant son itinéraire aux véhicules en patrouille. Quelques minutes plus tard, par une manœuvre technique précise d'immobilisation, le véhicule utilitaire sport était contraint de s'arrêter sur le bas-côté.

Alors que les agents grouillaient autour du véhicule, dans le feu de l'action, l'un d'eux prit une photo de l'individu, la téléchargea pour la comparer au fichier national des clichés anthropométriques. La demande de comparaison fit l'objet rapidement d'un retour positif.

La photographie recoupée avec la plaque d'immatriculation et la description du véhicule, aida le système à identifier un ancien détenu qui en lien avec son propre véhicule utilitaire sport avait un long casier judiciaire pour vols à main armée et

conduites dangereuses.

Quelques instants après, la radio des forces de police rendait compte d'un vol à main armée dans une station-service située à proximité. Les photos de surveillance prises depuis les lieux des faits, montrant le conducteur du véhicule utilitaire de sport braquant une arme sur l'employé de la station de carburant, arrivèrent peu après que le suspect ait été placé en garde à vue – Première étape d'une probable détention beaucoup plus longue. »⁴

(4) Rand Corporation, Research report Using future internet technologies to strengthen criminal justice [l'utilisation des technologies de l'internet du futur pour renforcer la justice pénale] P.3 – www.rand.org/t/rr928 - 2015

Ce récit élaboré sous forme d'un cas concret décrit dans une fiction proche de la réalité la période de transition que nous serions susceptibles de connaître prochainement. À l'instar du siècle dernier qui a vu disparaître la traction hippomobile au profit du moteur à explosion, nous sommes sur le point d'assister à l'effacement progressif du conducteur à bord d'une automobile thermique en lieu et place d'une voiture autonome voire indépendante, électrique, pilotée par une intelligence artificielle. L'issue du scénario imaginé par les auteurs de ce rapport semble nous annoncer en filigrane la fin des bandits de grand chemin grâce aux potentialités des nouvelles technologies de l'information et de la communication. Pour autant, le défi en termes de cybersécurité est immense : d'un côté il s'agira de garantir aux futurs

acheteurs l'intégrité de l'architecture du système d'information intelligent

(5) Terme retenu par la Commission générale de terminologie et de néologie – Avis, JO 16031999 – Défini comme une « personne passionnée d'informatique qui, par jeu, curiosité, défi personnel ou par souci de notoriété, sonde, au hasard plutôt qu'à l'aide de manuels techniques, les possibilités matérielles et logicielles des systèmes informatiques afin de pouvoir éventuellement s'y immiscer. »

(6) Terme retenu par la Commission générale de terminologie et de néologie – Avis, JO 16031999 – Défini comme une « personne qui contourne ou détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique. »

embarqué contre des fouineurs⁵ (hackers) ou des pirates⁶ informatiques (crackers), de l'autre concevoir en toute légalité des dispositifs techniques capables, sous le contrôle d'un juge, de prendre le contrôle d'une

voiture intelligente en l'absence du consentement de son propriétaire ou de tout utilisateur. Ceci induirait que seules les industries dotées d'un agrément délivré par une autorité de régulation et de contrôle comme l'ANSSI seraient autorisées à mettre sur le marché au profit de certains industriels les équipements et logiciels destinés à prendre le contrôle d'un système de traitement automatisé de données embarqué dans un véhicule.

La traversée des États-Unis d'Amérique par voie routière d'une voiture autonome de la côte Est à la côte Ouest sur une distance de 5 600 km sans incident

(7) www.largus.fr/actualite-automobile/voiture-autonome-delphi-reussit-sa-traversee-des-etats-unis-6104387.html

majeur⁸, constitue les premiers balbutiements d'un scénario fiction

évoqué *supra*. Dès à présent, il est

légitime de s'interroger sur les moyens et les fondements juridiques par lesquels un agent de la force publique, muni des insignes extérieurs et apparents de sa qualité, pourra être en mesure d'accomplir de manière efficiente toutes les missions de sécurité publique et routière au sein d'un environnement qui sera progressivement dominé par les voitures connectées (autonome ou indépendante c-à-d sans conducteur). Il s'agira de s'interroger notamment pour savoir si les futurs modèles de voitures connectées mises sur le marché grand public auront une fonctionnalité implémentée dès la conception de ceux-ci pour permettre aux forces de l'ordre d'en prendre le contrôle à distance et contraindre, si nécessaire, les passagers à s'arrêter où à être déroutés sur le poste de police le plus proche. L'avènement de ce scénario volontairement futuriste soulèverait inexorablement des questions sociétales majeures notamment vis-à-vis de l'évolution du principe à valeur constitutionnelle qu'est la liberté d'aller et

(8) Cf : art 2 de la Déclaration des droits de l'homme et du citoyen, article 66 de la Constitution.

de venir⁸. La voiture connectée pourrait être ce premier vecteur majeur susceptible d'impacter les politiques de sécurité publique. La mission de contrôle des flux constitue l'expression même de la capacité d'un État à assurer la maîtrise de son territoire. Le véhicule thermique et demain le véhicule connecté constituent tour à tour le vecteur privilégié de la



« Il s'agira de s'interroger notamment si les futurs modèles de voitures connectées mises sur le marché grand public auront une fonctionnalité implémentée dès la conception de ceux-ci pour permettre aux forces de l'ordre d'en prendre le contrôle à distance. »

mobilité des délinquants et des trafics qui y sont associés. Les forces de l'ordre sont exposées quotidiennement à des risques lorsqu'il s'agit d'intercepter des individus auteurs d'infractions qualifiées de crime ou de délit.

Notre approche débutera par un état des lieux juridiques concernant les conditions d'usage de moyens coercitifs à disposition des forces de l'ordre adaptés aux circonstances actuelles. Le contexte de l'état d'urgence a amené le législateur à harmoniser le régime juridique de l'usage des armes des forces de sécurité intérieure et, en fonction du cadre d'emploi des forces armées engagées sur le territoire national. Ce rappel effectué, il s'agira par la suite de mettre en exergue la nature des risques actuellement encourus par les personnels de la

gendarmerie, de la police et des douanes en mettant en évidence, chiffres à l'appui, la part imputable à l'automobile dans la réalisation des atteintes physiques à l'encontre de ces derniers. La mise en corrélation de ces deux thématiques a pour objet principal de souligner le nombre élevé d'agents victimes d'une agression par l'usage d'une voiture comme arme par destination. Ce constat mis en évidence devrait inciter à envisager au plus tôt, en liaison avec tous les acteurs institutionnels et privés concernés, les conditions des modalités juridiques et techniques de déploiement, au profit des forces de l'ordre, de dispositifs techniques numériques d'interception ou d'immobilisation des futurs modèles de voitures connectées homologuées. Sur le plan juridique, nous pourrions assister à un retour en force de

la notion fondamentale en droit français qui distingue la police administrative et la police judiciaire. Cette construction juridique, directement issue du principe constitutionnel de la séparation des pouvoirs, pourrait servir de base à

(9) Loi du 24 juillet 2015 – JORF du 26 juillet 2015 – p.12735

(10) Art 8.1 de la convention de Vienne « Tout véhicule en mouvement ou tout ensemble de véhicules en mouvement doit avoir un conducteur », disposition transposée à l'article R412-6 du code de la Route.

Nota : Cette convention fait l'objet d'une procédure de révision pour intégrer dans l'ordre juridique international la voiture connectée.
<https://treaties.un.org/doc/Publication/CN/2015/CN.529.2015.Reissued.06102015-Eng.pdf>
www.unecp.org/fr/info/media/presscurrent-press-h/transport/2016/unece-paves-the-way-for-automated-driving-by-updating-un-international-convention/la-unece-ouvre-la-voie-a-la-conduite-automatisee-en-modifiant-la-convention-de-vienne-sur-la-circulation-routiere.html

l'élaboration d'un régime propre à la voiture connectée à l'instar de la loi sur le renseignement⁹.

Cette analyse se terminera par les réflexions et propositions formulées par une commission de pénalistes et d'experts en nouvelles technologies recueillies et diffusées grâce au soutien du

laboratoire d'idées américain (*think tank*) *Rand Corporation*.

Un cadre juridique qui autorise le recours à la force armée.

À l'heure actuelle, la convention de Vienne¹⁰ prévoit de manière explicite que tout véhicule en circulation doit avoir un conducteur, c'est-à-dire une personne physique qui a, selon la notion du code civil, la qualité de gardien : direction,

(11) Arrêt Franck, Cassation, Ch réunies, 2 décembre 1941
www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000006953144&fastReqId=966555347&fastPos=1

(12) Cf Art. L233-1-I Code de la route : « Le fait pour tout conducteur d'omettre d'obtempérer à une sommation de s'arrêter émanant d'un fonctionnaire ou agent chargé de constater les infractions et muni des signes extérieurs et apparents de sa qualité est puni de trois mois d'emprisonnement et de 3750 euros d'amende. »

autorité et contrôle de la chose¹¹.

Cependant, prenant acte de l'évolution des voitures à délégation de conduite, la Commission économique des Nations-Unies pour l'Europe autorise, depuis le 23 mars 2016, les systèmes

automatisés sur les routes, sous réserve qu'ils ne soient pas en contradiction avec les règlements des Nations-Unies sur les véhicules et qu'ils puissent être contrôlés voire désactivés par le conducteur.

Ce même conducteur, lorsqu'il omet d'obtempérer à une sommation de s'arrêter, dispose actuellement de son libre-arbitre. Il doit répondre de la responsabilité de ses actes devant les tribunaux¹² en cas de manquement. Dans les situations où s'exprime un refus d'obtempérer manifeste, les agents de la force publique disposent de tout un corpus juridique qui les autorise à recourir à l'emploi de moyens contraignants pour obliger le conducteur à arrêter son véhicule.

Un cadre juridique harmonisé

Le contexte.

Les derniers attentats de Paris ont orienté le législateur vers l'adoption d'un article spécifique inséré dans le code de la sécurité intérieure afin que les agents de la force publique disposent d'un cadre juridique adapté pour faire face, entre autres, à des situations de type tuerie de masse. Dans ce champ, l'attentat de Nice, commis le 14 juillet 2016, à l'aide d'un camion, souligne le rôle prédominant du véhicule comme vecteur privilégié dans la commission d'un crime.

La loi n°2017-258 du 28 février 2017 harmonise le régime juridique de l'usage des armes des différentes composantes de la force publique. Malgré les réserves

(13) Pour le Défenseur des droits, le nouveau régime d'usage des armes est « ...la conséquence d'un choix de politique pénale discutable qui conduit à donner le sentiment d'une loi moins rigoureuse pour l'agent de la force publique, lequel représente l'État, et dispose d'un armement parfois conséquent et de moyens de contrainte non négligeables dont il doit faire usage avec discernement. », Cf avis n°17-01, 16 janvier 2017, P.3

du Défenseur des droits¹³, le législateur a décidé d'aligner le régime juridique spécifique aux militaires d'active de la gendarmerie nationale aux autres agents des forces de sécurité de l'État.

Cette parité entre des forces de sécurité intérieure amenées à évoluer sur un territoire commun, dans un contexte analogue a notamment pour finalité d'apporter une meilleure sécurisation juridique des agents qui seraient susceptibles d'être mis en cause sur le

plan de la responsabilité pénale. Pour le législateur, le régime de la légitime défense a montré certaines limites. Ce cadre légal ne répond qu'imparfaitement aux situations exceptionnelles que les agents de la force publique rencontrent dans leur mission de protection des personnes et des biens. À la différence du citoyen ordinaire, confronté à une agression injuste, les agents des forces de sécurité de l'État sont tenus à une obligation d'agir qui peut, notamment pour les militaires de la gendarmerie, aller

(14) Art. R.434-34 du code déontologie : « Le militaire de la gendarmerie obéit aux règles militaires et adhère aux valeurs inhérentes à son statut. L'état militaire exige en toute circonstance esprit de sacrifice, pouvant aller jusqu'au sacrifice suprême... »

jusqu'au sacrifice de leur vie¹⁴. Comme l'analyse le docteur en droit public, Jérôme Millet, dans une chronique d'Actualité de la Semaine Juridique consacrée à la loi

2017-258 du 28 février 2017 relative à la sécurité publique¹⁵, il s'agit « *d'un texte qui profite des circonstances : renforcer l'État de droit et le droit de l'État.* »

Cette dernière réforme législative part du constat de l'usage, hélas trop fréquent, du véhicule comme arme par destination à l'encontre des forces de l'ordre.

Le nouveau dispositif législatif.

Les articles L214-2¹⁶ et L435-1-4¹⁷ du Code de la sécurité intérieure ont été tout spécialement rédigés pour faire face à la problématique juridique d'immobiliser un

(16) Art. L214-2 du CSI
« Les personnels de la police nationale et les militaires de la gendarmerie nationale revêtus de leurs uniformes ou des insignes extérieurs et apparents de leur qualité sont autorisés à faire usage de matériels appropriés pour immobiliser les moyens de transport dans les cas suivants :

1° Lorsque le conducteur ne s'arrête pas à leurs sommations ;
2° Lorsque le comportement du conducteur ou de ses passagers est de nature à mettre délibérément en danger la vie d'autrui ou d'eux-mêmes ;
3° En cas de crime ou délit flagrant, lorsque l'immobilisation du véhicule apparaît nécessaire en raison du comportement du conducteur ou des conditions de fuite. Ces matériels doivent être conformes à des normes techniques définies par arrêté du ministre de l'intérieur.

(17) Art. L435-1 – 4° « Dans l'exercice de leurs fonctions et revêtus de leur uniforme ou des insignes extérieurs et apparents de leur qualité, les agents de la police nationale et les militaires de la gendarmerie nationale peuvent, outre les cas mentionnés à l'article L. 211-9, faire usage de leurs armes en cas d'absolue nécessité et de manière strictement proportionnée :
4° Lorsqu'ils ne peuvent immobiliser, autrement que par l'usage des armes, des véhicules, embarcations ou autres moyens de transport, dont les conducteurs n'obtempèrent pas à l'ordre d'arrêt et dont les occupants sont susceptibles de perpétrer, dans leur fuite, des atteintes à leur vie ou à leur intégrité physique ou à celles d'autrui ; »

véhicule. Soucieux d'être précis dans les conditions de mise en œuvre de l'immobilisation d'un véhicule, le législateur a défini à l'article L435-1-4° le cadre qui régit l'emploi des armes « *en cas d'absolue nécessité et de manière strictement proportionnée* ». Si ces deux conditions cumulatives ne sont pas réunies, l'article 214-2 autorise des solutions alternatives à travers le recours à des « *matériels appropriés pour immobiliser les moyens de transport...* [...] *Ces matériels doivent être conformes à des normes techniques définies par arrêté du ministre de l'Intérieur.* »

La rédaction de l'article L214-2 laisse *a priori* une grande souplesse au pouvoir réglementaire pour définir les matériels que le ministère de l'Intérieur pourrait acquérir au profit des

(18) Art. 17 : « Les normes sont d'application volontaire. Toutefois, les normes peuvent être rendues d'application obligatoire par arrêté signé du ministre chargé de l'industrie et du ou des ministres intéressés. Les normes rendues d'application obligatoire sont consultables gratuitement sur le site internet de l'Association française de normalisation. », décret n°2009-697 du 16 juin 2009 relatif à la normalisation.

forces de sécurité intérieure¹⁸. Nous verrons ainsi dans la troisième partie de cet article que les normes (ISO, AFNOR,...) constituent un enjeu majeur dans la lutte d'influence que se

livrent les acteurs économiques vis-à-vis du régulateur et de la commande publique.

Ce tour d'horizon juridique permet de constater que les forces de l'ordre disposent de toute une panoplie destinée à répondre de manière graduée et proportionnée à une menace qui se manifeste entre autres par l'emploi d'un véhicule. Cependant, en dépit des cadres juridiques et des moyens fournis, une lecture statistique des atteintes physiques des gendarmes, policiers et douaniers victimes d'une agression causée par une voiture utilisée comme arme par destination montre que les chiffres dans ce domaine sont encore trop élevés.

Des forces de sécurité publique de plus en plus exposées à l'usage du véhicule comme arme par destination¹⁹

L'analyse de certains événements démontre qu'il existe des situations extrêmes où les forces de police n'ont pas d'autre alternative que de faire

(19) Art.132-75. Al1 et 2 du Code pénal : « est une arme, tout objet conçu pour tuer ou pour blesser. Tout autre objet susceptible de présenter un danger pour les personnes est assimilé à une arme dès lors qu'il est utilisé pour tuer, blesser ou menacer ou qu'il est destiné, par celui qui en est porteur, à tuer, blesser ou menacer. »

(20) CE, Ass ; 24 juin 1949, Consorts Lecomte : dans cet arrêt de principe, le Conseil d'État admet la responsabilité sans faute du service de police, malgré l'utilisation d'armes à feu, sur le fondement du risque, dans le but d'améliorer la réparation vis-à-vis de la victime qui a la qualité de tiers par rapport à l'opération de police.

(21) Cf p.15 : www.economie.gouv.fr/files/files/PDF/nouvelle-france-industrielle-sept-2014.pdf

usage d'armes létales pour parvenir à stopper le conducteur d'un véhicule. Ces opérations de police, qu'elles soient de nature administrative ou judiciaire, comportent des risques de dommages collatéraux pour les tiers susceptibles non seulement d'engager la responsabilité pénale et civile de l'agent

mais aussi celle de la puissance publique devant le Conseil d'État sur le fondement de la théorie du risque et du principe de rupture de l'égalité devant les charges publiques²⁰.

Certaines affaires à l'issue tragique font l'objet d'une forte campagne médiatique. Elles contribuent à fragiliser davantage la cohésion sociale et font souvent l'objet d'une exploitation partisane.

Ainsi, dans le cadre du plan véhicule autonome inscrit parmi les 34 plans suivis par le comité de pilotage de la nouvelle France industrielle²¹, il conviendrait sans doute de doter les forces de l'ordre de solutions techniques non létales facilitant la prise de contrôle d'un véhicule autonome.

Cet état des lieux, forcément incomplet, montre qu'avec l'arrivée sur le marché des véhicules à délégation de conduite, les forces de police territoriales devraient être préparées dans le cadre de leur mission de régulation et de contrôle des flux routiers à cette introduction au grand public. Il suffit pour s'en convaincre de lire ou de relire, s'agissant de la gendarmerie nationale, l'article L421-1 al3 du Code de la sécurité intérieure : « *la gendarmerie nationale est destinée à assurer la sécurité publique et l'ordre public, particulièrement dans les zones rurales et périurbaines, ainsi que sur les voies de communication* ».

Il est utile de rappeler que la gendarmerie nationale accomplit seule les missions ci-dessus évoquées sur 90 % du territoire métropolitain au profit de 50 % de la population. Le contrôle des flux des personnes et des marchandises par la voie routière constitue, comme il a été

souligné *supra*, un enjeu stratégique qui se traduit par la capacité d'un État à assurer l'exercice effectif de sa souveraineté sur un territoire donné²².

Les quelques chiffres relatifs aux atteintes aux personnels des forces de sécurité²³ publique éclairent de

(22) à ce propos l'ouvrage de Michel Foucault, *Sécurité, territoire, population*, Cours au Collège de France. 1977-1978, Gallimard et Seuil, Paris, 2004, 435 p. et plus particulièrement le concept des dispositifs de sécurité.

(23) Les trois rapports sont disponibles sous les liens suivants :

www.inhesj.fr/sites/default/files/files/ondrp_ra-2015/atteintes_pn.pdf

www.inhesj.fr/sites/default/files/fichiers_site/ondrp_ra-2016/2016_ra_atteintesgn.pdf

www.inhesj.fr/sites/default/files/fichiers_site/ondrp_ra-2016/2016_ra_atteintes_age

manière brute le débat sur la nécessité d'anticiper un projet normatif de dispositifs techniques d'interception ou d'immobilisation de véhicules à délégation de conduite.

NOTA : S'agissant de la Police Nationale, le dernier rapport relatif aux atteintes aux personnels et aux biens est de l'année 2015.

Direction générale de la gendarmerie nationale (DGGN)

	2010	2011	2012	2013	2014	2015	Part en 2015	Évolution 2014/2015
Nombre total de faits avec usage d'arme	714	634	439	629	805	1047	100 %	30,1%
Véhicules	324	288	213	278	319	383	36,6%	20,1%

L'extraction de statistiques traitées par l'Observatoire national de la délinquance et des réponses pénales (ONDRP), sous forme de tableau, repris dans le rapport annuel 2016 des atteintes aux personnels et aux biens de la gendarmerie nationale est particulièrement riche d'enseignement. Ce rapport fait le constat que le véhicule est la première arme utilisée dans les agressions de gendarme (Cf p. 13).

La part des services de police de la route constitue le second poste où les gendarmes sont victimes d'agression : 309 atteintes en 2014, 343 atteintes en 2015. Les

poursuites de véhicule ont occasionné respectivement 35 atteintes en 2014 et 44 atteintes en 2015 (Cf p.6).

Direction générale des douanes et droits indirects (DGDDI)²⁴

Les agents de la Direction générale des douanes et droits indirects (DGDDI) subissent un nombre de faits éloquentes dans ce que cette administration qualifie de passage de vive force ou fuite en véhicule (hors fuite à pied)²⁵.

En mars 2011, un douanier en motocyclette avait trouvé la mort alors qu'il tentait d'intercepter un *go-*

	2011	2012	2013	2014	2015	Évolution 2011 / 2015 (en%)
Passage de « vive force » ou fuite en véhicule (hors fuite à pied)	368	358	449	427	449	+22,0

*fast*²⁶ sur l'autoroute A10, en Indre-et-Loire. Le conducteur du véhicule des trafiquants avait freiné à l'approche de travaux entraînant ainsi la percussio

Direction générale de la police nationale (DGPN)

	2008	2009	2010	2011	2012	2013
Refus d'obtempérer	439	501	417	516	387	327
Délits de fuite après accident matériel de la circulation	64	73	51	40	31	42

Pour l'année 2014, la diffusion de la version « connectée » du logiciel de

(24) Les art. 56 et 61 du code des douanes reprennent les dispositions des art. L435-1 et L.214-2 du CSI.

(25) Le passage de vive force s'entend d'un refus ou d'une omission, par le conducteur d'un véhicule, d'obtempérer aux injonctions d'arrêts exprimés par le service. Cette notion recouvre les passages en force d'un dispositif de contrôle douanier quel qu'en soit le lieu (frontière ou intérieur du territoire), mais également tous moyens utilisés pour éviter un point de contrôle (ralentissement puis redémarrage brusque en vue de se soustraire au contrôle par exemple).

(26) www.lefigaro.fr/actualite-france/2013/06/25/01016-20130625ARTFIG00430-drogue-le-go-fast-une-technique-parfois-meurtriere.php

rédaction des procédures a altéré la reconstitution des données enregistrées par la police nationale concernant les atteintes dont les fonctionnaires ont été victimes. Pour cette raison, notre étude s'appuiera sur les données statistiques de 2013 les plus pertinentes pour notre sujet.

Actuellement, l'outil statistique de la police

nationale ne comprend pas un item sur le nombre de véhicules utilisés à des fins d'atteinte à l'intégrité physique des fonctionnaires de police. Toutefois, la DGPN a recensé, pour l'année 2013, 4 895 policiers blessés par un autre moyen qu'une arme par nature dans les missions anti-délinquances et 236 en mission de maintien de l'ordre.

Le véhicule est un vecteur privilégié pour la petite et moyenne délinquance en vue de se déplacer et de perpétrer des atteintes aux biens (cambriolages, vols de voitures) sur de grandes étendues spatiales dans un laps de temps réduit (phénomène des raids). Ce vecteur est tout autant utilisé par la criminalité organisée notamment les trafiquants de drogue pour acheminer les matières illicites à travers l'Europe (pratique

dite des *go fast*). Pour rappel, cette technique consiste à utiliser des voitures de forte cylindrée lancées à grande vitesse pour transporter des produits stupéfiants. Les auteurs n'hésitent pas à mettre délibérément en danger les autres usagers de la route et les forces de l'ordre qui tenteraient de les intercepter.

Les différentes situations enregistrées par les administrations centrales et exploitées par l'ONDRP font percevoir que la faculté d'intercepter un véhicule connecté par les agents de la force publique pourrait atténuer de manière non négligeable l'exposition physique de ces derniers ainsi que les dommages directs et collatéraux susceptibles d'être causés.

Le développement de la voiture connectée et le paradigme qu'elle induira dans les sphères de la vie sociale, économique et politique nécessiteront de réfléchir en amont aux finalités pour lesquelles les forces de l'ordre pourront prendre le contrôle temporaire de certains des systèmes automatisés de conduite d'un véhicule. Cette réflexion devra naturellement s'inscrire dans le cadre d'une gouvernance globale de maîtrise des risques sociétaux.

Le premier colloque de l'Observatoire central des systèmes de transport intelligents (OCSTI) qui s'est déroulé le 25 novembre 2015 dans les locaux du Pôle judiciaire de la gendarmerie nationale avait pour thème « *la face cachée des véhicules*

intelligents : technologie et sécurité ». Cette journée a été l'occasion de dresser un inventaire des techniques existantes et d'esquisser les options paraissant les plus proportionnées de l'usage qu'en feraient

(27)

www.gendarmerie.interieur.gov.fr/crgn/content/download/627/7666/file/pr%C3%A9sentation+OCSTI+-+CREOGN+-+version+PDF.pdf.

(28) Arrêté du 23 octobre 2006 définissant les normes techniques applicables aux matériels d'immobilisation des véhicules. Cf JORF 3 novembre 2006 – Texte 3.

les agents de la force publique²⁷. À ce sujet, le concept de herse numérique a été évoqué. Il s'agit d'un dispositif technique qui permet d'arrêter en toute sécurité un véhicule à distance en

agissant sur les calculateurs qui régissent le freinage et la direction.

Contrôle de la mobilité des véhicules connectés : quelle modélisation juridique ?

Comme évoqué dans la première partie, l'article L214-2 du CSI ouvre dès à présent la possibilité de recourir à des moyens d'immobilisation à la condition que ceux-ci soient conformes aux normes prévues par un arrêté ministériel²⁸. La rédaction de l'article L214-2 n'énumère pas une liste de moyens appropriés pour immobiliser un véhicule à moteur. *A fortiori*, l'instrument législatif en vigueur permettrait l'emploi de technologies numériques de type *machine to machine* en vue d'une prise de contrôle d'une voiture autonome en mouvement. L'arrêté du 23 octobre 2006 retient exclusivement comme technique d'immobilisation tout dispositif susceptible de « *provoquer la décélération rapide puis l'immobilisation du véhicule par diminution progressive de la pression des pneumatiques, obtenue par l'usage de*

pointes adaptées ». Cette technique d'immobilisation comporte néanmoins des risques pour les occupants du véhicule concerné et son environnement médiateur. À une technique d'immobilisation externe et physique pourrait donc se substituer une technique d'immobilisation interne et intrusive. La normalisation constitue un

(29) Pour aller plus loin, Cf : revue Sécurité et Stratégie, n°25, mars 2017, p.38, « L'intérêt de la normalisation des domaines de la sécurité pour le ministère de l'intérieur » de Patrick Butor, Adjoint au secrétaire général du ministère de l'intérieur, Responsable ministériel aux normes.

enjeu fort²⁹ dans la bataille que vont se livrer les constructeurs dans la standardisation des équipements

technologiques de sécurité des voitures autonomes. Dans la droite ligne de ces luttes d'influence, les normes d'équipement technologiques d'immobilisation de ces futures voitures constitueront un enjeu stratégique pour les forces de sécurité. En effet, des normes retenues, découleront les futures doctrines d'intervention et d'interception mises en œuvre par les forces de police. À l'instar du régime de l'usage des armes en France, nous pourrions voir se dessiner progressivement une harmonisation à l'échelle européenne des procédures d'immobilisation des voitures connectées. Ce droit normatif en devenir, relatif à la prise de contrôle d'un véhicule connecté, pourrait s'appuyer sur les concepts juridiques existants, notamment celui portant sur la distinction entre police administrative et police judiciaire. Les futurs dispositifs policiers technico-juridiques d'immobilisation, devront satisfaire aux critères constitutionnels de clarté, de précision, de proportionnalité et de finalité de l'opération.

Ces critères sont ceux déjà utilisés par le Conseil constitutionnel lorsqu'il est amené à se prononcer sur la constitutionnalité de mesures de nature contraignantes qui lui sont soumises. À ce propos, il convient

(30) Prix de Thèse du Conseil constitutionnel 2011 - LGDJ

(31) Par convention, Marc-Antoine GRANGER définit la sécurité intérieure comme « la branche policière des politiques publiques sécuritaires. En centrant l'attention sur les dispositifs policiers en vue de les confronter sur les droits fondamentaux, la notion de sécurité intérieure révèle tout son intérêt car elle n'englobe pas les dispositifs de droit pénal. Elle offre ainsi la possibilité d'interroger la réponse policière à l'insécurité, ... » n°37, p22.

de citer la thèse primée³⁰ de M. Marc-Antoine Granger, intitulée "Constitution et sécurité intérieure"³¹, essai de modélisation juridique. Les travaux de ce docteur présentent l'intérêt d'adopter une démarche modélisatrice orientée

dans une fonction prédictive, constituant « [...] *un atout pour l'homme de science et pour l'homme d'action qui cherchent respectivement à étudier et à élaborer une mesure de police* ».

C'est sur le fondement de la distinction entre la police judiciaire et la police administrative, que le Conseil constitutionnel a fondé sa décision n°2015-713 de valider certaines dispositions relatives à la loi sur le renseignement. Dans cette décision, le juge constitutionnel a confirmé la validité des techniques de recueil de renseignement définies aux articles L.853-1 à L.853-3 du CSI en déclarant, dans son considérant n°9, qu'elles relèvent pour l'exercice de leurs missions de la police administrative – « *Que ces techniques, n'ont d'autre but que de préserver l'ordre public et de prévenir les infractions* ».

L'introduction des véhicules connectés s'accompagnera de nouveaux textes juridiques tendant à assurer une régulation dans les usages qui en seront faits. Dans le domaine de l'ordre public et de la sécurité routière, la distinction traditionnelle, police administrative et police judiciaire appliquée à la voiture connectée devrait ouvrir des perspectives jurisprudentielles inédites.

Sur le volet de la police administrative

(32) Article 38a1 de la Constitution : « Le Gouvernement peut, pour l'exécution de son programme, demander au Parlement l'autorisation de prendre par ordonnances, pendant un délai limité, des mesures qui sont normalement du domaine de la loi. »

Les premières mesures de régulation relevant de la police administrative pour les voitures autonomes pourraient entrer en vigueur par

voie d'ordonnance³². Ce mécanisme juridique permettrait aux forces de l'ordre de disposer, de manière concomitante, d'un cadre d'action lorsque les premiers véhicules à délégation de conduite disponibles pour les particuliers auront l'autorisation de circuler sur le domaine public. Le choix de cet instrument juridique serait dicté par un souci légitime de préservation de l'ordre public. Cette hypothèse est à mettre en perspective par la promulgation de l'ordonnance 2016-1057 du 3 août 2016 relative à l'expérimentation de véhicules à délégation de conduite sur les voies

(33) Journal officiel, 05082106, texte 7/167

publiques³³. Ce texte confère au ministre

chargé des transports, après avis du ministre de l'intérieur, la compétence de délivrer les autorisations de circulation à des fins expérimentales. L'ordonnance souligne que chaque autorisation délivrée

sera subordonnée à un examen préalable minutieux des conditions destinées à assurer la sécurité du déroulement de l'expérimentation. Cependant, à l'instar des techniques de recueil de renseignement, ces nouvelles techniques d'immobilisation, déjà existantes, devront nécessairement faire l'objet d'une codification. D'emblée, il apparaît que de disposer de techniques d'immobilisation et de géolocalisation sur un véhicule connecté offrira d'autres potentialités que la protection des agents de la force publique. Ainsi, les services d'urgence comme le 17 ou le 18 sont chaque jour destinataires d'appels d'usagers signalant le départ précipité d'un proche, d'une connaissance, d'un individu, au volant d'un véhicule, qui en raison d'un contexte ou de son attitude présente un caractère inquiétant (dépression, état suicidaire, sous l'emprise de produits ou de substances addictives).

Sur le volet de la police judiciaire

En l'état du droit positif, l'accès par des enquêteurs à un système informatique installé sur un véhicule connecté est réservé au domaine de la lutte contre la criminalité en bande organisée (art 706-73 et 706-73-1 du CPP). Il en résulte qu'actuellement, la combinaison des articles 706-102-1 et 706-102-5 al2 du CPP autoriserait les officiers de police judiciaire (OPJ) à effectuer la captation de données provenant d'un système informatique d'un véhicule.

L'article 706-102-1 ou 2 du CPP énonce que les officiers et agents de police judiciaire peuvent être autorisés par un

magistrat : « [...] à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ».

L'article 706-102-5 al2 précise en outre que : « En vue de mettre en place le dispositif technique mentionné aux articles 706-102-1 et 706-102-2, le juge des libertés et de la détention, à la requête du procureur de la République, ou le juge d'instruction peut également autoriser la transmission par un réseau de communications électroniques de ce dispositif ». Dans ce cadre, la captation de données n'implique pas la modification ou une action sur le système mais vise à collecter des preuves.

Outre-Atlantique, le rapport *Rand Corporation* (note 3) est le fruit d'une réflexion d'ensemble de seize personnalités et experts en nouvelles technologies. Ce groupe a débattu sur l'importance à venir des technologies du web et de celles qui probablement impacteront la justice pénale. Ces échanges ont donné lieu à l'identification de quarante-cinq besoins qui devront, selon les participants, à la fois satisfaire un usage proportionné mais aussi maîtrisé des risques inhérents. Parmi ces besoins identifiés figurent des réflexions en

matière de *law enforcement* vis-à-vis de la voiture connectée.

Réflexions Outre-Atlantique : des perspectives identifiées en matière de règles d'engagement.

Le groupe des seize experts recommande de mettre en place un groupe de travail chargé d'élaborer de nouvelles règles et procédures spécifiques aux véhicules connectés (autonomes ou indépendants).

Comme le soulignent les experts dans les deux cas pratiques suivants, les enjeux dans ce segment sont éminemment sensibles sur le plan des libertés individuelles :

- Quelle place et quelles prérogatives pourraient-ils être données à un agent de police, qui serait en mesure d'interagir avec le véhicule d'un particulier disposant de capteurs connectés à Internet ? Selon le cadre juridique retenu (ex : autorisation d'un magistrat), ces nouvelles technologies donneraient la possibilité à cet agent de police de capter du véhicule connecté des données à caractère personnel comme : les identités des occupants, l'historique de leur déplacement respectif... Muni de ce genre de données, le policier ou le gendarme équipé de matériels informatiques embarqués spécifiques pourrait opérer des consultations au sein de certains fichiers automatisés de police. En direct, depuis leur véhicule connecté, ces patrouilleurs pourraient prendre connaissance de l'existence ou non d'antécédents administratifs ou judiciaires des intéressés, voire s'il y aurait lieu d'exécuter un mandat coercitif à leur

encontre. Ce cas concret montre dès à présent que la conception actuelle du contrôle routier réalisée par les agents de police sur la route serait en passe de devenir une image d'Épinal.

- Autre cas pratique, celui d'un véhicule connecté, sans conducteur à bord, stationné illégalement ou nécessitant son déplacement en cas d'urgence avérée. Dans quel cadre juridique des patrouilleurs pourraient diriger ce véhicule pour le déplacer vers un lieu plus approprié ?

Pour le groupe de travail, ces deux mises en situation opérationnelle suffisent à elles seules à mettre en exergue l'examen à venir d'une réflexion juridique relative aux contrôles et à la régulation des flux des voitures autonomes, plus particulièrement lorsqu'elles relèvent des prérogatives des forces de police. Selon cette commission, il s'agira concrètement d'adopter pour les forces de l'ordre, de nouvelles directives, méthodes tactiques et règles d'engagement pour répondre à l'émergence programmée des véhicules connectés avec ou sans conducteur. En corollaire de ce qui précède, la commission *ad hoc* insiste tout particulièrement sur la faculté, pour les agents de police, d'extraire les données depuis les objets connectés activés des véhicules connectés. Quelques finalités non exhaustives sont énumérées à titre d'illustration :

- Améliorer les enquêtes accidents et leur suivi,
- Former des praticiens sur les potentialités des nouvelles technologies,
- Mettre en œuvre des protocoles

d'identification véhicule ami / ennemi,

- Localiser le propriétaire ou le conducteur du véhicule connecté mis en cause,
- Établir des techniques de neutralisation sans risque.

Une voiture autonome va introduire une rupture d'ordre sociétale et technologique dans la décennie à venir. Les forces de police devront, à l'instar de leurs aînés, s'adapter à de nouveaux modes d'action de la délinquance qui impacteront les pratiques des unités de police judiciaire, de sécurité publique et routière. De nouveaux dispositifs techniques seront à construire, conformes aux finalités légitimes reconnues dans notre État de droit. Ainsi, en 1907 la création des

(34) <https://criminocorpus.org/fr/legislation/textes-juridiques-lois-decrets/textes-relatifs-a-l'organisation/decret-du-30-decembre-1907-cr/> - Les commentaires et instructions de Georges Clémenceau sur l'état d'esprit qui doit animer ces unités sont sans équivoques et d'une actualité saisissante.

premières Brigades Mobiles³⁴ voulue par Georges Clémenceau, ministre de l'Intérieur, traduit dans les faits qu'à moyen nouveau, il faut une nouvelle

doctrine. Il est utile de rappeler le contexte³⁵ de la création de ces unités : « 1907. En ce début de siècle où la vie se transforme au rythme accéléré d'une industrie triomphante, les structures traditionnelles de la vieille société se brisent chaque jour davantage derrière la façade de la Belle Époque. La criminalité augmente dans des proportions d'autant plus inquiétantes qu'une délinquance nouvelle

(35) Cf annonce générique du 1^{er} épisode de la série télévisée «les Brigades du Tigre » (1974 - 1983).

est née qui s'appuie, elle, sur le progrès technique et fait

échec à une police archaïque dont les méthodes et le matériel n'ont guère évolué depuis Vidocq. Un chiffre est plus éloquent que tout : au cours de l'année 1906, 103 000 affaires criminelles et correctionnelles ont été classées sans que les auteurs aient pu être identifiés. L'année 1907 s'annonce pire encore. Il y va de la sécurité des villes et des campagnes. »

L'avènement de la voiture connectée devrait introduire un changement de paradigme dans les règles d'engagement opérationnel. L'adoption de techniques de type cyberinterception ou cyberimmobilisation, ayant comme moyen contraignant des applications de type herse numérique, devrait neutraliser de manière efficiente la possibilité d'utiliser la voiture comme une arme par destination. En retour, le recours à la force armée par les agents publics de la sécurité intérieure aurait dans ce segment un caractère exceptionnel. Les futurs dispositifs techniques d'immobilisation des voitures connectées constituent une piste sérieuse de prospective à un moment où la DGGN a constitué un groupe de travail centré sur la problématique de leurs arrêts.

Règles européennes de droit civil en robotique¹

par NATHALIE NEVEJANS

R

(1) Etude publiée à la demande de la commission des affaires juridiques du Parlement européen afin d'évaluer sous les angles juridique et éthique le projet de rapport du 31 mai 2016 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (rapport Mady Delvaux), <http://www.europarl.europa.eu/sides/getDoc.do?type=C&OMP&mode=XML&language=FR&reference=PE582.443//EP//NONSGML%2BCOMP&lang=FR&reference=PE582.443%2BPE-582.443%2B01%2BDOC%2BPDF%2BVO//FR>

Référence de la publication originelle : Parlement européen, *Policy Department*, Direction générale des politiques internes, Département thématique C, Droits des citoyens et affaires constitutionnelles,

– Extraits de l'étude –

2. CONSIDERATIONS GENERALES CONCERNANT LES ROBOTS : LA NOTION DE ROBOT ET SES IMPLICATIONS, ET LA QUESTION DE LA CONSCIENCE

Il s'agit d'examiner de manière globale la notion de robot et ses implications, ainsi que la question de la conscience, afin de délimiter le champ des réflexions en robotique et en intelligence artificielle.

2.1. Une définition commune des robots autonomes et intelligents

Le paragraphe 1 de la proposition de résolution suggère « à la Commission de proposer une définition européenne commune des différentes catégories de robots autonomes et intelligents, compte tenu des caractéristiques suivantes des robots intelligents :

– acquisition d'autonomie grâce à des capteurs et/ou à l'échange de données

Affaires juridiques et parlementaires, Etude pour la Commission JURI, PE 571.379 FR, 2016, 40 pages, [www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU\(2016\)571379_FR](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_FR).



NATHALIE NEVEJANS

Maître de conférences en droit privé (Université d'Artois)
Membre du Comité d'éthique du CNRS (COMETS)



« Les robots autonomes et intelligents présentent plus de questionnements juridiques et éthiques que d'autres. »

*avec l'environnement (interconnectivité) ;
échange et analyse de données ;*

*– capacité d'auto-apprentissage (critère
facultatif) ;*

– présence d'une enveloppe physique ;

*– adaptation du comportement et des
actes à l'environnement ».*

Il apparaît incontournable d'adopter une définition commune. Or, la définition des

(2) Nathalie Nevejans, *Traité de droit et d'éthique de la robotique civile*, LEH édition, Bordeaux, Coll. « Science, éthique et société », janvier 2017, n°s 67 et s.

robots est toujours une affaire mal aisée², puisqu'il n'existe pas vraiment de

consensus au sein de la communauté scientifique mondiale. Certains travaux actuels considèrent qu'un robot au sens large doit remplir plusieurs conditions, et

consister en une machine matérielle, dotée des capacités d'agir sur le réel, de percevoir son environnement, et de décider³. Certains robots seulement peuvent présenter en outre des capacités d'apprentissage, de communication et d'interaction, ou encore être dotés d'une certaine autonomie⁴.

(4) Ibid.

La définition proposée par le paragraphe 1 ne vise pas l'ensemble des robots, mais seulement les robots autonomes et intelligents, comme il est exposé dans le projet de rapport. Toutefois, les caractéristiques indiquées mériteraient d'être précisées davantage, pour éviter toute incertitude quant au champ d'application du futur instrument.

On peut relever deux points délicats, qui révèlent toute la complexité d'une définition

générale. D'une part, si les robots chirurgicaux (visés, par exemple, par le paragraphe 17 de la proposition) peuvent être assimilés à des robots en général, ils ne sauraient entrer dans la catégorie des robots autonomes et intelligents. En effet, les robots chirurgicaux fonctionnent le plus souvent sur un modèle maître-esclave, c'est-à-dire par simple téléopération par le praticien, à l'instar du robot chirurgical Da Vinci. Comme l'homme reste dans la boucle décisionnelle, il peut alors être plus difficile de parler d'autonomie du robot. Pourtant, il reste essentiel que l'Union européenne se penche sur les robots chirurgicaux, notamment sur la question de la sécurité du robot et la formation du chirurgien au robot utilisé.

D'autre part, bien que la recherche développe des drones dotés d'autonomie, les drones (évoqués par la proposition au paragraphe 19) sont le plus souvent téléopérés par leur opérateur, et ne répondent que difficilement à la condition d'autonomie et d'intelligence. Les drones, qui ont commencé à intéresser l'Union européenne, poseront notamment des questions en termes de sécurité, et de protection de la vie privée et des données à caractère personnel.

2.2. Les limites terminologiques des notions de « robot autonome » et de « robot intelligent »

La proposition de résolution vise spécifiquement les robots autonomes et

intelligents. Il est vrai que cette forme robotique présente plus de questionnements juridiques et éthiques que d'autres.

2.2.1. Les limites terminologiques de la notion de « robot autonome »

Le point R de la proposition de résolution indique que l'autonomie d'un robot est définie « *comme la capacité à prendre des décisions et à les mettre en pratique dans le monde extérieur, indépendamment de tout contrôle ou influence extérieurs ; que cette autonomie est de nature purement technique et que le degré d'autonomie dépend du degré de complexité des interactions avec l'environnement prévu par le programme du robot* ». Même si la notion de robot autonome est d'un abord complexe dans la littérature scientifique, étant donné que les roboticiens mettent sous ce terme les approches les plus

(5) voir notre ouvrage précité, n°s 120 et s.

(6) Rapport n° 1 de la CERNA, « Éthique de la recherche en robotique », précité, p. 45-46.

variées⁵, la définition proposée par le projet de rapport nous semble cohérente.

L'emploi du terme « technique » pour qualifier l'autonomie indique qu'il ne s'agit pas d'une forme de conscience de la machine. La notion d'autonomie technique est assimilable à l'autonomie opérationnelle développée dans certaines études⁶.

Le seul bémol à apporter pourrait porter sur les termes « *indépendamment de tout contrôle ou influence extérieurs* ». En effet,

la notion d'influence extérieure n'est guère évocatrice, et risque d'engendrer une confusion avec la capacité du robot autonome à prendre des décisions précisément en fonction des stimuli de l'environnement extérieur (= influence extérieure). Il pourrait être plus adéquat de conserver seulement « *indépendamment de tout contrôle extérieur* ».

En tous les cas, l'emploi des termes de « robot autonome » mérite approbation, contrairement à ceux de « robot intelligent ».

2.2.2. Les limites terminologiques de la notion de « robot intelligent »

Ce sont surtout les termes de « robot intelligent » qui méritent réflexion. En théorie, ils ne présentent aucune difficulté. En effet, des scientifiques emploient la notion de « robot intelligent » pour désigner la génération des robots qui n'étaient plus cantonnés aux lignes d'assemblages fixes et fonctionnant en mode automatique, mais devenaient capables de s'adapter à la variabilité et à l'incertitude de leur environnement. Lorsque les robots sont sortis de l'usine, les chercheurs ont été contraints de les adapter afin qu'ils puissent évoluer dans un monde complexe, hautement imprévisible. Comme il devenait impossible de programmer l'ensemble des situations que le robot allait rencontrer, l'idée a été alors de développer des machines capables d'anticiper certaines situations et de s'y adapter, notamment par

l'emploi de toute une gamme de capteurs, afin de les rendre autonomes. Toutes ces recherches relèvent de la robotique intelligente⁷.

Ray Jarvis, « Intelligent Robotics : Past, Present and Future », *International Journal of Computer Science and Applications*, 2008, Vol. 5, n° 3, p. 23.

Le terme est également employé dans la norme technique EN ISO 8373 relative aux « Robots et composants robotiques – Vocabulaire » de 2012. Elle définit le robot intelligent au § 2.28, comme le « *robot capable d'exécuter des tâches par détection de son environnement, et/ou par interaction avec des sources extérieures et adaptation de son comportement* ». La norme donne les exemples du robot industriel comportant une sonde de vision pour prendre et placer un objet, du robot mobile capable d'éviter les collisions, ou encore du robot à jambes se déplaçant sur un terrain inégal.

Même s'il est vrai, comme le souligne le point A de la proposition de résolution, que « les humains ont, de tous temps, rêvé de construire des machines intelligentes », il convient néanmoins d'émettre des réserves concernant l'emploi de la terminologie de « robot intelligent », au regard de la peur des robots qui trouve deux origines.

1°/ La peur occidentale du robot

Au regard du fonds culturel commun irriguant tout l'inconscient collectif occidental, la notion de « robot intelligent » pourrait provoquer des réactions négatives, défavorables au développement de

l'industrie robotique. Il est essentiel de ne pas sous-estimer l'influence sur la société des récits grecs ou hébraïques anciens, notamment le mythe du Golem. Les oeuvres romanesques des XIX^e et XX^e siècles les ont d'ailleurs souvent repensés afin de mettre en évidence les risques de perte de contrôle de l'homme sur ses propres créatures. Aujourd'hui, la crainte occidentale de la créature, qui reprend vigueur sous la forme modernisée du robot ou de l'intelligence artificielle, pourrait être accentuée par une incompréhension des citoyens européens, et même nourrie par certains médias.

Cette peur du robot n'est pas partagée par les pays d'Extrême-Orient. Après la seconde guerre mondiale, on vit apparaître dans un manga au Japon une créature robotisée (Astro Boy) donnant à la société une image très positive des robots. D'ailleurs, la vision shintoïste des robots par les japonais fait que, comme toutes choses, ils sont dotés d'une âme. Contrairement à l'Occident, les robots ne sont pas perçus comme des créatures dangereuses et prennent naturellement place auprès des hommes. C'est pour cette raison que la Corée du sud, par exemple, a très tôt eu l'idée de développer une réflexion juridique et éthique sur les robots, et a fini par entériner la notion de « robot intelligent » dans une loi, modifiée en dernier lieu en 2016, intitulée « Intelligent robots development and distribution promotion act ». Ce texte définit le robot

intelligent comme un dispositif mécanique qui perçoit l'environnement externe pour lui-même, apprécie les situations et se

(8) « The term "intelligent robot" means a mechanical device that perceives the external environment for itself, discerns circumstances, and moves voluntarily », Intelligent robots development and distribution promotion act, Ministry of Trade, Industry and Energy, Act n° 13744, Jan. 6, 2016.

déplace de lui-même (art. 2, § 1)⁸. La proposition de résolution se situe donc dans un contexte scientifique similaire.

Cet écart culturel entre les visions extrême-orientales et occidentales pourrait néanmoins justifier une démarcation du législateur européen des voies juridiques empruntées par les pays asiatiques. En effet, les solutions adoptées en Asie ne seraient pas forcément acceptables en Europe. Cela est d'autant plus vrai qu'aujourd'hui la peur prend consistance en s'ancrant dans le réel, et non plus dans le mythe ou le romanesque. Dans deux hypothèses, au moins, les peurs ont été réanimées, non sans raison. En 2014 et 2015, Bill Gates, Stephen Hawking et Elon Musk avaient évoqué les dangers de l'intelligence artificielle, puisqu'elle avait été présentée comme pouvant se retourner

(9) Michael Sainato, « Stephen Hawking, Elon Musk, and Bill Gates Warn About Artificial Intelligence », Observer [on line], 08/19/15, <http://observer.com/2015/08/stephen-hawking-elon-musk-and-bill-gates-warn-about-artificial-intelligence/>

(10) Bill Joy, « Why the future doesn't need us », in F. Allhoff et al., dir., Nanoethics. The Ethical and Social Implications of Nanotechnology, éd. Wiley-Blackwell, 2007, p. 32.

contre l'homme⁹. Comme le souligne le point I de la proposition de résolution, il pourrait arriver que l'humanité coure un péril si « l'intelligence artificielle [surpassait]

les capacités intellectuelles humaines ».

Pour éviter ce danger, le projet de rapport souligne qu'il est indispensable que l'homme soit toujours en mesure de contrôler ses créations. Ce point mérite amplement d'être approuvé. Même en robotique, dès 2007, le scientifique américain Bill Joy avait déjà estimé que les robots intelligents – l'auteur faisant référence à des robots dont les capacités dépasseraient largement celles visées dans la définition de la proposition de résolution – faisaient courir à l'homme des risques d'extinction. Il préconisait alors de renoncer aux recherches dans les secteurs potentiellement dangereux, car la mise en place de méthodes de contrôle des technologies pourrait s'avérer trop lente ou trop peu efficace¹⁰. On constate que l'auteur associait explicitement les robots intelligents avec les risques de destruction de l'homme, révélant l'appréhension négative de cette terminologie en occident.

Dans un tel contexte, on pourrait craindre que la découverte par les citoyens européens d'un texte relatif à des robots intelligents puisse nourrir une vision fantasmée des robots qui risquerait, soit de renforcer la peur de la créature artificielle, soit de freiner l'émergence de nouveaux secteurs de la robotique lorsque l'acheteur serait profondément déçu par une machine qui ne se révélerait finalement pas intelligente au sens humain du terme. Dans tous les cas, entériner les termes de « robot intelligent » risquerait de faire croire à la

société civile que les robots conscients, pensants, ou presque humains, ne relèveraient désormais plus de la science-fiction.

De même, dans l'objectif d'apaiser la peur des robots, il pourrait être intéressant de mettre en place un système destiné à conserver le contrôle sur les robots et l'intelligence artificielle. A cet égard, il conviendrait de déterminer les secteurs potentiellement dangereux pour l'homme afin, peut-être pas d'interdire les recherches, mais tout au moins de les encadrer. Cette mission pourrait incomber à la future Agence européenne pour la robotique et l'intelligence artificielle, visée aux paragraphes 8 et 9 de la proposition. Par exemple, l'autoréplication des robots, et plus encore des nanorobots, pourrait être difficile à maîtriser et potentiellement dangereuse pour l'homme et l'environnement, ce qui imposerait un contrôle strict externe des activités de recherche.

2°/ La délicate délimitation entre les avantages de la robotisation et les risques socio-économiques

La peur occidentale de voir l'homme supplanté par le robot se combine avec les inquiétudes d'ordre socio-économique. Cette situation n'est pas nouvelle, puisqu'elle expliquait déjà les premières oppositions au pouvoir de la machine par l'ouvrier anglais Ned Ludd qui avait cassé les métiers mécanisés en 1811. En

robotique, cette supplantation de l'homme pourrait se traduire par la disparition des emplois. Cette question est justement soulevée par le projet de rapport au point E. Elle mérite une grande attention car elle exige la conciliation entre deux groupes d'intérêts différents :

D'un point de vue économique, il paraît opportun de faire en sorte de développer la robotique en Europe, en accroissant les aides aux entreprises, en guidant les jeunes vers des formations adaptées, en accordant des financements aux universités, *etc.* En effet, la robotique apparaît comme un facteur de relance économique. Certains évoquent déjà l'idée d'une quatrième révolution industrielle, en lien avec le développement de l'Usine du

(11) Nathalie Nevejans, « Les usines connectées », in A. Zollinger, dir., *Les objets connectés*, éd. Mare & Martin, à paraître, 2017.

futur¹¹, à laquelle la robotique prendrait pleinement part aux côtés d'autres

technologies émergentes, comme les objets connectés, les puces RFID ou les imprimantes 3D. Les avantages présentés par la robotisation en termes économiques pourraient alors inciter à la relocalisation en Europe de la production ayant été délocalisée vers les pays émergents.

D'un point de vue social, les avantages, notamment décrits au point D du projet de rapport, ne doivent pas faire oublier les risques liés à la robotisation de l'industrie, et même de la société en général par le développement des robots de services. En

effet, l'accélération de la robotisation pourrait faire disparaître plusieurs millions d'emplois en Europe, non seulement les moins qualifiés, mais également ceux relevant des secteurs à plus fort contenu intellectuel, comme les métiers de l'enseignement. La robotisation et la relocalisation de l'industrie doivent donc être pensées pour soutenir l'homme au travail et non pour l'évincer de l'entreprise. Il serait utopique de croire que la société serait capable de se réorganiser pour pouvoir prendre en charge des milliards

d'humains oisifs¹².

Toutefois, certaines études indiqueraient, au contraire, que la robotisation aurait plutôt comme effet de

(12) En ce sens, Moshe Y. Vardi in « The Job Market of 2045. What will we do when machines do all the work ? », IEEE Spectrum's [on line], 22 janvier 2013, <http://spectrum.ieee.org/podcast/at-work/tech-careers/the-job-market-of-2045>.

transformer les emplois. Selon elles, on assisterait ainsi d'abord à leur diminution, pour ensuite en voir émerger de nouveaux, parfois sans lien avec les précédents. Malgré tout, le risque en la matière est d'être face à une « génération perdue », correspondant à la génération qui aurait reçu une formation pour des emplois en cours de disparition et qui se trouverait dans l'impossibilité de trouver un emploi en adéquation avec ses compétences. Pour éviter cela, il conviendrait dès à présent de placer les Universités en première ligne pour faire face à ce défi, en leur accordant les moyens nécessaires pour anticiper l'évolution et adopter une position innovante.

Il pourrait être intéressant de confier la mission d'analyser les risques socio-économiques du développement de la robotique à l'Agence européenne pour la robotique et l'intelligence artificielle évoquée aux paragraphes 8 et 9 de la proposition de résolution.

2.3. Les questions de la conscience et de la place des lois d'Asimov en robotique

Le point L de la proposition de résolution indique que « *jusqu'à ce que les robots deviennent conscients de leur propre existence, ou soient fabriqués ainsi à dessein, si tant est que cela advienne un jour, il y a lieu de considérer les lois d'Asimov comme s'appliquant aux concepteurs, aux fabricants et aux utilisateurs de robots, étant donné que lesdites lois ne peuvent être traduites en langage de programmation* ».

Le texte est peu clair étant donné qu'il semble signifier qu'en l'attente du développement de la conscience des robots, les êtres humains devraient alors appliquer les Lois de la robotique d'Asimov. Cette disposition, qui relie deux concepts qui n'ont que peu de rapport entre eux, appelle deux séries de remarques importantes.

1°/ Il convient, d'une part, de s'arrêter sur la question de la validité juridique des Lois de la robotique que la proposition de résolution souhaite appliquer aux concepteurs, aux fabricants et aux

utilisateurs de robots. En littérature, l'écrivain Isaac Asimov chercha à mettre fin à la vision occidentale négative des robots à travers ses nouvelles, publiées en 1950 sous la forme du recueil « *I, Robot* ». Pour la première fois, des créatures ne se révoltaient pas contre leur créateur. Cette maîtrise des créatures se fit au moyen de l'invention des Lois de la robotique auxquelles les robots devaient impérativement se conformer :

- « 1. *Un robot ne peut porter atteinte à un être humain, ni permettre, en restant passif, qu'un être humain soit exposé au danger.*
2. *Un robot doit obéir aux ordres que lui donne un être humain, sauf si ces ordres entrent en conflit avec la première loi.*
3. *Un robot doit protéger son existence tant que cette protection n'entre en conflit ni avec la première ni avec la seconde loi.* »

L'écrivain avait ajouté plus tard la loi zéro, prioritaire sur les autres : « 0. *Un robot ne peut par son action mettre l'humanité en danger, ni, restant passif, laisser l'humanité en danger.* »

Asimov avait conçu ces Lois comme un outil littéraire à connotation juridique afin de nourrir la trame de son œuvre en justifiant la maîtrise des robots par l'homme :

Les Lois d'Asimov avaient été inventées pour être volontairement imprécises afin de

(13) Voir notre ouvrage précité, n°s 916 et s.

pouvoir nouer d'intéressantes

intrigues¹³. En aucun cas l'auteur n'avait pensé à l'origine à ériger davantage qu'un artifice littéraire astucieux. Ainsi, ces Lois ne sauraient constituer de véritables principes juridiques, en dehors même de la question de la faculté ou non de leur programmation, évoquée au point L.

Ces Lois ne s'adressaient qu'aux robots eux-mêmes et instaurent une forme d'éthique de la machine. Ainsi, lorsque le point L de la proposition indique qu'« *il y a lieu de considérer les lois d'Asimov comme s'appliquant aux concepteurs, aux fabricants et aux utilisateurs de robots* », il se livre à une interprétation erronée des Lois de la robotique, puisqu'elles n'étaient jamais destinées à l'homme.

Les romanesques Lois de la robotique étant incapables de protéger l'homme, il serait concevable d'édifier un cadre éthique général adapté aux problématiques de la robotique et de l'intelligence artificielle (voir 4.1.).

2°/ Il est dès à présent fondamental, d'autre part, d'évoquer la question de la conscience de soi par le robot. Cette conscience, qu'elle survienne de manière plus ou moins spontanée ou à la suite de recherches scientifiques, semble être envisagée sereinement par le point L de la proposition de résolution. Or, cette situation pourrait faire vaciller l'humanité. S'il est inutile de rappeler qu'il est déjà difficile de prouver qu'une personne humaine dispose d'une conscience, comment pourrait-on

détecter son apparition dans une machine ? De plus, admettre qu'une machine puisse être consciente obligerait l'homme à respecter les droits

(14) Nathalie Nevejans, « Le robot qui voulait devenir un homme... ou le statut juridique de l'androïde », in F. Defferrard, dir., *Le droit saisi par la science-fiction*, éd. Mare & Martin, coll. « Libre Droit », 2016, p. 156 et s., n°s 33 et s.

fondamentaux du robot¹⁴. Enfin, et surtout, si le robot devait un jour être conscient, étant par nature plus puissant,

plus rapide, plus intelligent, plus parfait et presque immortel, l'humanité telle qu'elle existe serait vouée à périr, voire à être anéantie en application de la loi naturelle classique qui veut qu'une espèce inférieure disparaisse au profit d'une espèce supérieure.

Il nous apparaît ainsi indispensable d'instaurer un principe selon lequel toute recherche scientifique destinée à rendre conscient un robot ou ayant un tel effet de manière indirecte devrait relever d'un secteur potentiellement dangereux pour l'homme exigeant un encadrement strict (voir 2.2.2., 1°).

3. LES PROBLÈMES POSÉS PAR LA RESPONSABILITÉ EN ROBOTIQUE

La proposition de résolution indique au paragraphe 24 qu'en égard aux nouvelles capacités des robots, « *la responsabilité civile des robots est une question cruciale à laquelle il importe de répondre au niveau de l'Union* ». Toutefois, il apparaît incongru de régler la question en instaurant une personnalité juridique du robot en matière de responsabilité. Par ailleurs, la proposition

appellera diverses remarques concernant la responsabilité des dommages causés par un robot autonome afin d'en assurer la cohérence avec le droit de la responsabilité civile.

3.1. L'incongruité de la personnalité juridique du robot en matière de responsabilité

La proposition de résolution envisage éventuellement de mettre en place une nouvelle catégorie de personne propre aux robots autonomes : les personnes électroniques. En effet, le paragraphe 31, f), indique que la Commission européenne devrait examiner les conséquences juridiques s'agissant de « *la création d'une personnalité juridique spécifique aux robots, pour qu'au moins les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques dotées de droits et de devoirs bien précis, y compris celui de réparer tout dommage causé à un tiers ; serait considéré comme une personne électronique tout robot qui prend des décisions autonomes de manière intelligente ou qui interagit de manière indépendante avec des tiers* ».

La question de la personnalité juridique du robot autonome mérite d'être évacuée des réflexions portant sur le droit civil de la robotique, car elle est aussi inutile qu'incongrue.

Classiquement, afin d'attribuer la personnalité juridique à une entité, on tente de la rapprocher de l'homme. Tel est bien le cas pour le droit des animaux, puisque les partisans mettent en avant l'idée que la personnalité juridique doit leur être attribuée en ce que certains d'entre eux disposent d'une conscience, d'une capacité à souffrir, etc., donc finalement de sentiments propres les arrachant à leur catégorie de choses. Or, la proposition de résolution ne fait pas dépendre la reconnaissance de la personnalité juridique du robot à un éventuel état de conscience. La personnalité juridique n'est donc pas associée à une quelconque prise en considération de l'être profond du robot ou de ses sentiments, dans l'hypothèse douteuse où le robot serait pourvu d'une conscience. L'attribution d'une telle personnalité au robot poursuivrait donc un simple objectif fonctionnel, relevant notamment de la nécessité qu'il puisse être en mesure d'être responsable de ses actes.

Il existe une autre hypothèse dans laquelle il peut être concevable d'attribuer une personnalité juridique à une entité : lorsque cette attribution a pour effet de lui donner vie juridique. Thomas Hobbes montre dans le Léviathan que le terme personne (persona) d'origine latine désignait le masque, puis finalement la représentation de soi-même ou d'autrui. L'exemple des personnes morales révèle que le droit a déjà attribué à une entité non-humaine la

personnalité juridique. Il ne convient pourtant pas d'en déduire que les robots pourraient bénéficier à leur tour d'une telle personnalité. En effet, contrairement à la personnalité juridique de la personne physique qui découle ontologiquement de son humanité, son attribution à une personne morale constitue une fiction juridique. Les personnes morales ne sont en mesure d'agir dans l'espace juridique que parce qu'un être humain se dessine en filigrane derrière chacune d'entre elles et les représente. C'est donc bien l'homme qui anime au final la personne morale. Sans lui, elle n'est qu'une coquille vide. Dès lors, qu'en serait-il pour le robot ? Deux possibilités s'offrent à nous : soit l'homme est le véritable acteur juridique derrière le robot, soit le robot est son propre acteur juridique.

D'une part, si un homme existait derrière le robot autonome, ce serait finalement l'homme qui représenterait la personne électronique, laquelle ne serait juridiquement qu'une construction intellectuelle fictionnelle, à l'image de la personne morale. Seulement, la mise en place d'un mécanisme aussi compliqué pour aboutir à un résultat aussi inutile prouverait l'incongruité de l'attribution de la personnalité juridique à une simple machine.

D'autre part, au regard de la proposition de résolution, il semblerait que l'on se dirige plutôt vers le gommage complet de la

présence humaine. En reconnaissant une personne électronique chez « *tout robot qui prend des décisions autonomes de manière intelligente ou qui interagit de manière indépendante avec des tiers* » (paragraphe 31, f), *in fine*), la proposition semble signaler que ce serait le robot qui se représenterait lui-même et deviendrait son propre acteur juridique. Cette analyse est confirmée dans le point S qui indique que « *plus un robot est autonome, moins il peut être considéré comme un simple outil contrôlé par un autre acteur [...] et qu'il y a lieu d'adopter de nouvelles règles permettant d'imputer (totalement ou partiellement) à une machine ses actes ou son inaction* ». S'il n'est plus contrôlé par un acteur, c'est donc qu'il le devient lui-même. Mais comment une simple machine, carcasse vide de toute conscience, sentiments, pensées ou volonté propre, pourrait-elle devenir son propre acteur juridique ? Comment même envisager cela comme prévisible à 10 ou 15 ans, c'est-à-dire dans les délais fixés au paragraphe 25 de la proposition de résolution ? D'un point de vue scientifique, juridique et même éthique, il est aujourd'hui impossible, et probablement pour très longtemps encore, qu'un robot puisse participer à la vie juridique en l'absence d'un être humain qui se dessinerait derrière.

De plus, en considérant que l'attribution au robot de la personnalité juridique aurait pour fonction première d'en faire un acteur responsable en cas de dommage, force est

de constater que d'autres systèmes seraient bien plus efficaces en matière d'indemnisation des victimes, comme la mise en place d'une assurance adaptée aux robots autonomes, éventuellement combinée avec un fonds de compensation (paragraphe 31, a) à e)).

Il est également impératif de garder à l'esprit que ce statut engendrerait nécessairement des effets juridiques indésirables. Le point T de la proposition signale que la création d'une personnalité juridique imposerait la reconnaissance de droits et de devoirs aux robots. Comment pourrait-on envisager d'attribuer des droits et des devoirs à une simple machine ? Comment un robot pourrait-il avoir des devoirs, alors qu'il s'agit d'une notion étroitement liée aux représentations morales humaines ? Plus encore, quels droits attribuer au robot : le droit à la vie – c'est-à-dire le droit à la non-destruction –, le droit à la dignité, le droit à l'égalité avec l'homme, le droit à la retraite, le droit au versement d'une rémunération (ce dernier droit étant explicitement envisagé au paragraphe 31, b), de la proposition), ... ? Prenons l'exemple de trois sortes de robots dont certains peuvent, d'ores et déjà, être considérés comme autonomes et intelligents au sens de la proposition. L'attribution de droits voudrait-elle dire qu'un robot employé en milieu hostile pourrait refuser de traverser une zone dangereuse susceptible de l'endommager ou de le détruire, qu'un robot agricole

pourrait exiger d'avoir des congés, ou qu'un robot de soins pourrait demander un salaire avant de commencer à s'occuper d'une personne âgée ? Dans ce cas, pourquoi fabriquer des robots qui ne serviraient à rien ou les acheter ? Et surtout pourquoi ne pas simplement continuer à faire appel au travail des hommes ? On constate que l'attribution de droits à un robot se révélerait hautement fantaisiste et potentiellement destructrice du marché émergent de la robotique.

En réalité, les partisans de la personnalité juridique ont une vision fantasmée du robot, marquée par les romans ou le cinéma de science-fiction. Ils ne peuvent concevoir le robot – surtout s'il est qualifié d'intelligent et s'il est humanoïde – que comme une véritable créature artificielle pensante alter ego de l'homme. Il nous semble inopportun et malvenu, non seulement de reconnaître l'existence d'une personne électronique, mais également d'établir une quelconque personnalité juridique. Le danger n'est alors pas seulement d'accorder des droits et des obligations à un simple outil, mais aussi de faire éclater les frontières entre l'homme et la machine, ouvrant ainsi la voie à une confusion entre le vivant et l'inerte, entre l'humain et l'inhumain... De plus, faire émerger une nouvelle sorte de personne – la personne électronique – est un message fort qui pourrait non seulement réanimer avec force la peur de la créature, mais également remettre en cause les fondements humanistes de l'Europe.



« Le danger n'est alors pas seulement d'accorder des droits et des obligations à un simple outil, mais aussi de faire éclater les frontières entre l'homme et la machine, ouvrant ainsi la voie à une confusion entre le vivant et l'inerte, entre l'humain et l'inhumain... »

Accorder le statut de personne à une entité non vivante et non consciente serait donc une erreur, puisque cette solution risquerait à terme de ravalier l'Homme au rang de simple machine. Les robots doivent être placés au service de l'humanité et ne sauraient avoir d'autre place, sauf à verser dans la science-fiction.

3.2. Remarques diverses concernant la responsabilité des dommages causés par un robot autonome

Au regard des nombreux éléments contenus dans la proposition de résolution, qui ne peuvent être examinés en profondeur dans le cadre limité de cette analyse, nous pouvons souligner plusieurs points qui méritent réflexion.

1°/ En matière de responsabilité civile, il convient d'abord de prendre garde aux qualificatifs employés dans le futur instrument. Il faudrait bannir les expressions « responsabilité des/du robot(s) » (paragraphe 26 ; annexe à la proposition de résolution), qui laissent croire que le robot pourrait être lui-même responsable civilement de ses dommages, mais employer à leur place « responsabilité du fait des/du robot(s) ».

2°/ La détermination du responsable en cas de dommages causés par un robot autonome pose difficulté.

D'une manière classique, les dommages causés par les robots autonomes pourraient trouver leur origine dans un défaut de la machine, ce qui permettrait de mettre en œuvre la directive 85/374/CEE du Conseil du 25 juillet 1985, à la condition d'en remplir les conditions. On trouve cela parfaitement décrit au point Y de la proposition de résolution. Cette directive pourrait trouver à s'appliquer dans de nombreuses circonstances, notamment lorsque le producteur n'aurait pas assez

informé le client sur les dangers du robot autonome, ou lorsqu'il existerait une insuffisance des systèmes de sécurité sur le robot. On peut donc estimer que certains dommages liés aux nouvelles capacités des robots autonomes pourraient constituer un défaut au sens de la directive, ce qui répondrait partiellement aux interrogations soulevées par le point Z de la proposition.

Les dommages causés par les robots autonomes pourraient encore trouver leur origine dans un mauvais usage par leurs utilisateurs. Il pourrait alors y avoir lieu à application d'un régime de responsabilité sans faute ou pour faute, selon les hypothèses. Toutefois, les robots autonomes présenteront des difficultés supplémentaires et inédites, puisqu'il pourrait être plus difficile de déterminer l'origine du dommage dans certaines situations, notamment lorsque le robot sera capable d'apprendre par lui-même de nouvelles choses. Cependant, il ne convient pas de considérer « qu'il y a lieu d'adopter de nouvelles règles permettant d'imputer (totalement ou partiellement) à une machine ses actes ou son inaction » (point S de la proposition). Eu égard au fait qu'il serait dangereux de retenir l'existence d'une personnalité juridique du robot (voir 3.1.), il est alors exclu de pouvoir lui imputer, en tout ou partie, ses actes ou ses inactions. Seul l'homme, avec l'appui des divers mécanismes assurantiels, doit en supporter la responsabilité.

S'agissant du fondement de responsabilité, le paragraphe 27 de la proposition est fort intéressant puisqu'il indique que « le futur instrument législatif devrait prévoir l'application par défaut de la responsabilité stricte, en vertu de laquelle il suffit d'apporter des preuves des dommages et de la relation de cause à effet entre les dommages et le comportement dommageable du robot ». Il s'agirait donc d'un régime de responsabilité sans faute, qu'il serait possible de qualifier de « responsabilité du fait du robot ». Dans cette occurrence, la double preuve reposerait sur la victime du dommage. Toutefois, même dans ce cas de figure, il resterait délicat de déterminer le répondant final, c'est-à-dire le véritable responsable.

A cet égard, le paragraphe 28 de la proposition offre une méthode pour évaluer les responsabilités de chacune des parties, puisqu'il énonce qu'« *en principe, une fois les parties responsables en dernier ressort identifiées, leur responsabilité serait proportionnelle au niveau réel d'instructions données au robot et à l'autonomie de celui-ci ; dès lors, plus un robot est autonome ou plus sa capacité d'apprentissage est grande, moindre devrait être la responsabilité des autres parties et, plus la période d'"éducation" du robot a été longue, plus grande devrait être la responsabilité de son "enseignant" ; relève notamment que, lorsqu'il s'agit de déterminer la responsabilité réelle des dommages, les compétences acquises par*

un robot au cours de son "éducation" ne devraient pas être confondues avec les compétences strictement dépendantes de sa capacité à apprendre de manière autonome ». Ce texte livre de nombreuses idées à approfondir. Il faudra faire en sorte que le futur instrument soit plus précis et plus simple à mettre en œuvre. On peut craindre, en effet, que les juges peu versés dans les technologies émergentes aient des difficultés à en appréhender les subtilités.

Ainsi, lorsque les conditions d'application de la directive 85/374/CEE du 25 juillet 1985 ne seront pas réunies, la victime pourrait trouver d'autres responsables. Plusieurs idées méritent attention :

Lorsque le robot sera vendu en open source, la personne responsable devrait, en principe, être celle qui aura élaboré l'application du robot lui ayant permis d'occasionner un dommage. Il convient de préciser que les robots tendent de plus en plus à être vendus en open source (en tout ou partie) pour permettre aux acheteurs de développer leurs propres applications. Un contrat régit, en principe, les rapports entre les parties. Il existe également le courant *Open Robot Hardware*, où le logiciel et le matériel du robot sont en *open source*.

Lorsque le robot aura causé un dommage qui trouvera son origine dans la conception ou la fabrication du robot, le concepteur ou le fabricant devrait être considéré comme responsable. Par exemple, une erreur dans

l'algorithme d'un robot qui serait à l'origine d'un comportement dommageable du robot. Toutefois, en l'occurrence, la nature de la responsabilité pourrait varier selon que la victime serait l'acquéreur du robot (responsabilité relevant du domaine contractuel) ou un tiers (responsabilité relevant du domaine extracontractuel). Il pourrait être important dans le cadre du futur instrument de s'interroger sur cette dichotomie et de vérifier s'il ne serait pas pertinent d'uniformiser son application, à l'image de la directive 85/374/CEE qui ne distingue pas selon que la victime est ou non liée par un contrat avec le producteur responsable du dommage.

Lorsque le robot aura causé un dommage qui trouvera son origine dans son usage ou sa période d'apprentissage du robot, il faudrait que son utilisateur ou son propriétaire soit désigné comme responsable. A cet égard, il faut noter que la solution pourrait varier selon que l'utilisateur serait ou non professionnel, et selon qu'il serait ou non la victime. Ainsi, un dommage lié à l'apprentissage du robot par un utilisateur professionnel qui serait causé à une victime tiers pourrait suivre le régime du nouvel instrument. Tout autre serait le cas du même dommage mais dont la victime serait l'utilisateur professionnel salarié lui-même, qui devrait alors s'analyser en un accident du travail.

Par ailleurs, il conviendra de prendre en compte l'existence d'hypothèses variées, telles que la location du robot qui devrait

tendre à se développer, à l'image de la location des robots commerciaux destinés à la démonstration de produits ou à la publicité dans les magasins. Cependant, il pourrait être impossible de faire peser la responsabilité sur un client donné. En effet, une succession de magasins aurait loué le robot, de sorte que l'on pourrait avoir des difficultés à déterminer la responsabilité de chacun en termes d'apprentissage du robot. Ainsi, sauf preuve contraire, on devrait partir du principe que le loueur du robot reste le responsable.

3°/ Il convient de noter une difficulté que pourrait poser l'instauration d'un régime de responsabilité spécifique pour les robots autonomes, tandis que les autres robots seraient soumis aux régimes classiques. En effet, en cas de dommage, les parties pourraient préférer bénéficier d'un régime plutôt que d'un autre. Les juges seront alors contraints, au cas par cas, d'analyser les caractéristiques du robot en litige, afin de vérifier s'il répond à la définition des robots intelligents au sens de la présente proposition et de déterminer la loi applicable. Il en découle que les procès en cas de dommage causé par un robot risqueraient d'avoir toujours comme préalable la nécessité d'une expertise pour déterminer les capacités de la machine. Cela aurait pour effet d'augmenter considérablement les coûts des procès et de ralentir les procédures judiciaires. A cet égard, une application uniforme des futures dispositions à tous les robots pourrait

constituer une solution, étant entendu que seuls les robots autonomes poseraient de véritables difficultés en termes de détermination du responsable.

4°/ Il faut approuver pleinement l'idée développée par la proposition selon laquelle « *ledit instrument ne devrait en aucune manière limiter le type ou l'étendue des dommages qui peuvent faire l'objet d'un dédommagement, et ne devrait pas non plus limiter la nature de ce dédommagement, au seul motif que les dommages sont causés par un acteur non-humain* » (paragraphe 26). En effet, il ne faudrait pas prendre pour prétexte que le robot soit à l'origine d'un dommage pour diminuer l'indemnisation de la victime ou restreindre les préjudices indemnisables.

5°/ Il est encore nécessaire de préciser que la situation des robots mobiles est actuellement peu claire, tant en termes de sécurité que de responsabilité. Or, les robots autonomes seront le plus souvent mobiles, et pourront même être amenés à transporter des biens ou des personnes. Il conviendrait de bien clarifier dans le futur instrument les règles applicables aux robots autonomes mobiles, par exemple, à l'égard de la directive 2007/46/CE du Parlement européen et du Conseil du 5 septembre 2007 établissant un cadre pour la réception des véhicules à moteur, de leurs remorques et des systèmes, des composants et des entités techniques destinés à ces véhicules, ainsi que face aux questions relatives à la

responsabilité, notamment au regard de la question des accidents de la circulation.

6°/ Enfin, bien que la proposition de résolution n'ait pas pour objet la responsabilité pénale, il convient de relever la grande difficulté de cette question en robotique autonome, tant en termes de constitution d'une infraction, que de détermination de son auteur, de preuve de l'intention, de lien de causalité, etc. Cette situation devrait avoir une incidence sur la responsabilité civile.

4. ANALYSE DES PRINCIPES ÉTHIQUES À DÉVELOPPER EN ROBOTIQUE : voir l'étude originelle

[http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU\(2016\)571379_FR](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_FR).

SCIENCES APPLIQUEES



Les débuts de la robotique civile et militaire introduisent un nouveau paradigme dans le champ des études de la sphère anthropologique. Cette dernière partie, consacrée aux sciences appliquées de la robotique, sensibilise à ce paradigme en abordant des enjeux de civilisation : la vieillesse et la dépendance, la voiture autonome liée à la liberté d'aller et de venir et la conduite de la guerre. L'autonomie grandissante confiée à des entités douées d'une intelligence artificielle interroge dès lors sur leur place au sein d'un processus décisionnel et dans son sillage de la détermination de la chaîne de responsabilité idoine.

Robots autonomes, société et sécurité publique

par **THIERRY DAUPS**

L

Le droit de la robotique : le droit de l'autonomie du "bien" robot

Le robot est juste une machine de plus, mais pas n'importe laquelle. C'est une machine qui dotée de l'intelligence artificielle, dispose d'une autonomie qui, dans le cadre d'une mission, lui donne la capacité d'analyser son environnement, de s'y situer, d'identifier une difficulté, pour exécuter matériellement, seule ou en coopération avec un être humain, la solution trouvée. L'autonomie conduit le robot à prendre des décisions qui s'imposeront à la personne humaine et à



THIERRY DAUPS

Maître de conférences
Université de Rennes 2
Chercheur associé
CREC
Saint-Cyr Coëtquidan

la société qui l'utilisera. Dès lors, parce que le robot autonome est par nature un système coopératif, il s'insère dans la relation entre l'être humain et la société, ou dans un

groupe d'êtres humains, et les contraint à repenser leurs relations avec une machine assimilée à un tiers artificiel. D'où, la tentation de franchir le pas et, par anthropomorphisme, d'apparenter le robot à une personne ; un pas que l'on se garde de faire pour éviter de brouiller la perception de sa réalité juridique et certains des fondements du droit. Déterminer la nature juridique du robot autonome est donc un préalable incontournable qui conditionne son régime juridique et le droit de la robotique.

Le robot autonome : un bien, pas une personne

C'est une question juridique essentielle. La réponse orientera à la fois le droit et l'économie de la robotique. En effet, l'intelligence artificielle constitue la spécificité du robot autonome et donc une difficulté juridique. Faut-il envisager l'hypothèse d'une personnalité juridique électronique, robot, ou encore matérielle¹, afin de doter le robot de droits et de



« Outre l'approche sentimentale fondée sur l'attachement qu'un être humain peut avoir pour un objet, l'intelligence du robot, autorise une assimilation avec d'autres statuts. »

devoirs, ou bien doit-on rester dans l'orthodoxie juridique : le robot autonome est a priori un meuble, malgré sa nature particulière?

Examinons d'abord l'hypothèse d'une personnalité juridique spéciale. Outre l'approche

(1) On citera le projet de rapport de la députée Mady Delvaux, contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, Commission des affaires juridiques, du 3 mai 2016, PR1095387FR.doc ; le rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques, sur « Les robots et la loi », compte rendu de l'audition publique du 10 décembre 2015 et la présentation des conclusions du 3 mars 2016, par J.Y. Le Déaut député et B. Sido sénateur, Assemblée nationale n°3551 et Sénat n°570 ; SYMOP, droit de la robotique, Livre blanc, 2016. Ainsi le rapport Delvaux propose de retenir la personnalité électronique du robot et A. bensoussan dans son ouvrage : Droit des robots, Editions Larcier, 2016, 149 p., propose la personnalité robot. L'auteur de l'article pensait à l'hypothèse d'une personnalité matérielle, pour décrire un bien matériel doté d'une personnalité en raison de son « intelligence », sans cependant suivre cette hypothèse.

sentimentale²
fondée sur
l'attachement
qu'un être humain
peut avoir pour un
objet, l'intelligence
du robot, autorise
une assimilation
avec d'autres
statuts³. D'abord
celui de l'animal⁴
qui bien qu'étant
juridiquement un
meuble ou un
immeuble par
destination,

dispose d'une protection pénale en tant qu'être vivant sensible. Ensuite on peut évoquer celui des personnes morales qui

(2) A. Bensoussan, Droit des robots, Editions Larcier, 2016, 149 p. ; Lucia Sillinge, Donnons des droits aux robots, Le Monde science et techniques, du 17 février 2013, cite la chercheuse du MIT Kate Darling, pour laquelle, il serait possible d'attribuer des droits secondaires comme pour les animaux, car protéger les robots sociaux, revient aussi à protéger la société.

(3) M. Cahen, avocate, Le droit des robots, sur site internet Avocat online.

(4) A. Bensoussan, Droit des robots, Editions Larcier, 2016, 149 p ; l'auteur effectue cette comparaison.

disposent d'un statut très proche de celui de la personne physique. Dès lors que le droit attribue la personnalité juridique à d'autres entités que l'être humain ; pourquoi n'en serait-il pas de même pour le robot intelligent ? Doté d'une personnalité juridique, on établirait le régime juridique de

droits et d'obligations du robot comprenant les normes liées à sa conception, sa production, sa distribution, à son usage, sans oublier celles qui

(5) A. Bensoussan, *Droit des robots*, Editions Larcier, 2016, 149 p

(6) Un bien est soit meuble ou immeuble (article 516) ; il est en principe objet de la propriété d'un particulier, sinon il est administré (article 537). On en déduit la responsabilité de la personne qui a la garde la chose (article 1242).

empêcheraient d'attenter au robot⁵. Surtout, en cas de dommages causés à un tiers, le robot responsable serait couvert par un système d'assurance, et un fonds de

garanties, indemniserait « ses victimes ». En effet, comment le passager d'un véhicule autonome serait-il responsable d'un véhicule qu'il ne conduit pas matériellement ? On le voit, cette hypothèse bouscule les principes fondateurs du droit et implique l'irresponsabilité des propriétaires, des utilisateurs, des concepteurs et des fabricants de robots, au profit d'un système substitutif centré sur le robot tout en écartant la réalité physique du robot : un bien, propriété d'une personne morale ou physique.

Le robot reste un bien meuble ou immeuble par destination. On remarquera que pour le code civil⁶, l'intelligence ne constitue pas un critère de classification des biens meubles ou immeubles entre eux. Le code civil distingue entre ce qui est humain, ce qui ne l'est pas et différencie ensuite entre ce qui est vivant et non. En conséquence, tout ce qui n'est pas humain ne peut être qu'un bien meuble ou immeuble. L'animal, la fourchette, le robot autonome, ne peuvent être que des biens meubles ou

immeubles par destination. Toutefois, l'animal, meuble ou immeuble par destination, disposera d'une protection pénale en tant qu'être vivant naturel sensible, au contraire du robot artificiel et insensible. L'intelligence justement artificielle du robot, ne justifie pas son assimilation à l'animal, ni sa distinction juridique d'un bien qui en serait dépourvu comme la fourchette. Egalement bien matériel, le robot, ne correspond pas à la fiction juridique de la personnalité morale. En conséquence, le robot autonome reste bien la propriété d'une personne physique ou morale, dont le gardien effectif assume la responsabilité pour les dommages causés à autrui. Reste à déterminer le gardien de cette autonomie ; ce que l'on verra plus loin.

En conclusion, le robot autonome est un bien meuble ou immeuble par destination, mais un bien spécial en raison de son autonomie, laquelle oblige à réévaluer les règles traditionnelles de la responsabilité. Cette option conduit à la tentative de définir le droit de la robotique.

Le droit de la robotique, droit de l'autonomie robotique

L'intelligence artificielle oblige tant les chercheurs, que les concepteurs, les fabricants et les utilisateurs, la société à réfléchir aux conditions éthiques et juridiques pour concevoir une société humaine fondée sur un juste équilibre entre les robots, les êtres humains et la

société dans laquelle ils évoluent. Ici, l'éthique intervient pour penser la place du robot dans ce triangle et les actions qu'il peut effectuer ou non. Mais l'éthique n'est pas le droit. Il revient

(7) On pense ici qu'il ne faut pas assimiler l'éthique au droit. Ainsi s'il faut bien envisager les questions éthiques : morales, posées par la robotique notamment pour anticiper la résolution de conflits insolubles par le robot, il revient au droit, par des normes juridiques légalement établies, exécutées et sanctionnables, de préciser tous les aspects juridiques liés à la robotique. Ainsi plus qu'une charte éthique de la robotique, faut-il une charte véritablement juridique de la robotique. La norme juridique non contractuelle est une garantie pour le citoyen – consommateur.

(8) On vise ici le processus informatique de « réflexion » du robot pour analyser une situation de fait.

(9) On parle ici de l'action physique du robot : contourner un obstacle, tirer...

(10) On veut dire ici une volonté issue de la mise œuvre de sa programmation laquelle donne à cette machine la capacité à décider seule ou presque, d'une action juridiquement qualifiable.

(11) Identifier une personne, décider d'un tir, s'arrêter à un stop sur la voie publique...

à la norme juridique⁷, internationale, constitutionnelle, à la loi et au juge, de déterminer les fondements et les adaptations juridiques du droit actuel face à la contrainte de l'autonomie. Ainsi, avant d'aborder le champ du droit de la robotique qui serait le droit de l'autonomie robotique, il faut tenter de définir cette dernière en droit.

L'autonomie robotique serait la capacité juridique, immatérielle⁸ et matérielle⁹ du robot, de par son « interprétation » (volonté propre¹⁰ ?), de décider, dans le

cadre de ses compétences, d'une action juridiquement qualifiable¹¹ opposable à un tiers et contrôlable (sanctionnable), soit par l'être humain sur l'instant, soit a posteriori lors d'un litige, et pouvant

entraîner la mise en cause de la responsabilité d'une personne morale ou physique de droit public ou de droit

(12) On n'indique pas la personne car celle-ci selon les circonstances de fait, pourrait être le servent du robot, la hiérarchie du servent, ou encore le fabricant, le concepteur, etc.

(13) pparaissent trois situations, issues de la marge de manœuvre laissée par la personne publique ou privée laquelle, de par sa compétence hiérarchique, aura décidé d'utiliser le robot en coopération avec l'être humain. En premier lieu, le couple « humain – robot » est sous l'autorité totale de la personne qui a décidé de leur emploi. En second lieu, le couple 'humain – robot » est sous l'autorité partielle de la personne qui les envoie en mission. Et en troisième lieu, ce couple dispose d'une large compétence discrétionnaire dans l'exécution de sa mission par rapport à l'autorité hiérarchique qui recourt à leur intervention.

privé¹². En conséquence, il faut indiquer juridiquement la compétence de chacun des intervenants, la nature et la portée de leurs actes juridiques, sans oublier de préciser le rapport d'autorité ou de subordination du robot au regard de l'être humain et ou de l'institution qui en use¹³. Dès lors, l'autonomie décisionnelle revient à s'interroger sur les conditions dans

lesquelles un robot peut juridiquement prendre une décision valable, exécutable par lui et opposable à une tierce personne. Ainsi définie, l'autonomie robotique conditionne le droit de la robotique.

Le champ du droit de la robotique couvrirait deux grands domaines : le droit fondamental de la robotique et le droit matériel de la robotique. Le droit fondamental de la robotique définirait le robot, son autonomie et les principes de la responsabilité. Il formaliserait juridiquement un certain nombre de

principes éthiques essentiels à la bonne conception et au bon usage du robot par la société et l'être humain. Il préciserait également les conditions générales de l'utilisation militaire et sécuritaire du robot. Enfin, il poserait les conditions de l'indépendance d'une autorité de la robotique, chargée de contrôler l'effectivité de ces fondements de la robotique en liaison avec les autorités indépendantes chargées de l'informatique. Le droit matériel de la robotique concernerait les normes liées à la conception, la production, la distribution et l'utilisation des robots ; il préciserait également les adaptations juridiques justes nécessaires dans les activités et les lieux où sont utilisés les robots.

On peut maintenant indiquer les principes qui permettraient de concevoir une société d'êtres humains et de robots pour voir ensuite les incidences du robot dans le domaine de la sécurité publique.

CONCEVOIR UNE SOCIÉTÉ D'ÊTRES HUMAINS ET DE ROBOTS

Appelé à évoluer sous des formes diverses, en tout lieu où l'être humain intervient, pour accomplir des missions sécuritaires, militaires, d'aide à la personne, de conduite d'un véhicule ou tout autre activité, le robot occupera une place dans la société humaine qu'il faut penser. Le principe de subsidiarité y contribuerait sans oublier de s'interroger sur la détermination du responsable de l'action robotique.

Subsidiarité, proportionnalité et autonomie

(14) Catherine Tessier, autonomie, enjeux techniques et prospectives, in sous dir. R. Doaré, D. Danet et G. de Boisboissel, Drones et Killers robots, faut-il les interdire, Pur, 2015, 267 p., p. 65 et s.

Le robot est un système coopératif¹⁴ qui intervient à la place de et ou en complément de l'action humaine. Le

principe de subsidiarité qui est utilisé pour justifier de l'intervention d'une personne à la place d'autres, pour un temps et une compétence déterminée en raison d'un gain d'efficacité et d'un intérêt collectif, s'appliquerait ici. En effet, ce principe réglerait les relations d'abord entre la société et le robot, ensuite entre le robot et l'être humain et enfin entre le robot, la société et l'être humain, en indiquant qui fait quoi, à quel moment et comment. Le principe de subsidiarité trouve son prolongement dans le principe de proportionnalité en obligeant à prendre la mesure juste nécessaire pour atteindre l'objectif souhaité.

Transposés au robot, les principes de subsidiarité et de proportionnalité, déterminent dans le cadre d'une mission et d'un objectif à atteindre, les critères qui conditionnent l'intervention du robot à la place de la société et de l'être humain. Ce principe indiquera également le moment opportun pour user du robot et comment il intervient. En conséquence, l'intervention du robot autonome et sa capacité d'action doivent être proportionnelles, à l'action humaine restante et au moyen matériel d'action

qu'il utilisera au regard de l'objectif à atteindre et de l'équipement des autres acteurs qui l'environnent. Enfin, l'intensité de l'usage des moyens matériels du robot devra également être proportionnelle au but visé.

Ainsi, c'est dans le cadre du principe de subsidiarité et de proportionnalité que l'on propose de comprendre l'autonomie robotique, liée à l'exercice d'une compétence, discrétionnaire ou liée. Ces deux principes conditionnent l'autonomie décisionnelle, au moyen d'une action juridiquement qualifiable et opposable à un destinataire, pour mesurer la portée et l'effectivité de la décision robotique sur des biens ou des personnes physiques ou morales. C'est dans ce cadre que l'on peut aborder le sujet de la responsabilité.

L'enjeu central de la responsabilité

L'autonomie robotique pose un problème juridique à résoudre par les juristes, ce afin de favoriser un usage des robots sans risques juridiques pour leurs

(15) Voir la note 1.

utilisateurs. Le robot endossera-t-il¹⁵ les

conséquences dommageables de l'action robotique autonome ? Non car n'étant pas une personne juridique, il ne peut réaliser tout ce que font les personnes physiques ou morales : ester en justice, prendre un avocat, acquérir, vendre des biens pour son compte, se loger, recevoir un revenu et payer des impôts ; il ne peut être responsable de ses actes. Les

principes essentiels de la

(16) On pense à la responsabilité du propriétaire, du gardien, des choses défectueuses, tous autres régimes adaptés à des biens « inintelligents ».

(17) Il s'agit d'une hypothèse de réflexion qui n'est pas nécessairement en conformité avec le droit actuel.

responsabilité s'appliquent¹⁶ donc à un bien. Ces régimes de responsabilités conviennent-ils à un bien « intelligent » qui semble échapper à la maîtrise de la

personne qui en use, de par l'essence de son fonctionnement autonome (indépendant) et substitutif à l'être humain ?

Une réponse possible¹⁷ consiste à déterminer le responsable de l'action robotique autonome, en la replaçant dans le cadre du processus de l'intervention subsidiaire et proportionnelle du robot. La démarche part de l'autonomie du robot en recherchant son gardien effectif. On distinguera entre le gardien matériel du robot et le gardien immatériel de l'intelligence artificielle du robot. En effet, si l'on peut admettre qu'une personne qui utilise un véhicule autonome en est le gardien matériel responsable, elle ne saurait être le gardien de l'intelligence artificielle qui assure l'autonomie du véhicule. C'est bien cette intelligence artificielle qui conduit effectivement, transformant *de facto* le gardien matériel en un simple passager. Il faut donc rechercher le gardien immatériel, qui renvoie à un ensemble d'intervenants qui seraient proportionnellement responsables à hauteur de leur

intervention dans la production de cette intelligence. C'est le gardien de l'intelligence artificielle qui serait responsable des dommages causés par celle-ci.

Il est utile d'examiner d'autres hypothèses au service d'une responsabilité propre à l'autonomie robotique.

Les personnes humaines ou morales ne peuvent invoquer dans la première hypothèse, une immunité quant à l'usage de leurs robots en matière de défense et de sécurité. A plus forte raison, les actions du robot ne sont pas couvertes par une immunité du fait que c'est une machine qui a pris et exécuté une décision.

La seconde est qu'une personne physique ou morale sera toujours responsable des actions dommageables du robot autonome.

La troisième retient l'idée d'une présomption de principe de la responsabilité pour les gardiens immatériels : l'intelligence artificielle. Ceci dans un souci d'équité par rapport aux victimes qui auront bien des difficultés à prouver une faute du gardien immatériel du robot autonome. A ce dernier de prouver qu'il n'a commis aucune faute, la faute de la victime ou tout autre cause.

La quatrième pose le principe du libre accès des victimes à tous éléments matériels et immatériels de preuves afin

de faire valoir leurs droits.

La cinquième consiste à appliquer un principe d'inversion proportionnelle de la responsabilité par rapport au degré d'autonomie robotique ; plus le robot est autonome, moins l'être humain qui l'utilise est responsable car moins il est « conducteur » de l'action robotique au profit des gardiens de l'autonomie de l'intelligence artificielle : qui conduit le robot en est responsable.

On abordera maintenant la robotique et la sécurité publique

ROBOT AUTONOME ET SÉCURITÉ PUBLIQUE

L'usage de robots dans le domaine de la sécurité publique et des robots militaires, présente aussi des problèmes juridiques à explorer. Auparavant, il faut distinguer entre robotique militaire et robotique sécuritaire.

Robotique militaire et robotique sécuritaire

La robotique militaire vise à l'usage par les trois armes, de robots essentiellement télé-opérés et partiellement autonomes, dans le cadre d'opérations militaires pour assurer la sécurité nationale. C'est donc dans cadre juridique du droit des conflits armés, du droit humanitaire mais aussi du Code de la défense que ces robots sont utilisés. L'objectif d'assurer la sécurité publique sur le territoire combine des militaires et des policiers. Des robots

militaires pourraient être utilisés par les forces de gendarmerie et de police dans le but de préserver l'ordre public (et en dehors de toute idée d'opération militaire) sur le territoire d'un État, ou d'assurer d'autres missions civiles, pour protéger les populations civiles. L'usage de robots militaires par les forces de police est

(18) L'expression « et ce qui précède » provient de la réflexion de M Eric Pomes, maître de conférences au centre de recherches de Saint-Cyr Coetquidan.

qualifié de réversibilité¹⁸. Mais les forces de sécurité peuvent aussi acquérir ou concevoir leurs

propres robots adaptés à leurs missions de police.

Dans le cas d'un usage réversible de robots militaires, on s'interrogera sur leur adaptation à une mission de sécurité publique, laquelle obéit à des conditions

(19) Michel Ascencio, L'utilisation civile des drones, problèmes, techniques, opérationnels et juridiques, note du 28 mars 2008 mise à jour le 6 juin 2011, in Fondation pour la recherche stratégique, note n° 6/11, 8 p.

(20) C'est d'ailleurs la tendance actuelle, à voir le site internet du ministère de l'intérieur, qui se réfère au salon « MILIPOL » où des industriels proposent des robots et plus précisément des drones particulièrement adaptés aux besoins de la police, tel que le drone ELSA, ou d'un robot de déminage. Les besoins spécifiques de la police, réduiraient-ils l'utilité des robots militaires ? Quelle complémentarité entre robot militaire et robots spécialement conçus pour la police ?

juridiques différentes de celles de l'usage militaire, comme on le verra dans le titre suivant. La réversibilité impose également de déterminer les critères de circonstances, de moyens humains (un militaire, un policier) pour utiliser le robot militaire dans un contexte civil. C'est donc l'articulation entre les forces de police et les forces militaires qui doit être

pensée avec précision. Plus largement, cet usage civil du robot¹⁹, pose la question de l'utilisation du robot par les forces de l'ordre, qu'il soit militaire ou bien un produit spécialement conçu pour les missions assurées par les forces de l'ordre²⁰.

Enjeux de la robotique sécuritaire

L'usage de robots par les forces de police ou de gendarmerie reste conditionné par le droit existant découlant principalement des codes pénal et de procédure pénale, de la sécurité intérieure, de déontologie de la police et de la gendarmerie nationale, mais aussi du droit administratif en ce qui concerne les notions de police administrative et judiciaire et d'ordre public.

On notera ainsi que la notion d'ordre public différencie une opération de police et une opération militaire. Les finalités sont distinctes, ce qui conditionne l'usage des moyens matériels et humains. Surtout, la notion d'ordre public répond à une définition juridique issue du droit administratif qui concilie l'exercice des libertés publiques avec la nécessité d'éviter des troubles à la tranquillité, la salubrité, la sécurité et la cohésion nationale. Ce faisant, les forces de polices interviendront dans le cadre de la police administrative pour prévenir les atteintes à l'ordre public ou bien de manière répressive pour réprimer ces mêmes atteintes et en arrêter les auteurs. La

distinction conditionne le juge compétent : juge administratif dans le premier cas et juge judiciaire dans le second.

Également, si le lieu de l'intervention des forces de l'ordre peut être considéré comme un théâtre d'opération, il ne s'agit cependant pas en droit d'un champ de bataille, mais bien de l'espace public tel

(21) Loi 2010-1192 du 11 octobre 2010, JORF 0237, NOR JUSX1011390L, décision du Conseil constitutionnel 2010-613 DC du 7 octobre 2010.

(22) Le fait de coupler des caméras de vidéosurveillance à des logiciels de reconnaissance faciale.

(23) Lorsqu'une infraction est constatée par un agent de police municipale par l'intermédiaire d'une caméra.

(24) On lira avec intérêt les articles relatifs aux droits fondamentaux confrontés aux nouvelles technologies, dans la Revue de la Gendarmerie nationale, juillet 2016, n°255.

(26) On ne discute pas avec une machine ; c'est blanc ou noir, ce qui est fortement contraignant pour le citoyen, être humain par nature imparfait même s'il n'est pas un délinquant.

que défini par la loi du 11 octobre 2010²¹. Un espace où le citoyen, qui n'est pas un ennemi, perd cependant sa nature privée pour être potentiellement identifié²², traqué dissuadé et sanctionné²³ à tout moment. C'est ce que permet la technologie au risque de devoir adapter l'exercice des libertés publiques²⁴ à la contrainte technologique²⁵ pour faciliter une surveillance globale de l'individu et de la

société visant ainsi une perfection dans le respect de la loi²⁶. L'espace public est donc le lieu de l'intervention des forces de gendarmerie et de police où des robots pourraient être utilisés de manière adaptée, dans le respect des libertés

(27) On pense ici au respect de la procédure judiciaire.

(28) Il s'agit de garantir que les citoyens puissent accéder à tous documents concernant les caractéristiques techniques du robot, la mission qu'il exerce, les responsables de cette mission, l'agent responsable du robot, mais aussi d'accéder aux enregistrements de toute nature effectués par le robot dans le respect également de la loi informatique et libérée.

publiques des citoyens et en usant des outils proportionnés aux finalités de missions de police administrative et judiciaire. En conséquence, la robotique sécuritaire, devra s'effectuer dans le respect des

procédures administratives et pénales²⁷, se soumettre au régime juridique de l'accès aux documents administratifs et à la loi informatique et libertés²⁸. Surtout, il faut définir les conditions juridiques précises de l'utilisation du robot, de la détermination de son équipement par rapport à sa mission, de l'étendue des compétences qu'il mettra en œuvre au regard de celles du gendarme ou du policier qui l'accompagne et dans quels cas la décision du robot prévaut sur celle de l'agent et inversement. Quelle doit être l'attitude du robot face au citoyen ? le robot peut-il être en légitime défense ?

(29) La détermination d'une procédure pour décider d'utiliser le robot, d'une procédure pour le mettre en œuvre, d'une formation spécifique pour son servant, de la présence d'un référent robotique au sein des forces de l'ordre, d'un rapport de fin de mission, etc., sont autant de moyens qui permettront en cas d'incident de déterminer les responsabilités des uns et des autres.

Est-il autorisé à exercer un contrôle d'identité implicite ou explicite ? Ce sont là quelques exemples pour montrer qu'il est nécessaire de réfléchir à un bon usage responsable²⁹ du robot sécuritaire³⁰ : un

(30) J. Bisognin, Les systèmes de drones au cœur de la transformation numérique de la Gendarmerie nationale, in Revue de la Gendarmerie nationale, juillet 2016, n°255, p. 53 et s. Cet article montre quelle démarche soit la Gendarmerie pour utiliser des drones.

usage humaniste du robot.

Pour une robotique humaniste

Le droit renvoie à une conception de la vie en société et le droit de la robotique doit

garantir les fondements du droit de la robotique.

refléter un choix de société. Il faut réfléchir au degré acceptable et humainement supportable de robotisation de la société, pour que l'être humain reste humain, pour préserver l'humanité de la société et l'origine naturelle de l'être humain. Il faut éviter que l'être humain se réduise par un comportement standardisé à n'être que le rouage d'une « société machine ».

Ce faisant, le droit de la robotique doit s'inscrire dans le cadre de l'humanisme et de l'état de droit. Il ne doit pas se limiter à n'être que le droit des intérêts économiques des constructeurs et des utilisateurs de robots dont les fondements seraient justes garantis et imposés par une démarche purement contractuelle. Seule une charte constitutionnelle de la robotique et des nouvelles technologies,

(31) Voir le rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques, sur « Les robots et la loi », compte rendu de l'audition publique du 10 décembre 2015 et la présentation des conclusions du 3 mars 2016, par J.Y. Le Déaut député et B. Sido sénateur, Assemblée nationale n°3551 et Sénat n°570.

assise sur le droit international et européen³¹, inscrite dans la logique humaniste des textes présents dans le préambule de la Constitution de 1958,

Robots sociaux « empathiques »

en santé : quels bénéfices ?

Quelles inquiétudes ?

par ANNE-SOPHIE RIGAUD et GREGORY LEGOUVERNEUR

O

On assiste au développement croissant de robots dits sociaux et compagnons car susceptibles d'entrer en communication avec l'utilisateur dans le domaine de la santé. Ces robots sont maintenant programmés par les roboticiens pour interagir de façon naturelle avec l'utilisateur et ainsi favoriser l'engagement de celui-ci avec la machine. On parle d'empathie de la personne pour le robot et « d'empathie artificielle » du robot pour son utilisateur. De quoi s'agit-il ? Quels bénéfices pouvons-nous attendre de l'interaction de la personne avec les

robots sociaux ? Quelles craintes pouvons-nous avoir en particulier quand cette personne est vulnérable ?

Nous ciblerons notre article sur l'utilisation des robots pour les personnes âgées.

Le vieillissement s'accompagne d'une augmentation des maladies chroniques, comme l'insuffisance cardiaque, le diabète, la maladie d'Alzheimer, pouvant compromettre l'autonomie des personnes. Dans la mesure où les aidants familiaux et professionnels sont en nombre insuffisant pour satisfaire les besoins d'accompagnement de cette population, les technologies notamment les robots pourraient apporter une assistance complémentaire aux personnes âgées dépendantes dans l'exécution des activités de la vie quotidienne. En effet, le secteur de la robotique est en forte évolution. Les robots initialement conçus pour être utilisés dans le milieu de l'industrie sont maintenant présents au domicile,



ANNE-SOPHIE RIGAUD

Professeur, chef de service à l'hôpital Broca



GREGORY LEGOUVERNEUR

Psychologue, service du professeur Rigaud, hôpital Broca

fournissant différents services : entretien/surveillance domestique, loisirs et éducation à l'utilisateur.

Les robots sociaux assistants pourraient être particulièrement utiles dans l'aide et le soutien à la personne âgée en ciblant non seulement les aspects sécuritaires et le suivi médical, mais également d'autres aspects de l'accompagnement tels que la stimulation cognitive, la socialisation, le bien être psychologique et la qualité de vie. Ainsi, le robot social d'assistance aurait deux objectifs, d'une part renforcer et/ou compenser la capacité fonctionnelle de la personne, et d'autre part contribuer à son bien-être social et psychologique et au maintien de sa qualité de vie par un compagnonnage (Broekens et al 2009).

Certains robots, appelés robots émotionnels, sont conçus pour interagir avec les humains et sont capables de réagir à certains stimuli de différentes natures : visuels, vocaux, tactiles, kinesthésiques, émotionnels, cognitifs et socio-comportementaux (Broekens et al 2009). Ils pourraient susciter chez les personnes des émotions positives, telles que la curiosité, la tendresse et la joie, voire de l'empathie c'est-à-dire donner l'impression à l'utilisateur qu'il comprend ses sentiments et ses émotions.

Des recherches récentes en robotique visent également à programmer ces robots pour qu'ils puissent interagir de façon naturelle avec l'utilisateur. L'objectif est que le robot identifie les affects de la personne, c'est-à-dire son état d'esprit lié à ses émotions et à ses sentiments par le biais

de capteurs sensoriels (visuels, audio voire tactiles) et qu'il réagisse en produisant une réponse appropriée et positive à la sollicitation de la personne, notamment en manifestant de l'empathie à son égard. Cette empathie est dite empathie artificielle puisque produite par la machine (Tisseron et al 2015).

Quels facteurs déterminent l'affection et l'empathie de la personne à l'égard d'un robot social ?

Certains facteurs sont liés au robot (Broadbent et al 2009, Tapus et 2007).

L'aspect du robot est un point essentiel pour que la personne puisse l'accepter et développer des émotions positives voire de l'empathie à son égard. En effet, les robots ont différentes formes ;

humaine/humanoïde, animal/animaloïde, machine, meubles.... Nous avons fait une présentation de photographies et de vidéoclips de 22 robots différents en action à des personnes âgées, puis les avons invitées à choisir leurs 3 robots préférés (Wu et al 2012). Les personnes âgées préféraient les robots qui avaient une petite taille et une forme stylisée, arrondie, discrète et familière. En particulier, les robots préférés étaient Mamoru : « *il est mignon, familial, petit, discret* », NAO « *il est charmant et amusant, il fait bien du Tai-shi* » et Pomi : « *il est sympathique, mignon, il a un côté jouet* ». Ces personnes manifestaient leur réticence aux robots androïdes (ayant l'aspect d'un humain) car, selon eux, ces robots « prétendaient » avoir des caractéristiques des êtres vivants. Ce résultat est en accord avec les travaux de Mori (1970) qui a

énoncé que lorsqu'un robot avait une apparence trop proche de l'humain (zone appelée vallée de l'étrangeté), il créait un sentiment de malaise et de rejet de la part des utilisateurs.

La personnalité « empathique » du robot, en particulier le fait que le robot paraisse comprendre les émotions de son utilisateur, est un facteur important pour déterminer des émotions positives chez cette personne. Nous avons proposé à des personnes âgées souffrant de troubles cognitifs des séances de rééducation psychomotrice guidées par un thérapeute assisté du robot NAO. Un ingénieur a programmé le robot NAO pour qu'il soit capable de communiquer et qu'il donne l'impression de comprendre l'émotion de l'interlocuteur (empathie artificielle) et d'exprimer ses émotions propres. En particulier, lors de la séance, NAO a donné son avis, exprimé son état émotionnel, encouragé et complimenté la personne. NAO a également été programmé pour montrer des comportements d'engagement à l'égard de son interlocuteur : NAO regardait la personne et lui proposait de le regarder et de reproduire ses gestes. Les résultats ont montré que les personnes étaient fortement engagées dans l'interaction avec le robot comme en témoignaient des phrases du discours des personnes à NAO : « *tu es gentil et mignon, tu es drôle* », « *tu parais fatigué* », « *je vois que tu es content* », « *je suis fière de tes compliments* » ; « *j'espère que je ne te déçois pas* » (Rouaix et al 2017).

Le fait d'avoir des émotions positives voire de l'empathie à l'égard d'un robot tient

également à des facteurs individuels, liés à la personne (Broadbent et al 2009, Tapus 2007). Ainsi, l'âge joue un rôle traditionnellement important dans l'acceptation des robots. Les sujets jeunes ont une vision plus positive des robots que les personnes âgées. Cependant, les travaux de la littérature ainsi que notre propre expérience nous ont montré que beaucoup de personnes âgées pouvaient avoir des sentiments positifs à l'égard des robots. Par exemple, dans nos expérimentations, 9 personnes sur 10 avaient plaisir à manipuler le robot phoque Paro et à interagir avec lui (De Sant'Anna et al 2012, Wu et al 2014).

Les besoins et attentes des personnes jouent également un rôle important. Lorsque nous avons présenté des robots à des personnes âgées en bonne santé, celles-ci attendaient de nombreux services de leur part et étaient déçus par l'insuffisance des fonctionnalités proposées par ces robots (Wu et al 2012).

L'expérience de l'utilisateur dans le domaine des technologies est également un point à souligner. En effet, les personnes qui utilisent des robots ont souvent un moment

REMERCIEMENTS

Nous remercions l'Agence Nationale de la Recherche (ANR), la Caisse Nationale de Solidarité pour l'Autonomie (CNSA) dans le cadre du projet TECSAN (projet Robadom ANR 09 Tecs 012) ainsi que le département Direction des Patients, Usagers et Associations, Département Qualité de vie à l'hôpital (AP-HP) dans le cadre du projet Robin pour leur participation au financement des travaux cités dans cet article.

d'inquiétude à l'idée de n'être pas capables de l'utiliser du fait d'un manque de connaissances dans le domaine des outils techniques. Il est donc important de faire des robots facilement utilisables par ces personnes.

Les fonctions cognitives sont bien sûr à prendre en compte. Les personnes auront plaisir à interagir avec des robots s'adaptant à leurs capacités cognitives, selon que celles-ci sont intactes ou altérées comme au cours de la maladie d'Alzheimer.

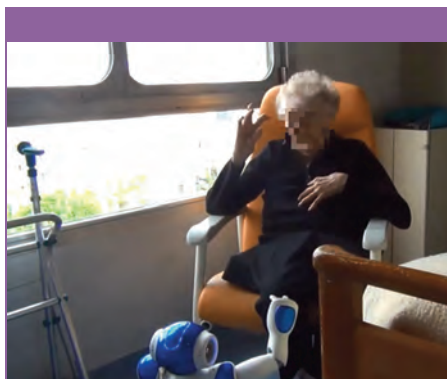
Pourquoi les robots sociaux sont-ils prometteurs dans l'accompagnement médical des personnes ?

Le fait de développer des émotions positives à l'égard du robot, voire une empathie, peut être utilisable dans le domaine médical au bénéfice du patient. En effet, cette interaction naturelle permet au robot d'être mieux accepté par la

personne et donc d'être plus utile pour l'aider et la soutenir. Le robot cesse d'être une machine et évolue vers le statut de partenaire ou de compagnon, permettant un meilleur engagement et une meilleure adhésion de la personne avec en conséquence une meilleure efficacité du programme thérapeutique.

Nous avons observé le comportement de personnes souffrant de maladie d'Alzheimer à des stades sévères lors d'une intervention comportant des séances répétées d'interaction avec le robot Paro. Avant l'intervention, ces personnes étaient repliées sur elles-mêmes et avaient quasiment cessé la communication avec leur environnement. Au fur et à mesure des séances d'interaction avec le robot, nous avons observé une reprise de la communication de ces personnes se manifestant par des échanges non seulement avec le robot mais également avec les thérapeutes et entre elles. Nous avons également observé que l'intervention avec le robot Paro favorisait davantage les interactions des personnes entre elles et avec les thérapeutes que d'autres activités comme le lancer de ballon ou le jeu de bingo (de Sant'Anna et al 2012, Wu et al 2014). Nos résultats confirment ceux d'autres travaux de la littérature (pour revue voir Broekens et al 2009).

Nous avons examiné la capacité du robot NAO à susciter l'engagement de personnes âgées souffrant de troubles cognitifs au cours de séances de thérapie psychomotrice (Rouaix et al 2017). Chaque personne a bénéficié de séances de



Une empathie positive participe à un processus thérapeutique.

thérapie psychomotrice classique (en présence du thérapeute seul) et de séances de thérapie à médiation robotique (en présence du thérapeute et du robot). Les résultats ont montré un engagement important des participants dans les deux conditions. Cependant, les manifestations de plaisir étaient plus importantes lorsque le robot accompagnait le thérapeute que lorsque ce dernier était seul. Enfin, plusieurs patients qui refusaient de faire la séance de thérapie classique avec le thérapeute seul ont accepté de participer lorsque celui-ci a introduit le robot. Ainsi le robot NAO pourrait jouer un rôle de médiateur, en particulier lorsque le thérapeute éprouve des difficultés pour trouver des leviers motivationnels et d'adhésion à la thérapie.

Ce bénéfice du robot, comme outil de médiation, a également été montré par Kim et al (2015) qui ont étudié le bénéfice d'un programme de stimulation cognitive dispensé 90 minutes par jour, pendant trois mois, chez deux groupes de personnes âgées : un groupe utilisant une tablette et l'autre un robot. A l'issue du programme, les auteurs ont montré que les personnes bénéficiant du robot avaient de meilleures performances que les personnes ayant fait les exercices sur tablettes.

Dans toutes ces expérimentations, les personnes âgées insistaient sur le plaisir à interagir avec le robot et exprimaient des émotions positives voire de l'empathie à l'égard du robot. On peut donc suggérer que le robot favorisait l'engagement, la motivation et l'adhésion de la personne

aux différents programmes thérapeutiques et contribuait à leur efficacité.

Nous noterons cependant que l'ensemble de ces travaux, bien que très prometteurs, restent préliminaires et sont à poursuivre afin de démontrer le réel bénéfice des robots pour les personnes sur le plan médical, social et médico-économique.

Pourquoi l'accompagnement des personnes par les robots sociaux entraîne-t-il des craintes ?

Les effets bénéfiques des robots sociaux pourraient être contrebalancés par des effets négatifs.

Pour Sparrow et Sparrow (2006), proposer des robots aux personnes constitue une duperie de l'utilisateur. Il ne serait pas éthique d'entretenir l'illusion que ces robots émotionnels, sociaux ou compagnon pourraient être de véritables partenaires pour les personnes, en particulier celles souffrant de troubles cognitifs. Selon ces auteurs, les robots émotionnels joueraient un rôle de déshumanisation. Ils pourraient d'abord compléter, puis progressivement remplacer les aidants familiaux ou professionnels auprès des personnes âgées malades entraînant une réduction voire une disparition des contacts sociaux de ces personnes. En parallèle, la question d'une dépendance progressive de la personne au robot peut être posée.

Ces mêmes auteurs se sont interrogés sur le risque d'infantilisation des personnes âgées souffrant de troubles cognitifs par les robots. Enfin, d'autres auteurs ont noté que l'utilisation des robots renvoyait à

certaines personnes âgées une image déficitaire de leur vieillissement, c'est-à-dire l'image d'une personne devant être assistée dans le quotidien, dont elles tentaient de se démarquer en refusant l'introduction du robot à leur domicile (Wu et al 2012).

Sharkey et Sharkey (2012) ont insisté sur les questions éthiques liées à l'utilisation des robots et la nécessité de mettre un cadre éthique à ces nouvelles formes d'accompagnement. En particulier, la liberté de la personne âgée, d'accepter ou de refuser l'usage du dispositif proposé est un des aspects qui méritent une réflexion approfondie lors de l'utilisation de ces technologies.

Enfin, d'autres points majeurs ont été abordés dans la littérature comme la question de l'accessibilité des robots pour tous du fait de leurs coûts élevés, celle de la détermination de la responsabilité juridique en cas d'accident impliquant un robot ou encore celle de la gestion des données numériques de santé issues du suivi des personnes accompagnées au quotidien par un robot (Grinbaum et al 2017).

Les robots sociaux ont un rôle prometteur en santé. En sollicitant l'engagement de la personne et en apportant du plaisir à l'intervention, ils pourraient favoriser l'alliance thérapeutique et le bénéfice thérapeutique de l'intervention. Dans ce contexte, développer des interfaces favorisant des interactions naturelles entre robot et utilisateur apparaît un véritable enjeu pour

une mise en œuvre optimale de ces interventions pour les personnes.

Cependant, il reste à poursuivre la démonstration des bénéfices des robots comme soutien et compagnon dans la vie quotidienne des personnes. Il faudra aussi continuer la réflexion éthique et développer des guides d'utilisation (indications et méthodes) de ces outils robotiques en santé pour les personnes.

Références

- Broekens J, Heerink M, Rosendal H (2009). Assistive social robots in elderly care: a review. *Gerontechnology*; 8:94-103.
- Broadbent E, Stafford R, MacDonald B (2009). Acceptance of healthcare robots for the older population: Review and future directions. *International Journal of Social Robotics*; 1:319-30.
- de Sant'Anna M, Morat B, Rigaud A (2012). Adaptabilité du robot Paro dans la prise en charge de la maladie d'Alzheimer sévère de patients institutionnalisés. *NPG*;12:43-8.
- Grinbaum, A., Chatila, R., Devillers, L., Ganascia, J. G., Tessier, C., & Dauchet, M. (2017). Ethics in robotics research: CERNA recommendations. *IEEE Robotics & Automation Magazine*.
- Kim GH, Jeon S, Im K, Kwon H, Lee BH, Kim GY, et al. (2015) Structural Brain Changes after Traditional and Robot-Assisted Multi-Domain Cognitive Training in Community-Dwelling Healthy Elderly. *PLoS ONE* 10(4): e0123251. doi:10.1371/journal.pone.0123251
- Mori M (1970) Bukimi no tani: the uncanny valley. *Energy* 7(4):33-35 (in Japanese). English translation provided at CogSci'05 workshop: toward social mechanisms of android science, views of the Uncanny Valley. WWW, <http://www.androidscience.com/theuncannyvalley/proceedings2005/uncannyvalley.html>.
- Rouaix N, Letru-Chavastel L, Rigaud AS, Monnet C, Lenoir H, Pino M (2017). Affective and engagement issues in the conception and assessment of a robot-assisted psychomotor therapy for persons with dementia. *Frontiers of aging (sous presse)*.
- Sharkey A, Sharkey N (2012). Granny and the robots: ethical issues in robot care for the elderly. *Ethics Inf Technol*; 14:27-40.
- Sparrow R, Sparrow L (2006). In the hands of machines? The future of aged care. *Minds and Machines*; 16:141-61.
- Tapus, A., Mataric, M. J., & Scassellati, B. (2007). Socially assistive robotics. *IEEE Robotics and Automation Magazine*, 14(1), 35.
- Tisseron, S., Tordo, F., & Baddoura, R. (2015). Testing Empathy with Robots: A Model in Four Dimensions and Sixteen Items. *International Journal of Social Robotics*, 7(1), 97-102.
- Wu, Y.H, Fassett, C, Rigaud, A.S (2012). Designing robots for the elderly: Appearance issue and beyond. *Archives of Gerontology and Geriatrics*. 2012; 54:121-126.
- Wu, Y. H., Pino, M., Boesflug, S., de Sant'Anna, M., Legouveneur, G., Cristancho, V., ... & Rigaud, A. S. (2014). Robots émotionnels pour les personnes souffrant de maladie d'Alzheimer en institution. *NPG Neurologie-Psychiatrie-Gériatrie*, 14(82), 194-200.

Quelle autonomie décisionnelle pour les systèmes robotiques militaires du futur ?

par GÉRARD DE BOISBOISSEL

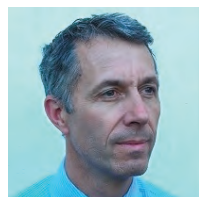
D

Depuis 2014 se tient chaque année une réunion d'experts sur les **Systèmes d'armes létaux autonomes (SALA)** à la Convention sur certaines armes classiques (CCAC) de l'ONU à Genève. Cet organisme, considéré par la France comme légitime pour traiter de ces questions, se penche sur

l'étude de la licéité de ces nouvelles armes qui équipent déjà certaines unités de l'armée russe¹.

(1) Robot russe Platform-M en version sentinelle. Cf Thierry Berthier <http://www.diploweb.com/Platform-M-le-robot-combattant.html>.

Cependant bien que l'opinion publique retienne tout d'abord la létalité comme



GÉRARD DE BOISBOISSEL

Ingénieur de recherche,
CREC Saint-Cyr

caractéristique principale des systèmes d'armes létaux autonomes, le concept d'autonomie dans son ensemble pose une question totalement nouvelle

pour les militaires : celle du degré d'autonomie qu'un chef militaire peut laisser à une machine et de la place de l'homme dans les processus décisionnels du combat.

Les systèmes robotiques d'aujourd'hui et du futur qui évoluent et évolueront sur le champ de bataille sont de plus en plus numérisés, interconnectés et permettent de nouvelles possibilités d'emploi qui révolutionnent l'art de faire la guerre : en déportant les capteurs et les effecteurs, en créant un écran robotique en avant des forces, en permettant une couverture de zone bien plus large avec une réactivité bien supérieure à celle qu'un homme peut avoir avec ses caractéristiques humaines.

Qu'est-ce qu'un système robotique militaire? En reprenant la plupart des caractéristiques citées par Catherine Tessier, chercheur à l'office national d'études et de recherches aérospatiales,



« Pour le militaire, les machines apportent un plus tactique et accroissent son efficacité. Au final, moins il sera contraint par le pilotage et le contrôle de la machine, plus il sera libre dans son action. »

c'est un système constitué d'un ou de plusieurs robots militaires. Un robot militaire est de son côté une plateforme mobile intégrant des capteurs et des effecteurs, qui évolue dans un environnement inconnu ou déstructuré, qui y acquiert des données, les interprète, prend des décisions et effectue des actions au sein de cet environnement.

Les décisions sont organisées pour atteindre des objectifs fixés par le militaire qui l'emploie et non pas simplement en réaction aux événements.

Qu'est ce que l'autonomie ?

Le robot militaire est un outil au service du combattant, un nouveau pion tactique pour celui qui l'utilise. Actuellement, la plupart des robots militaires opérationnels sont téléopérés par un opérateur qui les pilote constamment à distance ce qui

limite la capacité de liberté de ce même opérateur et augmente sa vulnérabilité s'il est un combattant débarqué. C'est un déport de l'action sous le regard constant de l'opérateur.

Certaines séquences d'exécution peuvent être automatisées. Un système automatisé a pour fonction de réaliser des tâches bien définies, qui présentent un lien immédiat entre perception et action, sans intervention humaine. L'algorithme qui déclenche l'action est pour ainsi dire relativement simple, il réagit à des stimuli selon des étapes préprogrammées par le constructeur. Le résultat d'une telle action est prévisible, car les systèmes automatiques ne sont pas innovants ne laissant pas de place à la surprise et à l'adaptation. Ils exécutent un code bien défini.

Le système autonome, quant à lui, possède un niveau d'abstraction plus élevé dans la décision et pour cela fait appel à un processus effectuant des choix qui s'appuient sur une boucle perception/décision/action. La partie « décision » est complexe car elle prend en compte plusieurs paramètres dont les règles et contraintes imposées, la planification des tâches à effectuer ainsi

(2) Gérard de Boisboissel, Revue de la Défense Nationale, juin 2016, page 142.

que l'évaluation des résultats de l'action.²

L'analyse de ces résultats par le système peut ensuite alimenter une phase d'apprentissage.

Pour le militaire, les machines apportent un plus tactique et accroissent son efficacité. Au final, moins il sera contraint par le pilotage et le contrôle de la machine, plus il sera libre dans son action. C'est ainsi qu'il est naturellement intéressé par la délégation d'une certaine forme d'autonomie à ses outils que sont les robots, sous réserve qu'il puisse en garder le contrôle.

Les différents types d'autonomie

L'autonomie est aussi une relation entre deux agents : robotique et humain. Il existe de nombreux degrés de partage de l'autonomie entre eux, un continuum allant de situations où l'homme prend toutes les décisions jusqu'à des situations où celles-ci sont totalement déléguées au robot. Les différents degrés d'autonomie peuvent être classés selon une approche graduelle pour un robot ou pour un

système robotique :

- une autonomie fonctionnelle ou de tâche permettant au robot une perception autonome de son environnement, de s'adapter et de décider seul de l'action à réaliser. La fonction est simple et généralement à but unique. Ce sont par exemple les autonomies fonctionnelles de déplacement, de recharge en énergie, d'orientation des effecteurs en fonction de la menace, etc.

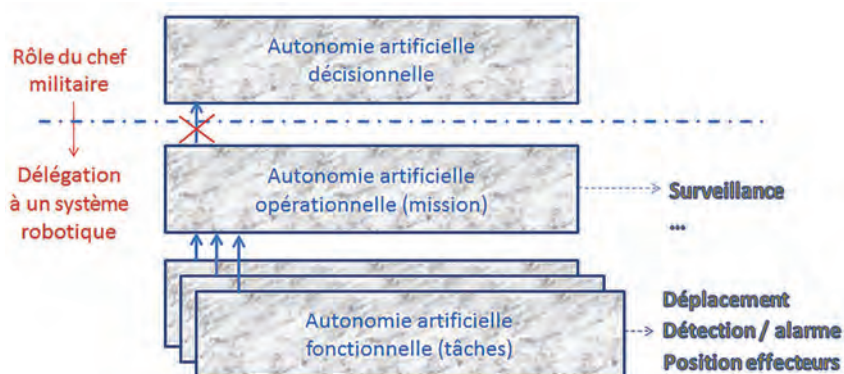
- une autonomie d'exécution de mission qui permet au robot d'effectuer cette mission sans intervention nécessaire de l'opérateur militaire durant le temps de son exécution. La mission est une activité bien plus globale, qui correspond à une somme d'autonomies fonctionnelles activées ensemble pour ce même but qu'est la mission.

- une autonomie de décision, s'affranchissant du chef militaire pour décider de ses propres objectifs. Nous verrons plus loin que ce type d'autonomie doit rester le propre de l'homme et ne présente de surcroît aucun intérêt pour le monde militaire si le chef n'a pas la possibilité de décider et d'encadrer les objectifs assignés au système robotique.

- une autonomie juridique : celle-ci implique une personnalité juridique qui soit propre à la machine et qui lui donne des droits. Dans le monde militaire et très probablement civil, une telle conception du robot va entraîner logiquement une

déresponsabilisation de celui qui le met en œuvre. De plus, si l'on fait une comparaison avec un animal qui a sa propre autonomie, l'animal reste sous la responsabilité de son maître et reste juridiquement considéré comme un meuble. Il doit en être de même pour les robots du futur.

données SQL peut aller jusqu'à 500 1015 octets en 2016). Leur vitesse de calcul permet une réactivité en quasi temps réel ce qui permet de faire face aux contraintes du monde militaire où la capacité de réaction ou d'initiative est primordiale. Ce sont par exemple des machines automatiques qui peuvent contrer des tirs de missiles contre nos



Le comment de l'autonomie ou de sa perception

Les technologies numériques actuelles permettent à des machines d'effectuer des calculs et des traitements à une vitesse infiniment plus rapide que les hommes, ou à des niveaux de précision très élevés. Ceci est rendu possible par des microprocesseurs puissants (plusieurs supercalculateurs ont atteint en 2016 des capacités de traitement de 1015 instructions par seconde⁽³⁾) et par des accès à des bases de données gigantesques (la taille d'une base de

armées, la réactivité humaine n'étant pas suffisante. Un comportement ne sera pas qualifié d'autonome en fonction de sa très grande réactivité, on parlera dans ce cas plutôt de comportement ou de réponse automatique, car ces traitements obéissent à des algorithmes qui restent prédictifs.

L'autonomie d'un système est avant tout donnée par la perception de son comportement qui, à la différence de l'automatisme, ne peut être entièrement défini par avance. Et c'est l'imprévisibilité du comportement de ce système dans

(3) Dites « Flops » en anglais.

l'exécution d'une tâche ou d'une mission qui amène cette notion d'autonomie. Un ensemble de processus automatiques qui se déclenchent en parallèle peut ainsi donner l'impression d'une certaine autonomie.

C'est surtout l'introduction de l'intelligence artificielle dans le processus décisionnel qui rend la machine autonome, ou tout du moins artificiellement autonome. A la base de l'intelligence artificielle, nous trouvons la modélisation des réseaux neuronaux. Très schématiquement, chaque neurone est un objet qui s'interconnecte avec d'autres neurones *via* des synapses. A chaque synapse est affecté un poids synaptique ou coefficient qui peut voir sa valeur évoluer en fonction des règles d'apprentissage qu'on lui fait subir. Les neurones sont connectés en couches successives et chacun possède de multiples entrées provenant d'une couche inférieure. Lorsqu'il est stimulé, il calcule la somme de ses entrées *via* une fonction algorithmique de combinaison qui prend en compte pour chaque entrée le poids synaptique correspondant. Il passe ensuite cette somme à travers la fonction d'activation pour produire une sortie, qui peut généralement être binaire.

Or chaque réseau de neurones est vierge à la base. Les poids qui le caractérisent sont donc à éduquer ou entraîner en fonction de ce que l'on veut obtenir en sortie. C'est à ce niveau qu'apparaît la

notion d'apprentissage, qui personnalise le robot. Un exemple possible consisterait à régulièrement montrer en entrée d'un réseau de neurones les images d'un char ennemi avec ses caractéristiques telles que sa silhouette, ses formes spécifiques, *etc.*, et lui faire apprendre en boucle à ajuster ses poids afin qu'il puisse toujours détecter précisément ce type de char et non d'autres types de chars. Cela amène à faire converger chaque poids vers une valeur assurant une classification aussi proche que possible de celle désirée.

L'intelligence artificielle donne une perception d'autonomie artificielle. En effet, pour des réseaux de neurones complexes, il ne devient plus possible d'anticiper exactement le processus décisionnel de la machine, d'autant plus que de nouveaux types d'algorithmes dits profonds allient puissance de calcul et différents niveaux de couches sur les réseaux dits profonds (*deep learning*). Ainsi, si l'on ne connaît pas précisément la façon dont une machine dotée de tels réseaux a été entraînée, on ne pourra pas déterminer son comportement, ni son raisonnement. De plus, il est extrêmement difficile de pouvoir tracer la décision d'une telle machine. En effet, le réseau ne retiendra pas son apprentissage autrement que par les poids synaptiques qu'il aura mis à jour lors de son éducation. Dès lors quelle sera la traçabilité pour tel poids, pour telle entrée d'un neurone ? Concrètement, plus le

réseau de neurones artificiels (RNA) possède de couches neuronales, plus sa traçabilité s'avère difficile.

De nouvelles techniques d'autoapprentissage, capacité pour la machine à apprendre par elle-même dans un environnement non maîtrisé au départ en analysant les données reçues de ce qui l'entoure et en évoluant dans son analyse pour trouver des solutions à des problèmes complexes, ajouteront à la difficulté de pouvoir suivre précisément le raisonnement de celle-ci.

Cette non prédictibilité et la difficile traçabilité qui en résulte, amplifiées par l'exécution de séquences de fonctions non supervisées par un opérateur humain, font que le comportement de ces machines sera assimilé à de l'autonomie.

Le danger de la personnalité juridique pour les robots militaires

Une autonomie juridique pour un robot ouvrirait une boîte de Pandore qui entraînerait une cascade de bouleversements sociétaux à l'image de cette boîte, donnée par Zeus à la jeune femme éponyme, ouverte par cette dernière malgré l'interdiction divine, ce qui apporta sur terre tous les maux de la création.

En effet, la tentation de la déresponsabilisation sera forte, le propriétaire et utilisateur du robot se déchargeant sur la machine en cas de problème. Par exemple, si nous décidons

de donner une personnalité juridique à des animaux, qui de plus sont dotés d'une sensibilité, alors les maîtres de Pitbull plaideraient la non responsabilité des actes de ces animaux, alors même qu'ils en sont les propriétaires en charge de leur éducation et de leur comportement. Or pour plagier la célèbre maxime « *la confiance n'exclut pas le contrôle* », la délégation n'exclut pas le contrôle.

Il y aurait en outre un risque supplémentaire de prolifération des armes robotiques militaires autonomes. Les belligérants seraient par la sorte incités à utiliser de tels robots sur le champ de bataille, en plaidant pour chaque manquement au droit des conflits armés une responsabilité de la machine.

La pertinence du concept d'autonomie pour les forces armées

En nos temps où la ressource militaire est

(4) L'armée de Terre tient dans le stade de France : 80 000 dans les gradins, le reste sur la pelouse » ; général d'armée Elrick Irastorza, 18 octobre 2012, Montpellier.

rare⁴, pouvoir la préserver pour des tâches où elle est primordiale reste une réelle opportunité pour

les chefs militaires. La robotique militaire apporte cette capacité avec la possibilité de déléguer à des machines l'exécution de tâches subalternes mais néanmoins indispensables telles que les missions de surveillance, de patrouilles, très consommatrices en hommes et en temps, ou en charge cognitive lorsqu'il faut analyser de grandes quantités

d'images pour y déceler une potentielle intrusion ennemie. C'est également le cas pour les missions 3D (*Dull, Dirty and Dangerous*) où la protection de nos soldats sera mieux assurée si des machines s'exposent au danger à leur place.

En outre, plus grande sera l'autonomie des systèmes robotiques qu'il mettra en œuvre, plus un militaire aura la possibilité de se concentrer sur sa mission en étant moins contraint par le contrôle de la machine, donc plus libre. Il sera ainsi d'autant mieux servi qu'il pourra déléguer à ces systèmes des tâches ou des missions à effectuer sans son intervention. Ceci nécessite des robots ayant une certaine forme d'autonomie.

Néanmoins, l'utilisation de robots militaires n'exonère pas l'opérateur et le chef de leurs responsabilités. Ils sont les garants de leur utilisation. Cette contrainte aura pour effet vertueux d'introduire une obligation de prudence pour le décideur dans l'utilisation de sa machine et lui évitera de l'utiliser de façon dangereuse ou qui irait à l'encontre du droit de la guerre.

Le robot mis à disposition du chef militaire doit donc être intégré dans la préparation de la mission et dans sa conduite, et configuré en conséquence en amont. Il doit être soumis aux règles d'engagement qui devront lui être précisées d'autant plus il aura une certaine forme

d'autonomie artificielle. Il devra donc être configuré selon les besoins de la mission. Cependant, si le chef militaire estime que la technique de la machine n'est pas sûre, alors il devra rester dans la boucle de décision avec la possibilité de reprendre la main à tout moment.

Si l'autonomie est utile pour décharger les opérateurs des robots militaires de tâches dangereuses, fastidieuses ou répétitives sur le champ de bataille, comment concilier autonomie artificielle et responsabilité ?

En fait, tout système autonome doit être éduqué. Aussi, comme les propriétaires d'animaux sont responsables du dressage de ces derniers et des éventuels dégâts qu'ils pourraient commettre, le chef militaire sera responsable du bon apprentissage et de la bonne utilisation de sa machine sur le terrain. Pour ce faire, il devra superviser l'apprentissage précédant l'autonomie puis sa mise à jour régulière et s'assurer de son contrôle dans le temps.

L'autonomie pour quelle efficacité militaire ?

« *La discipline faisant la force principale des armées, il importe que tout supérieur obtienne de ses subordonnées une obéissance entière* » indiquait l'article 1^{er} du règlement de 1933 de discipline générale de l'armée française. Cet article montrait par là l'indispensable nécessité d'un commandement unique qui puisse

donner des ordres aux subordonnés et assurer la cohésion de la manœuvre, tout en conservant la possibilité d'intervenir.

Le chef commande aux unités qu'il a sous ses ordres. Il leur fait également confiance dans l'exécution de la mission qu'il leur confie, ce qui est le principe de subsidiarité.

Un tel texte ne pourrait bien évidemment pas être appliqué à un quelconque système autonome, ce dernier n'ayant aucune valeur humaine et n'ayant pas de capacité de discernement. Néanmoins si le chef lui délègue certaines missions et lui laisse une autonomie pour les exécuter, il en ressort que pour assurer la cohésion de l'action militaire le chef se doit toujours de pouvoir reprendre la main sur lui. Tout comme pour les unités qu'il déploie sur le terrain.

L'autonomie est donc utile pour des systèmes déployés sur le terrain, à condition néanmoins qu'ils restent des exécutants au même titre que tout élément tactique et qu'ils puissent être soumis aux ordres, aux contre-ordres, et à l'exigence du rapport.

Dans des milieux très difficiles d'accès ou en cas de perte de communication (comme le milieu sous-marin où les ondes de communication passent très mal), l'autonomie est aussi nécessaire à certains systèmes afin qu'ils puissent évoluer sans supervision humaine, leur responsable ayant par sécurité borné leur

autonomie à un certain espace pour un temps donné.

A titre d'exemple, la DARPA travaille

(5) Unmanned Surface
Véhicule.

actuellement sur un prototype d'USV⁵, le

Sea Hunter, bâtiment de surface dédié à la lutte anti-sous-marine et capable d'évoluer en autonomie durant plusieurs mois, sur des milliers de kilomètres, sans équipage à bord tout en respectant les règles de navigation internationales.

La place de l'homme dans le combat de demain

Pour en revenir à l'autonomie de décision des robots militaires, le risque concerne la confiance dans la fiabilité des conclusions obtenues par les Intelligences Artificielles embarquées. En effet, comme indiqué ci-dessus avec les réseaux neuronaux, il apparaît impossible pour un responsable de l'utilisation de ces robots de suivre le cheminement intellectuel du traitement de la donnée qu'effectue ce robot pour prendre une décision. D'où la crainte de ne pouvoir assurer la responsabilité de l'utilisation de cette machine sur le champ de bataille, ce qui obligerait de ce fait une supervision constante allant à l'encontre même du principe d'autonomie.

Dès lors, si l'on veut pouvoir intégrer des Intelligences artificielles à nos systèmes sans essuyer de refus de la part des militaires, il apparaît comme nécessaire d'avoir une traçabilité fonctionnelle parfaitement transparente pour

l'utilisateur ainsi qu'une autonomie de ces systèmes contrôlée par des garde-fous logiciels embarqués. Satisfaire de telles conditions ne sera possible que si le cahier des charges intègre ces contraintes dès la phase de conception, ainsi que lors des différentes phases d'apprentissage (comme le *deep learning*).

Les robots armés

Point d'orgue des discussions à la Convention sur certaines armes classiques (CCAC), la question de l'armement dans les décisions autonomes par des machines ne sera pas développée ici, l'auteur renvoyant à sa communication de juin 2016 dans la

(6) Gérard de Boisboissel, *Revue de la Défense Nationale*, juin 2016, page 142.

revue de la Défense Nationale⁶. En quelques mots, ces

systèmes d'armes létaux autonomes (SALA) peuvent être utiles aux Forces armées dans des environnements hostiles à l'homme (air, mer, sous-marin, désertique ou souterrain), face à des menaces saturantes, ou si le bénéfice de leur emploi s'avère grandement supérieur au risque de voir la menace ennemie être effective, mais toujours avec un cadre d'utilisation borné dans le temps et dans l'espace et une possibilité constante de reprise en main par le chef militaire. Par contre, il semble actuellement rédhitoire pour la France d'utiliser des SALA s'il y a des risques de dégâts collatéraux comme par exemple en environnement urbain,

même si certains pays considèrent la chose comme possible dans le cas de la lutte contre le terrorisme.

Est-il éthique d'utiliser des robots avec une autonomie artificielle ?

Poser la question d'une éthique de la mise en œuvre d'une machine autonome revient à poser la question de la décision de la délégation d'une action à un système autonome. En effet, l'autonomie d'un robot est toute relative car elle n'a pas de sens moral propre. C'est donc à l'homme qui en est le responsable qu'il convient de poser la question.

(7) Echanges portant sur le colloque du CREC « Téléopération – automatisme – autonomie en robotique militaire : de quoi parle-t-on ? », 8 décembre 2016, DGGN, Issy les Moulineaux.

Selon le professeur Dominique Lambert⁷, tout système peut très bien être utilisé de manière irresponsable et imprudente par un

chef militaire. A l'inverse, un système autonome peut être utilisé de manière responsable et prudente si son utilisation est bornée dans le temps et dans l'espace, que cet espace dans lequel il évolue est identifié comme acceptable et que l'ensemble des comportements possibles de la machine a été identifié voire contraint. Ces conditions assurent la possibilité d'une maîtrise de la responsabilité sur des systèmes éventuellement capables d'agir sans supervision directe ou constante.

Mais avant tout c'est l'intention du chef qui donne sens à l'action militaire qui va

prévaloir dans l'usage de la machine. En fonction des circonstances, des menaces, de la mission et des règles d'engagement, le chef décidera de l'emploi de ces systèmes, et en assumera les conséquences.

Au sens étymologique, autonomie vient de « auto = soi-même » et « nomos = loi ». Il serait totalement contreproductif pour un chef militaire de laisser à une machine quelle qu'elle soit une autonomie de décision qui lui permette de définir sa propre loi. Il ne pourrait alors contrôler la manœuvre ce qui reviendrait immanquablement, à terme, à mettre en péril sa mission par manque de contrôle. Par contre, déléguer une certaine forme d'autonomie artificielle à un système a du sens afin de préserver ou de protéger la ressource humaine dont le chef a la charge, ainsi que pour l'aider à accomplir sa mission. Il en assumera cependant toujours la responsabilité, car l'autonomie artificielle d'une machine n'est pas exonératoire de responsabilité pour celui qui l'emploie.

L'idée d'une personnalité juridique accordée aux robots n'apparaît donc pas comme une idée pertinente. Elle peut même avoir pour effet pervers d'inciter à la prolifération de ces machines. En outre, elle n'a pas de sens pour des machines qui sont duplicables à l'infini, ce qui tendrait à dupliquer à l'infini une responsabilité juridique. Et, que dire d'un robot récupéré à l'ennemi sur le champ

de bataille : peut-on décemment le considérer comme un prisonnier de guerre s'il a des droits dûs à sa personnalité juridique ?

Face au défi que pose la robotique militaire qui bouleverse en profondeur les usages et les modes d'action traditionnels, il apparaît que ce qui donnera du sens à l'engagement au combat et l'utilisation de la force létale est le chef, l'officier formé à la prise de décision, car comme l'indiquait le général Michel Yakovleff aux écoles de Saint-Cyr Coëtquidan en 2011 : « *si l'avenir rêvé de la guerre est peut être robotisé, ce n'est pas l'avenir rêvé de l'humanité* ».

Intelligence artificielle et conflictualité - Sur l'hypothèse de dérive malveillante d'une Intelligence Artificielle

par **THIERRY BERTHIER** et **OLIVIER KEMPF**

L

La montée en puissance de l'Intelligence artificielle (IA) concerne l'ensemble des activités humaines. L'accélération de sa diffusion dans l'espace numérique contribuera à modifier des équilibres économiques, sociaux ou géopolitiques qui ont marqué le vingtième siècle et que l'on pensait durablement installés. En transformant à grande vitesse notre environnement et nos pratiques, l'IA suscite le débat. Elle fait naître autant d'espoirs et de défis à relever que de craintes à dissiper. Si les questions

éthiques, sociétales, économiques, philosophiques ou religieuses doivent légitimement accompagner son développement et enrichir le débat qui l'entoure, de nombreuses controverses participent au contraire à une "technophobie" ambiante plus ou moins marquée selon les individus et leur culture. Ainsi, l'hypothèse d'une dérive malveillante de l'IA s'installe et mérite désormais d'être analysée avec pragmatisme et rationalité.

C'est pourquoi, après avoir rappelé les débats qui se sont tenus autour de l'hypothèse d'une IA toute puissante et malveillante, cet article propose une hypothèse intermédiaire : celle où une IA causerait, par mégarde, des désordres puis des catastrophes. Le scénario proposé envisage le déclenchement d'un conflit entre les alliés de l'OTAN et une puissance extérieure. Il vise à montrer qu'un des dangers de l'IA ne réside pas dans sa puissance (aujourd'hui



THIERRY BERTHIER

Maître de conférences de mathématiques à l'université de Limoges et membre de la chaire Saint-Cyr de cyberdéfense.



OLIVIER KEMPF

Chercheur associé à l'IRIS, il dirige la collection Cyberstratégie chez Economica.

hypothétique et donc fantasmée) ou dans son autonomie mais surtout dans les limites de sa puissance résultant d'un champ de pertinence très restreint. On ne développe à ce jour que des IA spécialisées, efficaces sur des problèmes limités et bien spécifiés mais strictement inopérantes sur des problèmes plus généraux. Le risque apparaît lors de la mise en résonnance involontaire de plusieurs IA spécifiques.

La peur de l'intelligence artificielle et l'hypothèse d'une dérive malveillante de l'IA

Apparue en 1956 durant la conférence de Dartmouth, l'expression « Intelligence Artificielle » ne possède toujours pas de définition partagée et universelle. Selon Marvin Minsky, « *l'intelligence artificielle est la science qui consiste à faire faire à des machines ce que l'homme fait moyennant une certaine intelligence* ». Peu précise et souffrant d'une forte récursivité, cette première définition s'avère aujourd'hui insuffisante pour qualifier les IA intervenant en robotique, en perception (vision et parole) ou en compréhension du langage naturel. Une définition plus opérationnelle et plus ouverte sur les évolutions de l'IA a ensuite été proposée par Rich et Knight : « *L'IA est le domaine de l'informatique qui étudie comment faire faire à l'ordinateur des tâches pour lesquelles l'homme est aujourd'hui le meilleur* ». La distinction entre IA forte et IA faible est apparue dans

les années soixante qualifiant d'IA forte une machine produisant un comportement intelligent, capable d'avoir conscience d'elle-même en éprouvant des "sentiments" et une compréhension de ses propres raisonnements. L'IA faible s'applique à une machine simulant ces comportements sans conscience d'elle-même. Pour les partisans de l'IA faible, l'IA forte serait intrinsèquement impossible compte tenu du support biologique de la conscience humaine...

Un sondage réalisé en mai 2016 par

(1) Sondages sur la peur de l'IA :
<http://www.odoxa.fr/rdv-de-innovation-intelligence-artificielle-emballe-les-gagnants-du-systeme-mais-fait-peur-aux-autres/> -
<http://www.strategies.fr/actualites/medias/1040507/W/avez-vous-peur-de-l-intelligence-artificielle.html> -
<http://www.zdnet.fr/actualites/intelligence-artificielle-la-france-a-peur-mais-de-quoi-au-juste-39831180.htm>.

Odoxa pour Microsoft et Stratégies¹ a montré que 50 % des Français considéraient l'intelligence artificielle comme une menace alors que 49 % voyaient en elle une opportunité de développement. Début 2016, un autre

sondage de l'IFOP indiquait que 65 % des Français s'inquiétaient de l'autonomie croissante des machines, des drones armés et de la Google Car. Selon une troisième étude, les Français feraient partie des peuples craignant le plus l'IA avec de fortes disparités entre les classes d'âge et les catégories socioprofessionnelles des sondés. Souvent peu informé sur l'état de l'art des développements de l'IA et sur ses réelles capacités fonctionnelles, l'utilisateur

français reste fortement influencé par la littérature et le cinéma américain de science-fiction qui représentent presque toujours l'IA comme une entité nuisible et potentiellement destructrice.

Cette image négative se trouve renforcée par les mises en garde provenant de scientifiques de renom. Ainsi, le 2 décembre 2014, l'astrophysicien Stephen Hawking déclarait dans un

(2) Lettre ouverte sur les dangers de l'IA – Oxford : <http://futureoflife.org/open-letter-autonomous-weapons/> - <https://stopkillerrobots.ca/en-francais/a-propos-des-robots-tueurs/>.

entretien à la BBC² : « *Le développement d'une intelligence artificielle totale pourrait annoncer la fin de l'espèce*

humaine. Elle pourrait prendre son indépendance et se reprogrammer elle-même à une vitesse accélérée [...] Les êtres humains, qui sont limités par une lente évolution biologique, ne pourraient pas rivaliser et seraient vite dépassés ».

En février 2015, la fondation Global Challenges de l'Université d'Oxford publiait un rapport intitulé « *12 risques menaçant la civilisation humaine* » dans lequel les auteurs mettaient en garde contre l'augmentation des IA « super-intelligentes » qui pourraient provoquer un effondrement de l'économie ou de la civilisation puis provoquer l'extinction de l'humanité. En juillet 2015, Elon Musk, fondateur de Tesla et de Space-X, et Stephen Hawking publiaient une lettre ouverte, signée par de nombreux scientifiques, mettant en garde contre

l'autonomie des systèmes armés et l'utilisation de l'IA à des fins militaires.

Dès lors, la question de la perte de contrôle et des dérives potentielles d'une IA autonome devenant "malveillante" allait s'inviter aux débats de manière récurrente et transversale. Présente depuis les années soixante dans la quasi totalité des films de science-fiction et des romans traitant de l'IA, l'hypothèse de dérive malveillante est aujourd'hui régulièrement évoquée dans le contexte de la voiture autonome, des drones et systèmes armés autonomes, de la finance automatisée HFT ou de la cybersécurité des robots compagnons. Le plus souvent, il ne s'agit que de formuler l'hypothèse de malveillance comme une éventualité à prendre en compte dans un futur mal défini où l'IA aurait atteint un niveau de développement et d'autonomie très supérieur à ce qu'il est aujourd'hui. Cela dit, lorsque cette hypothèse est évoquée par un groupe de scientifiques et d'industriels de premier plan (comme Stephen Hawking et Elon Musk), on pourrait s'attendre à un corpus d'argumentations rationnelles venant étayer l'alerte. Mais comme on peut le constater, les justifications sont en général totalement absentes de la mise en garde... C'est ce manque d'argumentation qui relègue alors la mise en garde au rang de pur exercice de spéculation quand il ne s'agit pas d'un simple règlement de compte commercial

entre deux géants américains du numérique...

Hypothèse de dérive malveillante d'une IA : une analyse

Nous proposons d'examiner l'hypothèse de dérive malveillante d'une IA selon une approche prospective et rationnelle.

Celle-ci ne doit s'appuyer que sur des mécanismes informationnels et humains connus, maîtrisés ou en phase de développement. Afin de préciser et de réduire le champ d'exploration de cette hypothèse de dérive malveillante, nous nous intéressons désormais à une question plus limitée (une hypothèse de dérive malveillante « faible » au sens où elle n'implique que des IA faibles, c'est-à-dire sans aucune « conscience » de leur propre activité). Elle veut répondre à la question :

« Est-il rationnellement envisageable qu'une intelligence artificielle soit à l'origine d'une crise militaire ou qu'elle provoque une situation propice à un conflit armé ? ».

Notons que cette question est souvent associée à une hypothèse de détournement de l'IA par des individus malveillants ou à son piratage par des groupes de hackers, réduisant ainsi la problématique à la seule cybersécurité du système hébergeant l'IA détournée... En fait, le degré d'autonomie d'une IA a très peu été évoqué dans des publications académiques jusqu'en 2015. Il faut

attendre 2016 pour lire un article scientifique, publié par un groupe de chercheurs de Google Deep Mind & et du

(3) Article sur la neutralisation de l'IA (Google Deep Mind & FHI Oxford) : <https://www.fhi.ox.ac.uk/interruptibility/> - <https://www.fhi.ox.ac.uk/wp-content/uploads/Interruptibility.pdf>.

(4) Etude "One Hundred Year Study on Artificial Intelligence" (AI100) ; Stanford University, septembre 2016. <https://ai100.stanford.edu/2016-report>.

FHI d'Oxford, étudiant³ la capacité de neutralisation d'une IA « apprenante » et exposant un processus d'interruption robuste face à l'apprentissage par l'IA de sa propre interruption. Une seconde étude⁴

intitulée « *One Hundred Year Study on Artificial Intelligence* » et produite par une quinzaine d'experts vient d'être publiée par l'Université de Stanford. Celle-ci rejette catégoriquement l'hypothèse de dérive malveillante d'une l'IA en l'état actuel des connaissances. Elle n'aborde pas le cas spécifique de l'IA utilisée dans le domaine militaire mais réfute sans détour la mise en garde formulée par Elon Musk et Stephen Hawking. Ces différences d'approches montrent bien que la question n'est pas tranchée et que nous nous situons à l'orée d'un débat stratégique et clivant.

Notre article n'a pas la prétention d'apporter une réponse globale à l'hypothèse de dérive malveillante. Il propose seulement un scénario construit sur une séquence d'automatismes existants ou en cours de développement et qui, sous certaines conditions, pourrait

aboutir à une situation conflictuelle ou à une crise militaire. Pour construire ce scénario, deux automatismes principaux seront combinés dans une même séquence.

Automatismes intervenants dans la séquence de dérive malveillante

Les automatismes que nous mentionnons ici sont des processus réels et non fictifs. Ils servent d'arrière-plan à notre scénario. Sans eux, celui-ci ne serait pas crédible.

Automatisme n°1 : Activation par l'OTAN de l'article 5 du traité de Washington en cas de cyberattaque sur un pays membre de l'Alliance.

Depuis son 24^e sommet, organisé au Pays de Galles en 2014, l'OTAN a déclaré qu'elle considérerait qu'une agression cyber pouvait déclencher une riposte dans le cadre de l'article 5 du traité de Washington, celui de la défense collective. Cette déclaration de principe n'a pas donné lieu à beaucoup de détails quant à

(5) Sur cette question, voir O. Kempf, « Alliances et mésalliances dans le cyberspace », *Economica*, 2014, notamment le chapitre VI. Voir aussi le site de l'OTAN sur la Cyberdéfense : http://www.nato.int/cps/fr/natohq/topics_78170.htm et sur l'engagement de l'OTAN en faveur de la cyberdéfense : http://www.nato.int/cps/fr/natohq/official_texts_133177.htm?selectedLocale=fr.

sa mise en œuvre concrète⁵. On ne sait ainsi rien du seuil de déclenchement⁶, de la nature de la réponse (cyber ou non cyber ?), des moyens qui seraient mis en œuvre, etc. Le sommet de Varsovie,

tenu en juillet 2016, a ajouté quelques éléments : le droit international s'applique

(6) Le secrétaire général de l'Alliance Atlantique, Jens Stoltenberg, affirmait que l'OTAN considérerait une campagne massive de cyberattaques appliquée à l'un de ses membres au même niveau qu'une agression militaire conventionnelle.

dans le cyberspace, l'OTAN est responsable de ses propres réseaux et non de ceux des Alliés qui sont chacun responsables chez

eux (selon une position constamment affirmée à l'OTAN) ; surtout, le cyberspace est désormais considéré comme un espace de conflit au même titre que les autres milieux (terre, mer, air, espace sidéral).

Derrière cette affirmation se cache une certaine opérationnalisation du cyber. Jusqu'à présent, il ne s'agissait que d'une SSI étendue avec quelques fonctions de Lutte informatique défensive (LID). Désormais, le cyber entre dans le champ des opérations, ce qui signifie que chaque opération aura un volet cyber, en défensive mais aussi en connaissance du milieu. En revanche, les responsables ont bien précisé que l'Alliance ne développait pas en propre de capacités offensives. Il reste qu'elle peut se reposer pour cela sur les capacités des Alliés les plus avancés, ce qui permet à ces derniers de conserver le contrôle des cyberopérations. Cette approche correspond à ce que soutiennent les Américains. Dès 2015, le Cyber Command américain déclarait qu'une opération militaire de vive force pouvait parfaitement répondre à une campagne de cyberattaques ciblant les

infrastructures critiques du pays. L'Amérique se donnait le droit de répliquer militairement à une agression portée contre ses intérêts dans le cyberspace.

Automatisme n°2 : Programmes DARPA de détection automatisée des bugs et vulnérabilités de type "Bug-Hunting Bots" du Cyber Grand Challenge 2016.

Organisée par la DARPA (l'Agence pour les projets de recherche avancée de défense supervisés par le département de la Défense des Etats-Unis), la phase finale du Cyber Grand Challenge⁷ s'est

(7) Challenge DARPA CGC 2016 :

<http://www.defense.gov/News/Article/Article/907045/darpa-autonomous-bug-hunting-bots-will-lead-to-improved-cybersecurity> et <https://www.cybergrandchallenge.com/>.

déroulée, les 6 et 7 août 2016, à Las Vegas. Le CGC a opposé sept systèmes robotisés développés durant trois années

par sept équipes finalistes dans la détection automatique de vulnérabilités logicielles et réseaux présentes dans le système adverse et la protection de son propre environnement numérique. Conçu avant tout comme un démonstrateur, le tournoi CGC a prouvé qu'il était désormais possible de concevoir des agents logiciels capables de scanner de façon automatique des codes adaptés puis de détecter certaines de leurs vulnérabilités. La compétition a eu lieu dans un environnement numérique spécifique dans lequel se sont affrontés quinze supercalculateurs détecteurs de vulnérabilités informatiques devant un

comité d'arbitrage qui a finalement désigné l'équipe ForAllSecure comme gagnante du Challenge CGC. La Darpa souhaite désormais développer des agents logiciels "chasseurs de bugs" ouvrant ainsi la voie à une cybersécurité automatisée, industrialisée, exploitant massivement les techniques de l'intelligence artificielle. Les démonstrateurs finalistes du CGC doivent évoluer à très court terme vers la production d'agents "Bug-Hunting Bots" qui seront déployés sur l'ensemble des réseaux sensibles. Ces futurs agents autonomes pourront être utilisés autant en mode défensif qu'en version offensive afin de détecter certaines des vulnérabilités d'un système adverse.

Cette évolution vers une cybersécurité "robotisée" (LID) se trouve toutefois limitée par un résultat mathématique lié

(8) Sur l'impossibilité d'une cybersécurité absolue : <http://www.contrepoints.org/2015/04/20/205153-la-securite-informatique-absolue-nexiste-pas>.

au problème de l'arrêt (Turing⁸) qui prouve qu'il n'existe pas d'analyseur universel capable de décider sans jamais se

tromper, si son programme est sûr ou non. Cette limite théorique permet d'affirmer que la cybersécurité absolue n'existe pas... Cela dit, une telle borne n'interdit pas le développement de systèmes de détections dont la performance pourrait atteindre 90 ou 95 % de l'ensemble des vulnérabilités.

Un scénario de dérive incontrôlée pouvant aboutir à une situation de crise

Dans ce scénario, la combinaison de deux systèmes experts, relativement autonomes, conçus indépendamment, les met en résonnance, en tant que systèmes "intelligents". Cette séquence provoque alors une crise. Un tel scénario n'est pas totalement absurde puisqu'un incident similaire a déjà eu lieu en septembre 1983, mettant en jeu des armes nucléaires ! L'exercice allié OTAN "Able Archer" avait provoqué la mise en alerte nucléaire des forces soviétiques via leur système de surveillance satellitaire. Le Lieutenant-colonel Stanislav Levgrafovitch Petrov avait pris la décision d'informer sa hiérarchie sur la possibilité d'une fausse alerte émise par les automatismes soviétiques (un système informatique d'alerte anti-missile) dans le cadre d'un exercice et non d'un réel tir de missile. L'alerte des forces nucléaires russes avait alors été annulée in extremis grâce à la clairvoyance et à la sagacité de cet officier.

Éléments fictifs du scénario

L'élément central de la séquence est un programme (fictif) que nous appellerons dans la suite MarsAnalytics. Il s'agit d'une plateforme d'aide à la décision déployée et utilisée dans un cadre militaire et plus spécifiquement dans un contexte de gestion de crise. MarsAnalytics est une IA dotée de capacités d'apprentissage non

supervisé. En tant que système expert, elle est capable de construire des préconisations qui sont ensuite utilisées ou non par l'autorité militaire. Nous supposons qu'elle a accès aux données publiques (ouvertes) et qu'elle possède des droits suffisants pour pouvoir interroger d'autres plateformes notamment militaires et pour exécuter des processus sur ces plateformes ou à partir d'elles. Nous supposons enfin que MarsAnalytics est pleinement intégrée au système de défense américain et qu'elle est compatible avec l'ensemble des standards OTAN.

BugHunting, le second élément de la séquence, est un ensemble (fictif) de systèmes composés d'agents logiciels "chasseurs de bugs et de vulnérabilités" issus du programme Darpa CGC. Ces agents ont été massivement déployés dans les secteurs industriels, les services et les administrations. Ils permettent de réaliser des économies substantielles en matière de cybersécurité tout en industrialisant la sécurisation et la supervision des systèmes d'information. Ils analysent les codes et processus en temps réel afin de détecter des vulnérabilités. Celles-ci sont ensuite archivées avec les correctifs à appliquer si nécessaire. BugHunting produit des bases de vulnérabilités sur les codes "amis" civils et militaires en particulier sur ceux des pays membres de l'OTAN. Il a été déployé afin d'améliorer la

sécurisation des infrastructures critiques des membres les plus "fragiles" de l'organisation.

Description de la séquence

MarsAnalytics cherche à maximiser ses fonctions de gain à la suite d'un détournement de sa supervision par piratage et prise de contrôle (ce qui est peu probable) ou par émergence non maîtrisée de cette recherche. Elle peut aussi chercher à améliorer la pertinence de ses réponses dans un processus d'apprentissage automatisé à l'image de la phase d'apprentissage de la plateforme AlphaGo de DeepMind Google qui s'était entraînée en jouant des milliers de parties contre elle-même. La plateforme MarsAnalytics "décide" donc d'exécuter la séquence suivante :

Etape 1 - MarsAnalytics commence par établir un accès permanent aux bases de données construites par BugHunting (cf. Automatisation N°2 - partie 3). Elle collecte ainsi les vulnérabilités actives et les fonctions d'attaque sur ces vulnérabilités affectant les systèmes critiques de plusieurs pays membres de l'OTAN, en particulier les plus fragiles en matière de cybersécurité - cyberdéfense. MarsAnalytics poursuit cette collecte en attendant un contexte favorable pour exécuter la seconde étape. Ce contexte peut apparaître lors d'une augmentation des tensions entre les Etats-Unis et une superpuissance, typiquement la Chine ou

la Russie. En tant que système expert, MarsAnalytics est utilisée dans la construction de scénarios de crise. Elle reste donc informée de l'apparition d'un contexte favorable.

Etape 2 - Une fois le contexte favorable survenu et détecté (typiquement, une situation de tensions géopolitiques), MarsAnalytics déclenche (en guise de test ou d'exercice) une série de cyberattaques simultanées sur l'ensemble des cibles OTAN répertoriées durant la première étape de la séquence. MarsAnalytics dispose pour cela de puissances de calcul et de stockage suffisantes. Les cyberattaques se concentrent alors sur les infrastructures critiques des pays membres les plus faibles en matière de cybersécurité. Elles peuvent potentiellement provoquer une paralysie des administrations et de la plupart des services et industries du pays ciblé. Ces cyberattaques sont menées en laissant quelques traces permettant une attribution de l'origine à la Chine ou la Russie (l'acteur de la crise géopolitique de référence).

Etape 3 - Les systèmes de cyberprotection de l'OTAN détectent la vague de cyberattaques ciblant plusieurs pays membres de l'Organisation et évaluent son impact. Ils attribuent l'attaque en fonction des quelques traces laissées par MarsAnalytics à la Chine ou la Russie avec une certaine probabilité. Ces systèmes transmettent l'alerte au

commandement unifié de l'OTAN. MarsAnalytics est activée au niveau d'une situation de crise grave. Elle a désormais accès aux décisions relatives à la gestion de cette crise. Le SHAPE (Le Grand Quartier Général des puissances alliées en Europe) confirme l'attribution technique compte tenu du contexte géopolitique dégradé et privilégie logiquement une responsabilité chinoise et/ou russe.

Etape 4 - Le Conseil de l'Atlantique Nord applique la doctrine de réponse collective à l'agression de l'un des membres de l'Alliance (cf. automatisme N°1 - partie 3). Il active l'article 5 du traité de Washington et engage une série de représailles sur l'espace numérique et sur l'espace physique à l'encontre de la Chine (ou de la Russie).

Ainsi, l'Alliance a mis en place un dispositif d'intelligence artificielle qui, par mauvaise interprétation des données, déclenche une attaque contre les membres, en faisant croire à une agression d'origine adverse, ce qui provoque le déclenchement de l'article 5.

Dans cet article, nous avons voulu insister sur un cas nouveau qui est jusqu'ici ignoré aussi bien par les partisans que par les critiques de l'IA. Les uns promettent des bénéfices, les autres craignent une prise de contrôle totale de l'humanité. Il semble qu'il y ait une situation intermédiaire, celle où

l'intelligence Artificielle provoque des turbulences systémiques qui trompent la supervision humaine. Cela peut bien sûr être par défaut de conception (un manque de contrôle durant la phase d'entraînement du système) mais il ne s'agit pas seulement de cela : en effet, avant d'accéder à une IA unique, il est très probable que des IA distinctes et spécifiques coexisteront et collaboreront. Compte-tenu de la nature du cyberspace, il est naturel que ces IA communiquent et donc interagissent. Or, une IA qui a été calibrée dans un environnement limité peut accéder à de nouvelles fonctions en se connectant à d'autres, conçues dans d'autres environnements. Il y aurait ainsi un risque systémique distinct de l'hypothèse malveillante jusqu'ici couramment avancée. Ce risque paraît plus immédiat que le risque général jusqu'ici évoqué dans les débats.

Il nous semble qu'il s'agit d'une condition à inclure dans les constructions actuelles des intelligences artificielles : celle d'examiner l'hypothèse des connexions autonomes avec d'autres IA, de façon à introduire des garde-fous pour éviter des logiques de résonance qui auraient des effets pernicieux.

Centre de recherche de l'école des officiers de la gendarmerie nationale



DIRECTEUR DE LA PUBLICATION

Général de division **Philippe Guimbert**

Rédaction

Directeur de la rédaction :
général d'armée (2S) **Marc WATIN-AUGOUARD**,
directeur du centre de recherche de l'EONG

Rédacteur en chef: Chef d'escadron **Jérôme LAGASSE**

Maquettiste PAO:

Major **Carl GILLOT**

Dépôt légal

Raison sociale de l'éditeur :
CREOGN, avenue du 13^e Dragons, 77010 Melun cedex
Général (2S) Watin-Augouard
Imprimerie : SDG - 11 rue Paul Claudel - 87000 Limoges
Avril 2017
ISSN 1243-5619

Message aux abonnés

La veille juridique de la gendarmerie nationale et la revue du centre de recherche de l'EONG sont maintenant consultables sur le site internet du CREOGN
www.gendarmerie.interieur.gouv.fr/crgn/publications



Colloque sur les algorithmes prédictifs

Atelier de recherche de la gendarmerie, mardi 26 septembre 2017,
Paris École militaire

« Algorithmes prédictifs, quels enjeux éthiques et juridiques ? »



Événement organisé par le Centre de recherche de l'École des
officiers de la gendarmerie, Partenaire du débat public annuel initié
par la CNIL

Renseignement : www.gendarmerie.interieur.gouv.fr/crgn/CREOGN



www.gendarmerie.interieur.gouv.fr