

**Véhicule Autonome et connecté :
aspect juridique**



Étudiants

COTIER Charlotte
DESSOULIERS Elise
LEGER Victor

NTICHA Baraa
PROUVOST Mathilde
SAINT-ETIENNE Maëlys

Enseignant-responsable du projet :

Abdelaziz BENSRAIR

Date de remise du rapport : 08/06/2021

Référence du projet : STPI/P6/2021 – 04

Intitulé du projet : Véhicule autonome et connecté : aspect juridique.

Type de projet : Veille technologique, documentation et bibliographie.

Objectifs du projet :

L'objectif de ce projet est tout d'abord d'en apprendre plus sur le véhicule autonome, sujet très actuel aujourd'hui en France, et notamment sur le Campus du Madrillet. : il n'est pas rare de voir une Renault Zoé autonome de Rouen Normandy Autonomous Lab en se rendant à l'INSA ! Mais c'est également de se renseigner et de découvrir les aspects juridiques de cette dernière, qui suscitent encore beaucoup d'interrogations aujourd'hui.

Mots-clefs du projet : Véhicule autonome, éthique, risques, sécurité.

Tables des matières

1. Introduction.....	6
2. Méthodologie/Organisation du travail.....	7
2.1 Description de l'organisation adoptée pour le déroulement du travail.....	7
2.2. Organigramme des tâches réalisées et des étudiants concernés.....	8
3. Quid de la voiture autonome	8
3.1 Présentation de la voiture autonome.....	8
3.2 Les risques possibles.....	9
3.2.1 Des risques en raison de la connectivité.....	10
3.2.2 Des risques en raison de la modification de la répartition des tâches et de l'interaction entre l'homme et la machine.....	11
4. Dilemmes éthiques.....	12
4.1 Les études (comme « la machine morale ») faites à travers le monde.....	12
5. Lois déjà en vigueur du véhicule autonome.....	14
5.1 Les droits de l'utilisateur d'un véhicule connecté.....	14
5.2 Les DCP (données à caractère personnel).....	15
5.3 Les responsabilités juridiques.....	17
5.4 Assurance.....	18
6. Sécurité du véhicule.....	19
6.1 La question du traitement des données personnelles et de la vie privée.....	19
6.2 La question de la cybersécurité.....	20
7. Conclusions et perspectives.....	22
8. Rapport d'étonnement.....	23
9. Bibliographie et crédits d'illustrations.....	24

Lexique, Notation, Acronymes

Sonar : appareil de détection sous-marine, utilisant les ondes sonores et permettant le repérage, la localisation et l'identification des objets immergés.

<https://www.larousse.fr/dictionnaires/francais/sonar/73442>

Lidar : radar de sondage atmosphérique qui fonctionne avec des ondes optiques émises par laser. <https://www.larousse.fr/dictionnaires/francais/lidar/47055>

Servocommande : mécanisme interposé entre une commande manuelle et l'organe commandé, dans le but de produire la force nécessaire à la manœuvre par emprunt d'énergie à une source extérieure. <https://www.larousse.fr/dictionnaires/francais/servocommande/72407>

ECU : appelé « Engine Control Unit » en anglais et « Unité de contrôle du moteur » en français, c'est tout simplement l'ordinateur embarqué dans toutes les voitures récentes qui permet de gérer toutes les opérations liées au moteur. <https://www.capcar.fr/lexique-auto/ecu>

Corpus : recueil de documents, de textes, en vue d'une analyse.
<https://www.linternaute.fr/dictionnaire/fr/definition/corpus/>

1. Introduction

Au quatrième semestre de notre deuxième année de cycle préparatoire à l'INSA de Rouen Normandie, un projet de P6 nous a été proposé. Ce projet permet d'étendre nos connaissances et notre culture scientifique, mais aussi de travailler notre capacité d'adaptation et de travail d'équipe sur un long terme.

Le sujet sur lequel nous avons décidé de travailler est celui de la voiture autonome, l'idée de cette conception est de transporter des personnes, ou des marchandises d'un point A à un point B de manière totalement automatisée sans qu'un être humain ne prenne les commandes du véhicule. Ainsi, le véhicule prend des décisions sans assistance de l'humain, il pourra contribuer à favoriser l'autonomie et la mobilité des personnes en situation de handicap. La voiture autonome possède de nombreuses technologies pertinentes à étudier, mais nous nous pencherons plus particulièrement sur l'aspect juridique qui est au cœur des débats actuels. En effet, lorsque l'on conçoit un objet scientifique, il est nécessaire de s'interroger sur les problèmes éthiques que cette innovation peut engendrer pour ensuite réglementer l'utilisation de l'invention. Concernant la voiture autonome, son marché est en pleine expansion depuis les dix dernières années. De nouvelles lois et règles autour de ce véhicule sont primordiales afin d'établir un cadre juridique qui n'existait pas avant.

Nous étudierons dans un premier temps le concept de la voiture autonome et les différents risques qui en résultent. Ensuite, nous nous focaliserons sur le dilemme éthique émergeant de cette innovation. Nous analyserons et commenterons les lois déjà en vigueur de la voiture autonome, pour finalement finir par la sécurité du véhicule en abordant les questions du traitement des données personnelles et de la vie privée et de la cybersécurité.

2. Méthodologie / Organisation du travail

2.1 Description de l'organisation adoptée pour le déroulement du travail.

Dans le cadre de notre projet de physique, le thème sur lequel nous avons travaillé est le suivant : « Véhicule Autonome et connecté : aspect juridique ». Notre groupe de projet P6 est composé de 6 membres qui pour la majorité ne se connaissaient pas avant la mise en place du projet. Malgré cela, notre groupe a pu s'organiser de manière très fluide et agréable dans l'optique d'achever un projet sur le long terme et demandant un temps de recherches important. Il est vrai que pour la plupart d'entre nous, ce projet relevait de l'inédit. En effet, ce projet n'est pas fondamentalement scientifique : il n'y a pas d'aspect calculatoire, ni d'expérience et c'est ce qui nous a attirés. On ne peut concevoir en tant qu'ingénieur une invention sans aborder l'aspect juridique et éthique de celui-ci. Nous avons été encadrés par Monsieur BENSRAHIM Abdelaziz qui nous a accompagnés dans l'avancement du projet. Nous nous sommes réunis tous les lundis matin à 9 h 45. Lors de la première séance, nous avons élu un chef de groupe qui avait pour rôle de faire le lien avec notre encadrant. C'est Elise qui a été désignée.

Du fait des conditions sanitaires particulières, nous avons travaillé à distance en nous réunissant dans un premier temps sur Zoom puis sur Discord afin d'échanger avec Monsieur BENSRAHIM sur les séances prévues pour cela. De plus, nous avons de notre côté créé un groupe Messenger afin de pouvoir échanger sur l'avancée du projet entre les séances.

Au début de notre projet, nous avons eu du mal à nous organiser car il était difficile de se concentrer et de nous focaliser sur les idées diverses que nous pouvions trouver sur internet. En effet, le sujet est très vaste et la plus grande difficulté pour nous, fut de concentrer nos idées et de ne pas trop divaguer autour de notre sujet principal.

Afin de réaliser ce projet, nous avons dans un premier temps établi un plan en travaillant en commun. Suite à cela, nous avons pu nous répartir les différentes parties.

- Bara et Elise ont travaillé sur la présentation de la voiture autonome et les risques liés.
- Maëlys s'est intéressée au dilemme éthique.
- Charlotte s'est chargée de l'assurance et des données à caractère personnel.
- Mathilde s'est occupée des droits de l'utilisateur d'un véhicule connecté ainsi que des responsabilités juridiques.
- Victor a quant à lui travaillé sur la sécurité du véhicule.

Une fois la répartition établie, nous avons pu travailler chacun de notre côté. Cependant, nous échangeons sur nos parties respectives en cas d'interrogations afin de pouvoir être aidés par un autre membre du groupe. De plus, lorsque l'un des membres du groupe trouvait un élément au cours de ses recherches qui pouvait être intéressant pour une partie d'un des autres étudiants, il le partageait avec celui-ci.

Nous avons utilisé tout au long du projet un Google doc afin d'y déposer l'avancée de nos recherches et que chacun puisse voir ce que faisaient les autres. Une fois nos différentes parties rédigées, nous avons mis en forme le rapport et apporté des commentaires pour améliorer le travail de chacun.

2.2. Organigramme des tâches réalisées et des étudiants concernés.

Elise	Bara	Maëlys	Charlotte	Mathilde	Victor
Quid de la voiture autonome : les risques possibles	Quid de la voiture autonome : présentation de la voiture autonome	Dilemme éthique	Assurance et DCP	Droits de l'utilisateur d'un véhicule connecté et responsabilités juridiques	Sécurité du véhicule
Introduction	Conclusion	Objectifs	Lexique	Organisation du travail	Introduction
Relecture du rapport et mise en page					

3) Quid de la voiture autonome

3.1 Présentation de la voiture autonome

Un véhicule est qualifié d'autonome s'il peut se déplacer sans l'intervention continue d'un opérateur humain. Le concept désigne ainsi, un véhicule pouvant circuler sur la voie publique dans le trafic sans la surveillance du conducteur en toutes situations.

Un véhicule autonome est équipé de capteurs d'images par caméras, de radars, de sonars et de lidars, dont les données sont traitées par des processeurs et des logiciels dédiés. En prenant en compte toutes les données recueillies, ces logiciels reconstituent la situation routière 3D par reconnaissance de formes : à savoir les voies, les véhicules, les obstacles, les panneaux, les limites de chaussées...

L'intelligence artificielle et l'usage des algorithmes sont au cœur de ce système, puisqu'ils sont nécessaires pour décider et mettre en place les différentes actions à réaliser sur les commandes du véhicule. De plus, les actions décidées par ces logiciels sont réalisées par servocommandes sur le volant pour gérer la direction, la vitesse en contrôlant l'accélération et le freinage, et diverses interfaces, notamment avec le conducteur du véhicule et avec les conducteurs des autres véhicules en diffusant des signaux lumineux. Il s'agit donc d'une application typique du domaine de la robotique mobile dans laquelle de nombreux acteurs sont engagés.

Néanmoins, le niveau d'automatisation du véhicule reste l'élément le plus important. On distingue 6 niveaux d'automatisation d'un véhicule : le premier est où il n'y a aucune automatisation, tel que le conducteur a la maîtrise complète du véhicule. Le deuxième correspond à l'automatisation d'une fonction précise : le conducteur dispose d'un dispositif d'aide à la conduite, notamment à l'aide d'un

système de contrôle électronique de la stabilité ou d'assistance au freinage. Le troisième niveau concerne l'automatisation de plusieurs fonctions combinées : deux fonctions se combinent dans certaines situations précises, par exemple un système de régulation adaptative de la vitesse et un dispositif de maintien au centre de la voie de circulation. Quant au quatrième niveau, il s'agit d'une automatisation partielle de la conduite : le conducteur peut déléguer une partie de la conduite dans certaines situations précises, des capteurs lui indiquant à quel moment il doit reprendre les commandes. Le cinquième niveau permet au conducteur d'assurer une conduite autonome à la demande. On assiste finalement au sixième et dernier niveau d'automatisation qui correspond à une automatisation complète de la conduite du véhicule : le véhicule est entièrement autonome et surveille les conditions de circulation sans aucune intervention humaine. Il suffit donc qu'une personne indique la destination à atteindre puis délègue l'ensemble de la conduite du véhicule.

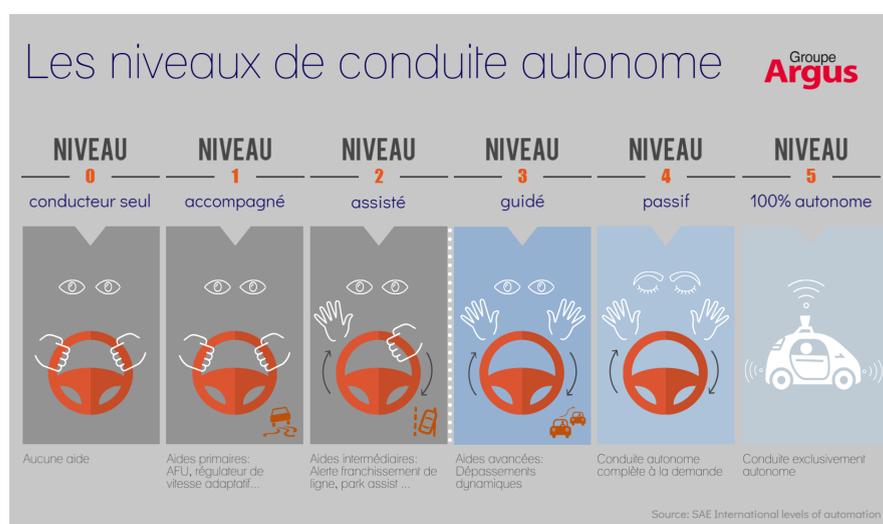


Figure 1 : Les différents niveaux de conduites expliqués par le groupe Argus

3.2 Les différents risques possibles

En France, depuis 2015 plus de 80 expérimentations menées sur la voie publique ont permis aux entreprises d'obtenir de multiples données de conduite afin d'améliorer les algorithmes permettant le fonctionnement de la voiture autonome d'aujourd'hui. En conséquence, après 200 000 kilomètres parcourus, les véhicules expérimentés d'aujourd'hui peuvent gérer des situations plus imprévisibles et d'incidents aléatoires qu'il y a deux ans. Les nombreuses démonstrations de navettes autonomes dans les métropoles ont permis de présenter ce projet au grand public.

Cependant, d'après les travaux menés aux niveaux national, européen et international par de nombreuses commissions comme le CEE ou l'ONU par exemple, il est primordial de développer des études sur l'ensemble des risques qui peuvent perturber le bon fonctionnement et l'équilibre de la conduite de la voiture autonome. Ces risques, qui sont partagés entre les autorités publiques (autorités routières et de sécurité routière), doivent prendre en compte la diversité des cas d'utilisation, en particulier de la diversité de l'environnement de conduite. Ils sont par ailleurs de tout type. D'une part, il peut s'agir de risques dus à une connectivité défectueuse ou à une mauvaise interaction entre le conducteur et le système d'automatisation.

3.2.1 Des risques en raison de la connectivité

Les risques liés à la connectivité sont l'une des principales menaces qui peuvent survenir lors de l'utilisation d'une voiture autonome. En effet, une faille de sécurité peut mener à l'intrusion illégitime d'un tiers dans le système. Cette intrusion est susceptible de provoquer la prise en main de la direction du véhicule, du contrôle d'un quelconque élément du système voire même l'activité de conduite dans son intégralité.

Les attaques informatiques contre les systèmes embarqués des véhicules autonomes n'ont rien de nouveau. Cependant, les voitures ont toujours été conçues pour fonctionner dans des systèmes fermés avec peu ou aucune interaction avec l'extérieur. Ainsi, les attaques externes étaient moindres et plus faciles à éviter ou à détourner. Depuis l'évolution des relations externes, une nouvelle surface d'échanges et de communication est apparue et ne fait qu'augmenter les possibilités d'attaques. Aujourd'hui, il est indispensable d'intégrer au sein de la voiture autonome cette technologie créant de nouvelles possibilités innovantes. Cependant, il faut aussi admettre qu'en contrepartie, le contrôle à distance du véhicule devient un risque réel et présent qui doit être géré.

La prise de contrôle à distance d'un véhicule est ce qu'on appelle le "car hacking". La cybersécurité est au cœur des interrogations et recherches des constructeurs de véhicules autonomes de demain. En effet, il est question d'une distinction entre les réseaux de fonctionnements liés au système de conduite d'une part, comme le freinage par exemple, et la sécurisation du boîtier de communication d'autre part. Les applications Web posent aussi problème et sont un autre aspect clé en termes de sécurité. En effet, celles-ci permettent l'échange de nombreuses informations entre le véhicule et/ou le conducteur et le système informatique du constructeur.

En effet, les hackers sont capables grâce à des sites illicites disponibles sur Internet de se procurer le code de démarrage du moteur que l'on trouve dans l'ECU de la voiture. Cette donnée permet de programmer de nouvelles clés vierges afin de démarrer et voler un véhicule. Ainsi, en 2019, 85 % des voitures volées en France ont été piratées électroniquement. Les ingénieurs en sécurité informatique ont réalisé de nombreux tests afin de comprendre au mieux la vulnérabilité et les différentes failles de ces nouvelles voitures. Grâce à un ordinateur externe, ils ont pris le contrôle des essuie-glaces engendrant une mauvaise visibilité, puis se sont "amusés" à changer le volume de la radio, actionner les freins, mais aussi tourner le volant et couper le moteur.

Mark Greven, Directeur des affaires juridiques de l'Association des constructeurs européens d'automobiles (ACEA) met en lumière ce problème majeur lors d'un discours en février 2018. En effet, celui-ci pose clairement le problème de la durabilité du système de sécurité : *“Entre la mise sur le marché d'un modèle et le jour où le dernier exemplaire de ce modèle disparaît de la circulation, il s'écoule une période d'environ 25 ans. Cela signifie que les équipements de sécurité informatique installés au début de cette période doivent rester valides 25 ans plus tard de façon à pouvoir résister à des attaques extérieures. C'est extrêmement difficile à réaliser et c'est pourquoi nous pensons que l'accès en temps réel crée un risque majeur que nous ne voulons pas courir.* » Cependant, nous sommes tous témoins et conscients des avancées technologiques fulgurantes que l'Homme peut concevoir en quelques années. Il nous est difficile d'envisager une confiance totale dans notre véhicule à l'avenir. En effet, chaque voiture connectée est aujourd'hui dotée de nombreux dispositifs divers tels que les clés USB, Bluetooth, puces, 5G voir 6G... Toutes ces nouvelles technologies sont une révolution pour notre quotidien, mais ce sont autant de portes d'entrée possibles pour un hacker

d'atteindre les données convoitées dont le niveau de sécurité serait, estime-t-on, équivalent à celui des PC aux débuts d'Internet... En exposant ce problème de manière claire et précise, les constructeurs automobiles comme Mark Greven sont dans l'optique d'informer en toute transparence les utilisateurs. Les questions de sécurité et d'authentification doivent aujourd'hui être sérieusement prises en compte afin de pallier ce risque majeur et handicapant à la mise en place de la voiture autonome sur le marché mondial.

L'intrusion illégitime dans le système est aussi susceptible d'entraîner la captation et l'utilisation illicites de données à caractère personnel des conducteurs (DCP) que nous détaillerons dans une autre partie. L'accès à ces données pose problème si le constructeur ou toute autre personne ayant accès aux données dispose d'informations lui permettant d'identifier le conducteur alors que ce n'est pas nécessaire pour atteindre l'objectif visé, constituant une atteinte aux droits fondamentaux.

Dans un second temps, les risques liés à la connectivité engendrent des risques de traçabilité et d'identification des porteurs des objets connectés, comme la géolocalisation. Ce faisant, elle informe sur l'endroit où se trouve le porteur de l'objet et permet de tracer ses déplacements. Des chercheurs ont d'ailleurs montré que seulement 4 points de localisation étaient suffisants pour identifier une personne, alors même qu'aucune des données recueillies n'était identifiante à elle seule. Ces données sont désormais encadrées dans le règlement européen pour la protection des données (RGPD) appliqué depuis 2018.

L'usage de la voiture autonome nécessite l'échange de nombreuses informations, entre les véhicules eux-mêmes et les infrastructures routières : la vitesse du véhicule, son positionnement identifiable grâce au GPS, les différents changements de trajectoire, mais aussi les alertes sur le trafic... Toutes ces informations posent la question de la protection des données à caractère personnel ainsi que la préservation de leur intégrité. D'après le G29 (2011), les objets mobiles connectés sont donc "inextricablement liés aux personnes physiques" et permettent de connaître leurs habitudes de déplacements, leur comportement et leur manière de conduire provoquant un risque de profilage. Ainsi, pour que les usagers donnent confiance à la voiture autonome de demain, la sécurité doit être plus que maîtrisée, la protection de ces informations ressort clairement comme essentielle. Aujourd'hui, tous ces questionnements sont au cœur de réflexions menées par divers groupes de travail comme l'ISO, la Commission européenne de normalisation, et l'ETSI (European Telecommunications Standards Institute). Ces organismes se questionnent sur les canaux de communication envisageables : Wi-Fi véhiculaire, réseaux cellulaires ou réseau satellite. La sécurisation des protocoles de communication est aussi un sujet majeur de discussion.

Cette notion du respect de la vie privée et des données personnelles est fondamentale dans le cadre juridique du véhicule autonome.

3.2.2 Des risques en raison de la modification de la répartition des tâches et de l'interaction entre l'homme et la machine.

La mauvaise répartition des pouvoirs de direction et de contrôle du véhicule s'avère être l'un des risques majeurs pour les conducteurs. En effet, la modification des tâches de conduite et des interfaces hommes-machine pourrait générer un syndrome d'excès de confiance, conduisant à une sous-reprise en main du véhicule pour les niveaux d'automatisation intermédiaires.

L'usage inapproprié d'un système par un conducteur est aussi un problème récurrent. Par exemple, il y a quelques années avec les premiers régulateurs de vitesse, de nombreuses plaintes de conducteurs avaient été soulevées en cas d'accidents. Souvent, la cause du problème n'était pas le système, mais les conducteurs qui avaient mal utilisé le régulateur : pour désactiver le régulateur, ils avaient appuyé sur la mauvaise pédale. De plus, la mixité sur la route entre véhicules classiques et véhicules automatisés, entre véhicules autonomes de conception et de générations différentes, pourrait poser des problèmes de cohabitation et d'adaptation. Par ailleurs, il ne faut pas perdre de vue qu'une partie des usagers de la route, en particulier les plus vulnérables, échappera à cette automatisation : piétons, cyclistes mais aussi les deux-roues motorisés qu'il ne faut absolument pas négliger car trop souvent victimes d'accidents.

Ainsi, il en découle le dernier risque : celui du dysfonctionnement d'un élément du système. En mai 2016, un accident mortel causé par une Tesla, est la conséquence d'un dysfonctionnement : « *Éblouis par une forte luminosité, ni l'Autopilot, ni le conducteur n'ont vu la remorque blanche du camion, et le frein n'a pas été engagé* », a expliqué Tesla. La collision entre ces deux véhicules provoqua la mort du conducteur. Après cet accident, Tesla rappelle que l'utilisation de l'Autopilot requiert une vigilance permanente. Les utilisateurs doivent garder les mains sur le volant en permanence ce qu'il n'est pas le cas de beaucoup de conducteurs souligne Tesla. Une formation des conducteurs avant l'utilisation d'une voiture autonome pourrait être la solution pour pallier ce manque d'assiduité. La marque affirme tout de même que cette innovation réduit considérablement le risque d'accidents en améliorant la sécurité des utilisateurs tout en rappelant que le risque zéro n'existe pas.

4. Dilemmes éthiques

Dans cette seconde partie, nous allons nous focaliser sur les différents dilemmes éthiques soulevés par l'introduction de la voiture connectée dans notre vie quotidienne. Afin de commencer cette réflexion, la première question qui nous vient naturellement à l'esprit est la suivante : qu'est-ce qu'un dilemme moral ?

Un dilemme moral est une situation dans laquelle nous devons faire un choix qui nous mène, dans tous les cas, à commettre une mauvaise action. Pour illustrer ce propos, nous pouvons prendre comme exemple une situation de la série *Good girls*. Dans cette intrigue, une mère de famille, avec que peu de moyens, se voit confronter à un dilemme afin de sauver sa fille qui a absolument besoin d'un donneur de reins pour survivre. Elle se retrouve face à un choix des plus complexe : celui de braquer une banque pour récupérer l'argent nécessaire à l'opération de sa fille, ou ne rien faire et la perdre. Dans une telle situation, le problème qui se pose à nous n'est plus celui de faire le bon choix, mais de faire le moins pénible.

4.1 Les études (comme « la machine morale ») faites à travers le monde.

Publiée le 24 octobre 2018 dans la revue *Nature*, la plus grande enquête réalisée sur l'éthique des véhicules autonomes se nomme la « Machine morale ». Ses auteurs sont Jean-François Bonnefon (docteur en psychologie cognitive et directeur de recherche CNRS), Iyad Rahwan (informaticien à l'Institut de technologie du Massachusetts) et Azim Shariff (psychologue social). Grâce à un questionnaire en ligne, les auteurs ont pu récolter des informations précieuses. Pour cela, les participants sont confrontés à des situations diverses où ils doivent choisir qui épargner entre par exemple des personnes de situations financières différentes, de genres différents, le nombre de

personnes impliquées dans l'accident, ou même choisir entre une personne respectant le code de la route, et une autre non. Cette enquête a été répandue à travers le monde entier. En effet, en 18 mois, ce questionnaire a récolté 40 millions de réponses prises par 2,3 millions de personnes dans 233 pays différents.

Après avoir recueilli les réponses, les auteurs ont analysé les différentes réactions provenant des 130 pays ayant comptabilisé au moins 100 participants, ils ont constaté que les pays pouvaient être divisés en trois groupes. L'un comprend l'Amérique du Nord et plusieurs nations européennes ; un second groupe comprend des pays comme le Japon, la Chine et le Pakistan. Finalement, un troisième groupe se distingue, comprenant l'Amérique centrale et l'Amérique du Sud, ainsi que la France. Dans ces trois groupes, quel que soit leur âge, leur sexe ou leur pays, des premières constatations se dessinent: la plupart des gens préfèrent épargner les humains plutôt que les animaux de compagnie, et plutôt les groupes que les individus seuls. Mais les similitudes s'arrêtent là. Les autres réponses varient selon la localisation dans le monde : par exemple, les participants des pays du troisième groupe préfèrent plutôt sauver les personnes plus aisées en sacrifiant ceux qui le sont moins, a contrario des pays du second groupe.

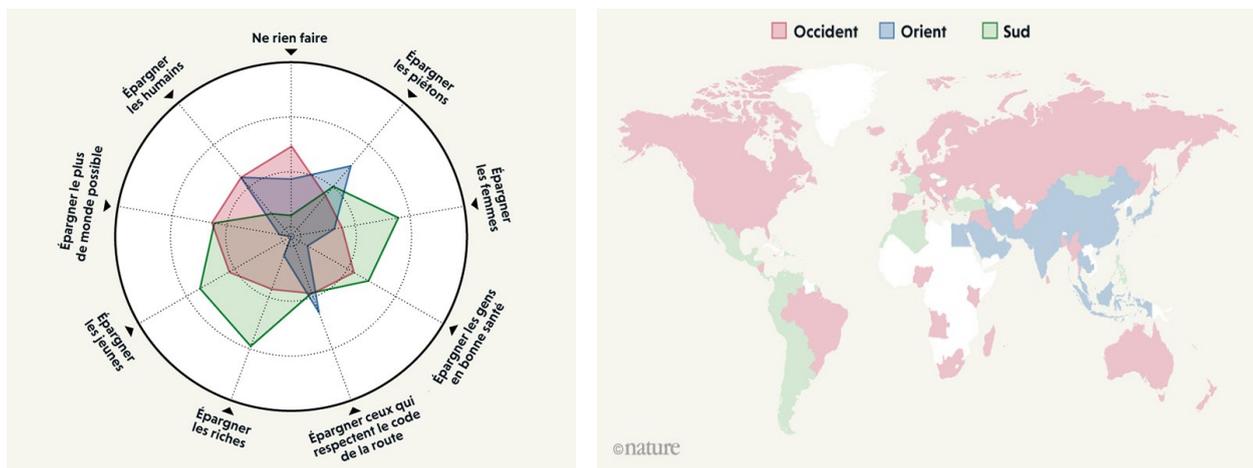


Figure 2 : “Il n’y a pas de solution universelle au dilemme moral de la voiture autonome.”

L'un des auteurs de la “machine morale”, Iyad Rahwan explique qu’il n’y a pas de décisions basées sur un accord commun : « Les gens qui réfléchissent à l'éthique des machines partent du principe que l'on peut trouver un ensemble de règles parfait pour les robots. Mais ce que nous montrons avec ces données, c'est qu'il n'existe pas de règle universelle ».

En réalité, les gens sont rarement confrontés à de tels dilemmes moraux. De plus, dans de telles situations, rare est le temps que nous avons pour réfléchir... Certains se demandent si les scénarios proposés dans le questionnaire sont pertinents par rapport aux questions éthiques qui se posent dans la « vraie vie » avec les voitures sans conducteur. Mais les auteurs de l'étude affirment que ces scénarios sont un bon modèle des subtiles décisions morales que les conducteurs prennent chaque jour. En effet, Jean-Gabriel Ganascia, spécialiste d'intelligence artificielle au laboratoire d'informatique de l'université Paris-VI, explique qu'en réalité, “il y a peu de situations où de tels dilemmes se rencontrent. Le véhicule cherche à limiter les accidents et à anticiper. Elle limitera la casse de toute façon”. Les auteurs soutiennent que les résultats révèlent des nuances culturelles que les

gouvernements et que les constructeurs de voitures autonomes devraient prendre en compte s'ils veulent que ces véhicules soient acceptés par le public.

Le dilemme éthique qu'évoque la machine normale a donc évoqué les principales polémiques qui ne mettent pas tout le monde d'accord. Mais l'ambiguïté n'est pas qu'ici. En effet, il y a également d'autres sources d'interrogations : et si l'intelligence artificielle ne fonctionne pas ?

Tout d'abord, pour les constructeurs de voitures autonomes, il est très difficile de comprendre pourquoi un élément du système ne fonctionne pas. Cela est dû à un problème de répétabilité. Par exemple, si l'on effectue exactement 3 fois le même test, il peut très bien s'avérer que 2 fois le test ne marche pas et la troisième fois, il fonctionne parfaitement. Comme ces voitures autonomes fonctionnent essentiellement grâce au machine learning et sur l'intelligence artificielle, il est extrêmement difficile de comprendre quelle est la cause d'un tel dysfonctionnement. L'origine de la faille peut-être due à des problèmes de capteurs ou à l'interprétation défectueuse d'un signal qui a été enregistré. D'ailleurs, les tests qui seront effectués dans un avenir proche pour motoriser ou mettre en service les voitures autonomes seront très difficiles à interpréter pour ces différentes raisons.

Par ailleurs, un point important à prendre en compte est le fait que l'homme a une tolérance plus faible envers l'erreur machine qu'envers l'erreur humaine. C'est pourquoi, pour que les voitures autonomes soient acceptées par le grand public, elles devront être quasiment parfaites.

Finalement, après avoir analysé les différents dilemmes éthiques soulevés par la question de la voiture autonome et la difficulté d'anticiper les actions de l'intelligence artificielle, nous sommes en capacité d'étudier et d'interpréter les lois déjà mises en vigueur sur le sujet du véhicule autonome.

5. Lois déjà en vigueur du véhicule autonome

5.1 Les droits de l'utilisateur d'un véhicule connecté

L'utilisateur d'un véhicule connecté possède un ensemble de droits variés. Pour les illustrer, nous allons détailler ces différents droits notamment par l'exemple d'un système de géolocalisation installé dans des voitures de fonction. Toutefois, les droits sont les mêmes pour les particuliers qui détiennent un véhicule connecté. Dans le cadre des systèmes de géolocalisation dans le milieu professionnel, l'employeur doit respecter l'article L. 1121-1 du Code du travail « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ». Ainsi par ce biais, l'utilisateur d'un véhicule connecté possède les droits suivants :

- *Le droit à ne pas être connu ou reconnu dans ses déplacements :*

L'utilisation de dispositifs de géolocalisation dans des véhicules de fonction est autorisée. En dehors du temps de travail, les employés peuvent désactiver la collecte des données de géolocalisation. Ces données ne peuvent être accessibles que par l'employeur, par le personnel habilité des services concernés et par le personnel habilité d'un client. De plus, le nom du conducteur n'est communiqué à aucun client ou donneur d'ordre. De plus, l'employeur doit fournir à son salarié les données d'utilisation du véhicule à sa demande. Afin d'accéder au dispositif de suivi en temps réel sur Internet, il faut se munir d'un identifiant et d'un mot de passe.

- *Le droit à l'information :*

L'utilisateur du véhicule a le droit à l'information. En effet, lors de l'installation d'un dispositif de géolocalisation, l'employé doit être informé : *“de l'identité du responsable de traitement, des finalités poursuivies, de la base légale du dispositif, des destinataires des données issues du dispositif de géolocalisation, de son droit d'opposition pour motif légitime, de la durée de conservation des données, de ses droits d'accès et de rectification et de la possibilité d'introduire une réclamation auprès de la CNIL”*.

- *Droit à consentir :*

L'utilisateur dispose du droit à consentir pour certaines choses. Notamment en ce qui concerne le recueil et le traitement des données. De plus, il peut faire savoir son souhait de désactiver le dispositif en cas de non-respect des conditions légales posées par la CNIL ou d'autres textes.

- *Droit d'accès, d'opposition, rectification et effacement :*

L'utilisateur peut accéder aux données afin de les consulter. Il peut dans certains cas les effacer. Les données sont conservées deux mois. Cependant, on peut les conserver un an si elles sont utilisées à des fins d'optimisation ou de preuve des interventions effectuées. On peut les conserver jusqu'à 5 ans lorsqu'elles sont utilisées pour le suivi du temps de travail.

L'ensemble de ces droits respecte donc le RGPD « *Règlement Général sur la Protection des Données* ». Celui-ci concerne le traitement des données personnelles sur le territoire de l'UE.

5.2 Les Données à Caractère Personnel (DCP)

Les Données à Caractère Personnel correspondent à toute information relative à une personne identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un ou plusieurs éléments qui lui sont propres. Par exemple, un identifiant, un nom, un numéro d'identification ou, dans le domaine de véhicule autonome : les données de localisation, le numéro de plaque d'immatriculation et le numéro de série du véhicule sont des données à caractère personnel. Ce sont donc des éléments spécifiques qui se rapportent à *l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale d'une personne* d'après le projet RGPD de juin 2015.

Pour assurer la protection de ces données personnelles, plusieurs lois ont déjà été mises en place. Les données sont donc protégées par des obligations de sécurité afin de respecter les droits fondamentaux. Ces obligations sont imposées par des corpus juridiques européens et français. Parmi ces lois, on retrouve la convention européenne pour la protection des DCP de 1981 instaurée par la Cour Européenne des Droits de l'Homme (CEDH). On distingue aussi, le droit communautaire, c'est-à-dire l'ensemble des règles qui s'appliquent à l'intégralité des pays membres de l'Union européenne. Ce droit a établi plusieurs mesures notamment avec la directive 95/46/CE sur la protection des DCP, avec la directive 2002/58/CE « *vie privée et communications électroniques* » avec la charte des droits fondamentaux de l'Union Européenne. Par ailleurs, le droit interne, c'est-à-dire le droit français, dispose de la loi Informatique et Libertés du 6 janvier 1978 qui régit l'utilisation des données personnelles. Cependant, cette loi a été remplacée par le Règlement Général sur la Protection des Données (RGPD) qui s'applique au niveau européen depuis le 25 mai 2018 et permet donc d'unifier tous les pays sous une même réglementation. Le RGPD a modifié le renseignement de données. Le

consentement doit désormais être explicite pour communiquer des informations. Le RGPD apporte aussi de nouvelles mesures qui protègent encore plus les données personnelles et leurs différentes utilisations.

<p>1 Votre consentement pour communiquer vos informations doit être explicite</p> 	<p>Votre consentement doit maintenant être donné aux entreprises par une approbation très claire, fini les cases pré-cochées !</p>	<p>RGPD pour les nuls Les 7 points clés RGPD, en vrai, c'est quoi ? Destiné à remplacer la loi informatique et libertés, le règlement général sur la protection des données personnelles encadre la manière dont les géants du numérique gèrent les informations dont ils disposent sur vous, internautes.</p>
<p>2 Les entreprises n'ont le droit de collecter que ce qui est strictement nécessaire</p> 	<p>Pour toute newsletter ou promotion, une entreprise n'a besoin que de votre adresse mail ou de votre numéro (que vous aurez consenti à lui donner).</p>	<p>5 15 ans : l'âge légal pour s'inscrire sur les réseaux sociaux (sans autorisation parentale) Les députés français ont retenu, pour l'instant, l'âge de 15 ans pour que chaque mineur puisse consentir seul au traitement de ses données personnelles en ligne.</p>
<p>3 Vous pouvez demander que toutes vos données soient transférées</p> 	<p>Si vous changez d'opérateur téléphonique, vous pouvez demander que toutes vos informations soient transférées de votre ancien opérateur vers le nouveau (et supprimées chez l'ancien).</p>	<p>6 Possibilité d'exercer une action de groupe devant la justice Si vous vous sentez victime d'une violation de la protection de vos données, vous pouvez exercer une action de groupe (« class action »).</p>
<p>4 Vous pouvez demander que vos données soient supprimées à tout moment</p> 	<p>Si vous en faites la demande, vos informations personnelles peuvent désormais être supprimées à tout moment.</p>	<p>7 Sanctions pour les entreprises Pour les entreprises qui ne seraient pas conformes à cette réglementation, le risque de sanctions est élevé : jusqu'à 20 millions d'euros ou 4 % du chiffre mondial annuel de l'entreprise.</p>

Figure 3 : Protection des données : la RGPD

Afin de protéger les données personnelles, différents principes ont été mis en place. Toutes données récoltées doivent avoir été recueillies à des fins légitimes, explicites et déterminées. Cela signifie que l'utilisation des données est définie clairement par des règlements ou des contrats où le consentement pour les différentes utilisations est demandé. Ces finalités peuvent avoir pour but la recherche, les statistiques ou l'historique. De plus, ne peuvent être collectées que les données nécessaires, qui sont pertinentes à la finalité. Une fois que les données personnelles sont collectées, les détenteurs de ces données doivent assurer la transparence des traitements faits avec les utilisateurs. Ils doivent faire preuve d'une certaine loyauté. Ce sont deux caractères fondamentaux imposés par la Cour de Justice de l'Union européenne de 2015. Tout système qui utilise ou stocke ces données doit être sécurisé et chaque donnée doit être confidentielle et à conservation limitée. Cela passe par un effacement ou une anonymisation irréversible dès que les données ne sont plus nécessaires.

Cependant, d'autres lois protégeant les données personnelles existent dans les autres pays. Ces lois sont plus ou moins en accord avec celles de l'Union européenne. Par exemple, l'Argentine et le Canada sont respectivement en adéquation et en adéquation partielle avec le RGPD alors que les Etats-Unis ou l'Australie possèdent une autorité indépendante et des lois différentes qui sont reconnues par la conférence internationale des commissaires à la protection de la vie privée et des données personnelles. La Chine et la Russie détiennent une législation générale sur la protection des données ou quelques dispositions spécifiques.

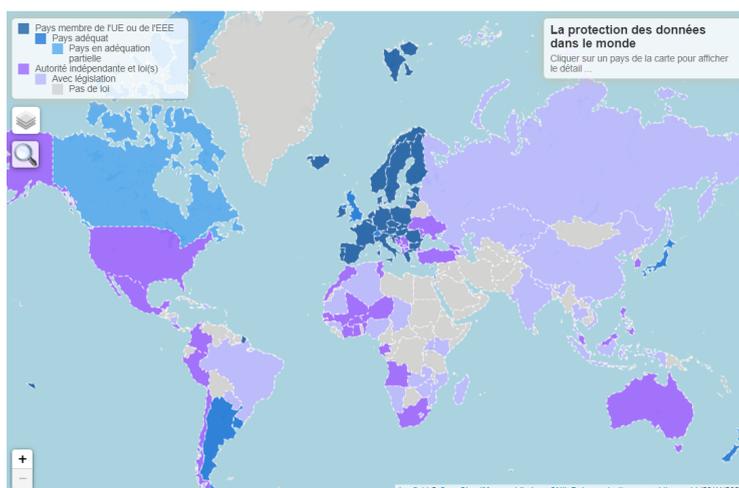


Figure 4 : La protection des données dans le monde

5.3 Responsabilité juridique

Les véhicules autonomes et connectés soulèvent une nouvelle question. En effet, quand est-il de la responsabilité juridique en cas d'accident ? Quel est le ou bien les responsables ? Cette responsabilité peut se répartir entre trois cas : le concepteur du véhicule, son constructeur ou alors le conducteur.

Les lois qui entourent cette avancée technologique sont encore très récentes. La première législation concernant la mise en circulation de ces véhicules a vu le jour en France avec le décret du 28 mars 2018. Ce décret concerne l'expérimentation des véhicules à délégation de conduite. Plus précisément les véhicules autonomes de niveau 4. Ce sont des véhicules pouvant effectuer des tâches ordonnées par le conducteur et ne nécessitant pas l'intervention de celui-ci. L'expérimentation de ceux-ci ayant lieu sur les voies de circulation avec les autres usagers de la route implique la possibilité d'un accident et donc le besoin d'une législation autour.

Tout d'abord, afin de s'adapter à cette avancée, le décret a modifié l'article R 322-3 du Code de la route. Il stipule maintenant que les véhicules autonomes ayant reçu l'autorisation pourront évoluer sur des voies ouvertes à la circulation publique. En ce qui concerne l'expérimentation des véhicules autonomes de transport public et de marchandise, ce sont les articles R 3113-10 et R 3211-12 du Code des transports qui sont modifiés par le décret.

En ce qui concerne la responsabilité en cas d'accident, d'après la loi Badinter du 5 juillet 1985, c'est celle du conducteur qui est retenue. D'après le décret, ce conducteur qu'on appelle dès lors « superviseur humain » devra être en mesure de reprendre le contrôle du véhicule à tout moment. Le superviseur se trouve soit à l'intérieur du véhicule soit à l'extérieur et sera donc en mesure de reprendre le contrôle de celui-ci au moyen d'un processus de télécommande. C'est pourquoi l'article L 121-1 du Code De La Route s'applique aux véhicules autonomes et connectés. L'article déclare la chose suivante « *le conducteur d'un véhicule est responsable pénalement des infractions commises par lui dans la conduite dudit véhicule. Toutefois, lorsque le conducteur a agi en qualité de préposé, le tribunal pourra, compte tenu des circonstances de fait et des conditions de travail de l'intéressé, décider que le paiement des amendes de police prononcées en vertu du présent code sera, en totalité ou en partie, à la charge du commettant si celui-ci a été cité à l'audience* ».

De plus, d'après la loi Badinter, elle souligne que concernant la responsabilité civile, il y a obligation d'indemnisation à charge du conducteur ou du gardien du véhicule impliqué.

Une nouvelle question accompagne la responsabilité juridique autour de ces véhicules. Comment distinguer le commettant et le préposé ? En effet, avec l'avancée de cette technologie, le superviseur pourrait perdre le réel statut de conducteur. Dans ce cas, qui serait le responsable ? D'après l'article 1242 du Code Civil « *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* ». La question de la distinction entre le commettant et le préposé se pose alors. L'article L 121-1 du Code de La Route, cité précédemment, soulève également cette question concernant la responsabilité d'autrui. On définit le commettant comme étant « *la personne qui exerce une autorité sur une ou plusieurs personnes appelées préposés* ». Il a pour rôle de donner des consignes, ordres à des préposés effectuant la mission qui leur a été demandée. Le préposé est quant à lui défini comme « *la personne qui accomplit un acte ou exerce une fonction sous la subordination du commettant* ». Dans certains cas, c'est le commettant qui est mis en cause et non le préposé.

Il est aussi intéressant de s'intéresser à la responsabilité juridique dans le cas d'un accident dû à une défaillance de l'algorithme de conduite. Des dispositifs d'enregistrement permanent des paramètres de conduite sont installés dans les véhicules autonomes. Ce sont des données confidentielles qui sont effacées régulièrement. Dans le cas d'un accident, elles sont conservées un an afin de servir de support pour déterminer la responsabilité mise en jeu ? En effet, soit cela va permettre au superviseur d'être mis en cause, ou bien d'être exonéré dans le cas d'une défaillance de l'algorithme de contrôle du véhicule ou d'une défaillance du véhicule indépendante de l'aspect autonome de celui-ci. Dans ces deux cas, la responsabilité s'orienterait sur le constructeur. En effet, d'après la loi du 19 mai 1998 et la directive de 1985, c'est la responsabilité du producteur qui est engagée. Il s'agit de la responsabilité civile.

5.4 Assurance

En France, la loi oblige toute personne qui possède un véhicule terrestre à moteur à souscrire à une assurance automobile. Pourtant, en mai 1977, la France signe la Convention de Vienne du 8 novembre 1968 qui précise que seuls les véhicules ayant un conducteur sont autorisés à circuler et que ce conducteur doit tout le temps avoir la maîtrise de son véhicule. C'est en 2016 que l'Organisation des Nations Unis (ONU) a réformé cette convention pour que les voitures autonomes soient autorisées à circuler du moment que celles-ci puissent être contrôlées par un conducteur à n'importe quand..

Avec le développement des véhicules autonomes, les assurances vont devoir s'adapter et trouver une nouvelle manière d'assurer les propriétaires de ces nouvelles voitures. En effet, les véhicules autonomes permettent de baisser la fréquence des accidents de la route de 80 %, selon une étude du cabinet KPMG, d'ici à 2040 puisque la majorité de ces accidents est due à une erreur humaine. On estime que cela reviendrait à une baisse de 10 milliards d'euros par an. De plus, la question de la responsabilité juridique lors d'un accident pose problème, car l'assureur ne saurait pas contre qui, entre le fabricant, les pouvoirs publics, le propriétaire de la voiture, se tourner pour payer les indemnités. C'est pourquoi les assurances devront aussi innover en modifiant leurs formules. Ils devront désormais prendre en compte la sécurité informatique du véhicule avec les risques de piratage des systèmes ainsi que les risques technologiques.

Cependant, aucune loi ne peut encore être définie concernant les assurances automobiles puisque la législation a encore besoin d'être définie clairement pour les véhicules autonomes. En effet, comme ces véhicules sont seulement autorisés à circuler pour des expérimentations, les différents assureurs ne peuvent pas encore prévoir de clauses spécifiques pour leurs garanties. En revanche, les assurances peuvent anticiper certains points de leur évolution en réfléchissant à des solutions concernant la responsabilité juridique en cas d'accident. Par exemple, les futurs assureurs pourraient directement être les constructeurs automobiles ou si deux voitures autonomes ont un accident alors les deux conducteurs seraient indemnisés à parts égales, aussi appelées la responsabilité sans faute. Certaines pistes sont donc à développer.

En attendant la mise en circulation des véhicules autonomes, les assurances doivent déjà prévoir une période de transition où ces nouveaux véhicules côtoieront les plus anciens qui n'ont pas un niveau d'assistance aussi élevé. Durant cette période, les assurances vont devoir réfléchir à différentes solutions par rapport aux éventuels problèmes liés aux réactions humaines des conducteurs et celles automatiques des différents instruments de la voiture face aux risques.

6. Sécurité du véhicule

6.1 Protection des données personnelles et de la vie privée

La sécurité du véhicule connecté et autonome est au cœur de toutes les questions des ingénieurs et des entreprises. Cette sécurité réside entre deux points majeurs, la protection des données personnelles de la vie privée de l'utilisateur et la grande question de la cybersécurité.

Le défi de la protection des données personnelles reste très dur et complexe à aborder aussi bien par les entreprises que par les organismes de défense de la vie privée. En effet, quelle est la limite du privée et du public, mais quels seraient les dangers pour un particulier sur cette collecte de données parfois essentielle au bon fonctionnement du véhicule autonome. Le traitement de données personnelles est défini comme ceci par la CNIL : « *Un traitement de données personnelles* » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement). La CNIL commence à s'intéresser à cet aspect des données personnelles. En effet, avec plusieurs acteurs publics et privés, elle a mis en place un « pack de conformité ». Il permet aux entreprises de maîtriser l'aspect « protection des données personnelles » pour les appliquer sur leurs futurs produits.

Cette nouvelle invention du CNIL et des acteurs privés et publics met en avant plusieurs scénarios. Le premier stipule que les données collectées dans le véhicule doivent rester dans le véhicule et qu'elles n'iront jamais chez le fournisseur. Le deuxième scénario est que ces données pourront sortir de l'habitacle du véhicule pour être fournies à un fournisseur, on peut prendre dans ce cas l'exemple de l'assurance « Pay as you drive » (assurance au kilomètre) qui permet de payer son assurance selon l'utilisation réelle que l'utilisateur fait de son véhicule grâce à un logiciel de géolocalisation embarqué dans la voiture. Le dernier scénario précise que les données se verront envoyées à l'extérieur du véhicule pour ensuite y revenir, par exemple dans le cas d'un changement d'itinéraire sur Google Maps, car une route vient d'être bloquée pour travaux. Le problème des deux premiers scénarios est qu'ils sont compliqués à mettre en place dans le cadre des véhicules autonomes. Effectivement, le

troisième scénario est le plus réaliste pour les constructeurs. Grâce à un GPS, une voiture peut facilement se déplacer sur un itinéraire, mais pour les deux premiers scénarios, le véhicule ne pourrait pas communiquer avec son environnement extérieur, il ne pourra donc que se reposer sur ses capteurs internes et sur une carte de route intégrée. Ce qui nous amène au deuxième point qu'un véhicule autonome ne pourra se faire sans une voiture connectée.

De nombreux ingénieurs et scientifiques affirment que plus un véhicule est autonome, plus il faut que ce dernier soit connecté. Aujourd'hui, les multitudes de capteurs, de systèmes embarqués et d'applications du véhicule autonome nécessitent que ce dernier soit relié au réseau Internet. Ces technologies sont vitales au bon fonctionnement de la voiture autonome. On peut donc à juste titre se demander où se termine cette collecte de données et comment protéger l'utilisateur d'une collecte un peu trop intrusive par les entreprises.

En première instance, les entreprises pourraient traiter les données de manière totalement anonyme pour ne pas pouvoir faire le lien entre données et clients. Cette technique appelée anonymisation de données est déjà utilisée dans plusieurs secteurs. Parmi ces secteurs, on retrouve les sondages, les votes électroniques ou sur des cas judiciaires. L'anonymisation est irréversible, en aucun cas, on est en état de remonter jusqu'à la personne derrière ces données sinon cela s'appelle de la pseudonymisation qui est nettement moins sécurisante pour la personne originelle. Encore aujourd'hui aucune loi n'oblige une anonymisation des données des usagers.

Si une anonymisation des données se révélait trop contraignante pour les entreprises, la loi pourrait encadrer cette collecte de données pour tendre à une limitation de données personnelles qui serait plus raisonnable. Elle pourrait imposer une transparence envers les utilisateurs concernant leurs données qui sont traitées, ou obliger une suppression des données après un certain temps. Ce qui rendrait totalement introuvable l'ancien utilisateur. En ce qui concerne les passagers d'un véhicule, les chiffrements, les authentications et les déconnexions régulières permettent au propriétaire du véhicule d'être plus serein s'il faut prêter sa voiture ou même la louer. Les accès aux caméras, qui seront légion dans une voiture autonome, devront être également réglementés, ou tout simplement d'empêcher de s'y connecter physiquement pour en récupérer les données.

En troisième partie, dans le cas du troisième scénario du « pack de conformité » évoqué plus haut, il mentionne les seules données qui devraient être récoltées sont : « Celles qui sont indispensables à la fourniture du service. ». Il évoque aussi la conservation de ces données qui verront leurs durées être plus ou moins longues selon la durée du contrat lors de l'achat du véhicule..

En conclusion, l'aspect juridique des futures voitures autonomes reste donc très flou, même si les pays ont de nombreuses possibilités pour protéger la vie privée de leurs citoyens.

6.2 La cybersécurité et le véhicule autonome

Comme évoqué précédemment, le véhicule autonome requiert une connexion aux environnements en ligne comme Internet, ou le système GPS. Ce qui nous amène au second point : la cybersécurité du véhicule autonome. Les entreprises travaillent dur pour empêcher des pirates ou autres personnes malintentionnées de s'introduire dans le système de leurs voitures. En effet, les raisons sont nombreuses ; pillage de données, dégradation du véhicule de façon virtuelle et matérielle, mise en danger de l'utilisateur ou encore une prise de contrôle à distance.

Le 23 juin 2020, l'ONU élabore une base pour les véhicules concernant la cybersécurité, les logiciels et les systèmes automatisés de maintien de la trajectoire (ALKS : Automated Lane Keeping Systems). Les principales exigences des règlements établis sont que la cybersécurité doit étudier tous les risques possibles que pourraient engendrer le véhicule, et ce, dès la chaîne d'assemblage. Pour cela, les constructeurs devront mettre en place des tests pour détecter les différents incidents de sécurité qu'il pourrait y avoir avec le véhicule. L'ONU évoque également des organismes de contrôle qui prendraient soin de vérifier que les risques sont gérés, de surveiller les cyberattaques et de les contrer au besoin, de toujours se tenir à jour concernant les nouvelles menaces et vulnérabilités qui pourraient évoluer avec le temps. Les règlements ne concernent que les voitures autonomes de niveau 3, et à ce jour, seul Honda, au Japon, commercialise une voiture autonome de niveau 3.

En cas de cyberattaque sur un véhicule autonome, des chercheurs proposent de développer la résilience des systèmes embarqués. Pour notre voiture autonome, cela signifierait que lorsqu'une intrusion malveillante a lieu dans notre système le véhicule bloque toutes ses fonctionnalités et donne accès aux options de bases à l'utilisateur, c'est-à-dire la direction, le frein ou encore la vitesse du véhicule. Les autres solutions pour affronter les cyberattaques seraient de développer des antivirus spécialement conçus pour se protéger des attaques, ou alors de tout simplement couper la connexion au réseau du véhicule, mais ce qui rendrait ce dernier difficilement autonome, on en revient dans ce cas à la résilience des systèmes embarqués, car ces derniers ne pourraient plus utiliser la connexion avec le monde extérieur.

Par ailleurs de plus en plus de constructeurs s'associe avec de grands groupes informatiques, nous pouvons prendre pour exemple Sysgo (filiale de Thalès), une société allemande de technologies de l'information qui fournit des systèmes d'exploitation et des services pour les systèmes embarqués, qui s'allie avec le groupe Vector travaillant dans les systèmes électroniques embarqués pour l'automobile. Ces deux groupes vont travailler ensemble pour répondre aux besoins croissant de la sécurité dans les véhicules connectés et/ou autonomes. Cette recherche dans la sécurité n'est pas nouvelle pour le groupe Thalès, « La cybersécurité et la sécurité des systèmes d'information critiques font partie de l'ADN Thales. Pour le groupe, cette coopération innovante entre Vector et Sysgo est un pas de plus pour l'industrie automobile en matière de services et de conseils en cybersécurité », souligne Laurent Maury, Vice-président, Systèmes d'Information Critiques et Cybersécurité. Ainsi, cette société commune répondra aux défis d'intégration des systèmes et de la cybersécurité dans les voitures connectées et autonomes.

Ainsi, les organismes mondiaux commencent doucement à s'intéresser à la grande question de la cybersécurité pour les véhicules autonomes, mais cela reste malgré tout insuffisant. Dans quelques années, le véhicule autonome sillonnera les routes du monde entier et sa protection contre les attaques extérieures devra être primordiale.

7. Conclusion sur le travail réalisé

Pour conclure, l'étude de l'aspect juridique de la voiture autonome nous a beaucoup apporté. Les recherches que nous avons effectuées sur ce sujet nous ont permis d'acquérir de nouvelles connaissances sur le fonctionnement, les innovations et la progression du véhicule autonome d'une part, et de découvrir la pertinence de cette technologie sur le plan éthique, de l'autre. Ainsi, nous nous sommes très vite rendu compte qu'au-delà de l'aspect technique, les voitures autonomes doivent répondre à des problèmes juridiques et éthiques avant de pouvoir circuler sur les routes.

De plus, tout au long de cette étude, nous nous sommes attachés à analyser les grands axes de l'aspect juridique autour de cette technologie. En effet, nous avons vu que le dilemme éthique associé, remet en question l'intelligence artificielle en faisant apparaître des ambiguïtés et des polémiques qui ralentissent l'avancement de cette technologie. Les différentes interrogations autour des droits de l'utilisateur et de la sécurité du véhicule confirment davantage l'existence de ces ambiguïtés, notamment les questions du traitement des données personnelles et de la cybersécurité qui constituent un défi pour aboutir à une technologie sécurisée des attaques extérieures et qui définit clairement toutes les responsabilités juridiques.

Ainsi, ce projet nous a été très enrichissant sur le plan de la méthode, de la recherche et de la synthèse puisqu'on était amené grâce au travail de groupe à élargir nos connaissances associées au milieu de la voiture autonome et de découvrir la pertinence de son aspect juridique. Le travail d'équipe nécessaire pour mener à bien ce projet a été une expérience très positive pour tous les membres du groupe et nous a permis de nous confronter aux difficultés du travail au sein d'un groupe. Cela ouvre de nouvelles perspectives pour nous sur ce que signifient le travail d'ingénieur et la dimension de gestion de projet qui y est associée.

Pour finir, nous tenions à remercier Mr. Bensrhair, qui a su nous guider et nous fournir de la documentation tout au long de nos recherches, malgré les conditions inédites.

8. Rapport d'étonnement

COTIER Charlotte : Ce projet était très intéressant, car nous avons abordé le sujet du véhicule autonome, un sujet très actuel, par l'aspect juridique que nous connaissons moins contrairement à l'aspect plus technique. De plus, le travail de groupe m'a permis de m'organiser correctement grâce aux réunions hebdomadaires et au suivi de projet.

DESSOULIERS Elise: Ce projet m'a permis d'approfondir le sujet de la voiture autonome, non pas par le biais scientifique, mais par son aspect juridique. Se questionner et comprendre les dilemmes éthiques qui sont au cœur des débats actuels, m'ont permis de développer une vision critique. S'interroger sur les questions morales dans le cadre d'un objet scientifique est, je trouve, très intéressant pour notre formation d'ingénieur.

LEGER Victor : Je connaissais déjà l'aspect scientifique de la voiture autonome, mais concernant l'aspect juridique, je n'avais que très peu de connaissances. Ce projet m'a permis de renforcer mes bases et de découvrir de nouvelles perspectives de la voiture autonome. Le travail de groupe étant essentiel en tant que futur ingénieur, cette expérience a été très enrichissante et elle a amorcé une première approche dans l'organisation d'un projet de groupe.

NTICHA Baraa : J'ai trouvé intéressant de travailler sur un sujet d'actualité et de découvrir le domaine des véhicules autonomes sous une approche juridique qui m'était jusque-là inconnue. De plus, j'ai beaucoup apprécié le travail de groupe qui m'a motivé à m'impliquer davantage dans le but d'aboutir à un travail satisfaisant pour l'ensemble du groupe.

PROUVOST Mathilde : Ce projet était très intéressant, il m'a permis de découvrir un autre aspect des voitures autonomes, celui de la question juridique. J'ai trouvé intéressant de se pencher sur un aspect moins scientifique et d'en découvrir une autre approche. De plus, ce projet m'a permis de travailler en groupe, notamment avec des personnes que je ne connaissais pas avant et j'ai beaucoup apprécié ce travail de groupe. Je trouve cela très bénéfique pour notre formation d'ingénieur.

SAINT-ETIENNE Maëlys : En plus de m'avoir apporté des connaissances sur l'aspect juridique de la voiture autonome, ce projet m'a également permis d'en apprendre davantage sur un sujet aujourd'hui au cœur des polémiques. En effet, il est difficile de savoir où en est l'avancement des recherches sur la voiture autonome sans creuser un minimum ! Malgré les difficultés qu'apportent les cours à distance, notre motivation et notre entraide au sein du groupe nous ont permis d'aboutir à un travail recherché et cohérent. Ce travail m'a donc permis d'échanger avec d'autres élèves, et on sait que la communication est un outil essentiel dans le métier que nous voulons exercer plus tard, celui d'ingénieur.es.

9. Bibliographies et crédits d'illustrations

- [1] Conférence : *véhicule connecté, véhicule "autonome", aspects juridique*. Michèle GUILBOT
IFSTTAR - Département TS2 / Laboratoire MA Séminaire ASPROM – Paris, 11 février 2016
- [2] Pour la Science (2016, 27 juillet) - Le dilemme morale de la voiture autonome
<https://www.pourlascience.fr/sd/science-societe/le-dilemme-moral-de-la-voiture-autonome-9197.php>
- [3] Pour la Science (2018, 26 octobre) - Il n'y a pas de solution universelle au dilemme moral de la voiture autonome
<https://www.pourlascience.fr/sd/science-societe/il-n-y-a-pas-de-solution-universelle-au-dilemme-moral-de-la-voiture-autonome-15004.php>
- [4] Science et Vie TV (2018, 12 septembre) - Les voitures autonomes, sont-elles dangereuses ? (YouTube) <https://www.youtube.com/watch?v=x5LDAjJXiEA>
- [5] Wikipedia contributors. (2021, 17 avril). *Véhicule autonome*. Wikipedia.
https://fr.wikipedia.org/wiki/V%C3%A9hicule_autonome
- [6] *Véhicule à pilotage automatique*. (2014).
<https://www.citrap-vaud.ch/wp-content/uploads/2014/10/Vhc-pilotage-automatique-citrap-vaud-022016.pdf>
- [7] Colombain, J. (2016a, juillet 1). *Une voiture autonome cause la mort d'un conducteur*. Franceinfo.
https://www.francetvinfo.fr/replay-radio/nouveau-monde/une-voiture-autonome-cause-la-mort-dun-conducteur_1786339.html
- [8] *Sécurité des voitures connectées : l'importance de la méthode*. (2016, 27 juillet). Thales Group.
<https://www.thalesgroup.com/fr/systemes-dinformation-critiques-et-cybersecurite/news/securite-des-voitures-connectees-limportance>
- [9] Palfroy, M. (2019, 15 octobre). *Géolocalisation des salariés : que dit la loi ?* Cadremploi. [Géolocalisation des salariés : que dit la loi ? - Cadremploi](https://www.cadremploi.fr/actualites/2019/10/15/geolocalisation-des-salaries-que-dit-la-loi)
- [10] *La géolocalisation des véhicules*. (s. d.). cnil.fr. [Travail et données personnelles \(cnil.fr\)](https://www.cnil.fr/fr/travail-et-donnees-personnelles)
- [11] S. (2020, 12 août). *Droit de la responsabilité et véhicules autonomes*. UCLy. [Droit de la responsabilité et véhicules autonomes - UCLy](https://www.uclouvain.be/fr/actualites/2020/08/12/droit-de-la-responsabilite-et-vehicules-autonomes)
- [12] Salaun, P. (2018, 19 avril). *Véhicules autonomes : quelles responsabilités juridiques en cas d'accident ?* Contrepoints. [Véhicules autonomes : quelles responsabilités juridiques en cas d'accident ? | Contrepoints](https://www.contrepoints.org/2018/04/19/ANALYSE/Vehicules-autonomes-queles-responsabilites-juridiques-en-cas-daccident)
- [13] Données personnelles. (2021, 9 avril). Dans *Wikipédia*.
https://fr.wikipedia.org/wiki/Donn%C3%A9es_personnelles#D%C3%A9finition
- [14] Règlement général sur la protection des données. (2021, 18 avril). Dans *Wikipédia*.
[Règlement général sur la protection des données - UCLy](https://fr.wikipedia.org/wiki/R%C3%A8glement_g%C3%A9n%C3%A9ral_sur_la_protection_des_donn%C3%A9es)

[15] *Assurance auto et voiture autonome : quelles conséquences ?* (2020, 31 juillet). Réassurez-moi.
<https://reassurez-moi.fr/guide/assurance-auto/voiture-autonome>

[16] *La voiture autonome va-t-elle bouleverser le monde de l'assurance auto ?* | Assurpeople. (s. d).
assurpeople.
<https://www.assurpeople.com/assurance-auto/59-la-voiture-autonome-va-t-elle-bouleverser-le-monde-de-l%E2%80%99assurance-auto>

[17] Brause, S. R. B. (2016, juillet). *Comment concevoir la vie privée des passagers à l'ère de la voiture autonome ?* CNIL.

<https://linc.cnil.fr/fr/comment-concevoir-la-vie-privee-des-passagers-lere-de-la-voiture-autonome>

[18] AFP. (2018, octobre). *La cybersécurité, cruciale pour la voiture connectée et bientôt autonome.* Le Point.
https://www.lepoint.fr/automobile/la-cybersecurite-cruciale-pour-la-voiture-connectee-et-bientot-autonome-04-10-2018-2260257_646.php

Crédits d'illustrations :

Page de couverture :

<https://cdn2.nextinpact.com/compress/900-435/images/bd/wide-linked-media/17166.jpg>

Figure 1 : Les différents niveaux de conduites expliqués par le groupe Argus

<https://blog.econocom.com/wp-content/uploads/2018/02/Voiture-autonome-infographie.png>

Figure 2 : "Il n'y a pas de solution universelle au dilemme moral de la voiture autonome"

<https://www.pourlascience.fr/sd/science-societe/il-n-y-a-pas-de-solution-universelle-au-dilemme-moral-de-la-voiture-autonome-15004.php>

Figure 3 : Protection des données : la RGPD

<https://www.republicain-lorrain.fr/economie/2018/06/11/donnees-personnelles-que-change-la-loi>

Figure 4 : La protection des données dans le monde

<https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>