REVUE
de la gendarmerie nationale
REVUE TRIMESTRIELLE / SUPPLEMENT THEMATIQUE / GRATUIT

Le Supplément

Le droit des robots

SOMMAIRE

NUMÉRO HORS SÉRIE

ÉTHIQUE ET SOCIÉTÉ

DOCTRINE JURIDIQUE

SCIENCES APPLIQUÉES

Voiture autonome : quel droit pour les forces de l'ordre ?

par DIDIER GAZAGNE

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 ou que vous soyez sur l'espace public ou privé.

Essayez d'imaginer que les forces de l'ordre[1] 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.

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

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 BASt[2] 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-Autonome.pdf

– la nomenclature NHTSA[3] de l'administration de la sécurité routière aux États-Unis (*National Highway Traffic Safety Administration*) ;

– les travaux de pré-normalisation de l'organisme SAE International[4], situé aux États-Unis, (anciennement *Society of Automotive Engineers*) ;

– la nomenclature du Plan industriel véhicule autonome en France[5].

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.

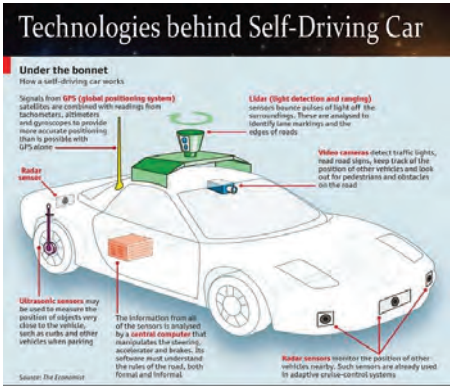
		2 juillet 2014	
Niveau 0 : Pas d'automatisation	Conducteur uniquement	Niveau 0 : Pas d'automatisation	Niveau 0: Pas d'automatisation
Niveau 1: Assistance à la conduite	Conducteur uniquement	Niveau 1 : Automatisation de fonctions spécifiques	Niveau 1 : Assisté
Niveau 1: Assistance à la conduite	Automatisation 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.

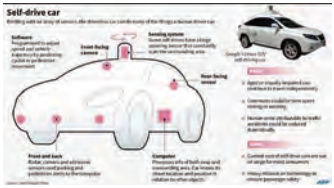
Les 4 schémas ci-après illustrent respectivement :

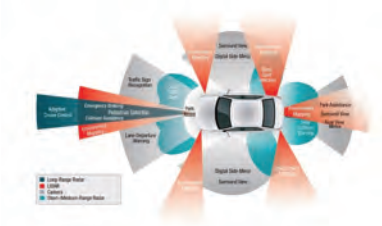
Schémas 1 et 2 : le positionnement des différents capteurs sur un véhicule autonome ;

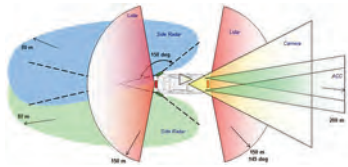
Schémas 3 et 4 : le rôle des différents capteurs sur un véhicule autonome et la surface ou l'environnement de collecte des données.



La voiture autonome intègre également de l'intelligence artificielle (Artificial Intelligence ou IA) qui traite les flux de données propres au véhicule avec les données routières externes et active les commandes du véhicule autonome.







Véhicule autonome et IA

Très récemment, le 16 juin 2016, les sociétés Local Motors et IBM ont présenté Olli[6], le premier véhicule de transport autonome intégrant de l'intelligence artificielle, déjà mis en service à Washington. Le programme informatique 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.

(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

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).

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 ordonne 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 (*vehicule 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 6e pack de conformité[8] afin de concilier l'innovation dans les écosystèmes de l'automobile et la protection des données à caractère personnel des usagers de l'automobile.

(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

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.

(9) http://www.mycarmydata.eu/ ;

Alliance of Automobile Manufacturers

Aux États-Unis, des initiatives d'autorégulation voient le jour. Les constructeurs automobiles ont ainsi adopté une déclaration de grands principes qui entend donner des gages aux possesseurs de voitures concernant le sort réservé à leurs données[10].

(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

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 données[11],

l'approche privacy by design consiste 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.

(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 ;

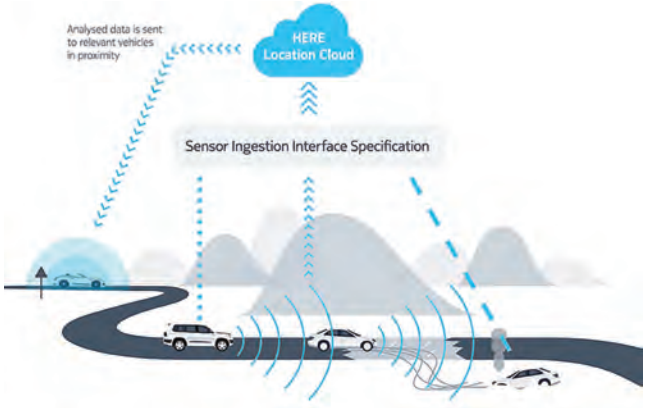
(12) Sur cette question : Chloé Torres, Mettons le cap sur l'approche Privacy by design ! Lexing Alain Bensoussan Avocats http://www.alain-bensoussan.com/privacy-by-design-2/2016/06/09/

L'approche *privacy by design* sera obligatoire en Europe dès le 25 mai 2018[12].

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.



Source : Here.com

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 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

(13) https://lts.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/.

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 d'assurance[15]. 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

(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=JORFTEXT000022227831 ;

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 juge[16].

(16) Cass.crim. 22 octobre 2013, n°13-81945 https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028116516&fastR

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

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 juillet 2015[17] 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

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

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 magistrat[18] en tous lieux et sans le consentement de l'intéressé.

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

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

Les origines du 4e 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 4e 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* ».

(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'État.

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

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 4e Amendement (*unreasonnable 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.

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 4e 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 4e 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 4e 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 4e Amendement, la Cour suprême des États-Unis a fait évoluer sa jurisprudence à la fin du XXe siècle.

Début du XXe

Au début du XXe siècle, la Cour Suprême s'est montrée réticente à appliquer la protection conférée par le 4e 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 Olmstead v. United States (1928)[21], la Cour Suprême a expressément refusé la protection par le 4e Amendement des activités menées dans les lieux publics.

(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

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 énoncé le principe selon lequel le 4e 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* ».

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

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 4e 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 4e 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. Ohio[24] (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 reasonable 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 4e 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 4e 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 (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.

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

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 4e 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 l'affaire Smith v. Maryland[28]. 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.

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

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 4e 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 13 avril 2012[30] faisant état d'un programme informatique intégré aux Google Cars conçu pour collecter ces données personnelles.

(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

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 motifs[31].

(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

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://humanoides.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 spécifiques[33].

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.