Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

L'automatisation des véhicules
Annexes cahier N°2

INSPECTION GENERALE
DE L'ADMINISTRATION
N° 16-040R

CONSEIL GENERAL
DE L'ENVIRONNEMENT
ET DU DEVELOPPEMENT DURABLE
010629-01

- Février 2017 -

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

INSPECTION GENERALE
DE L'ADMINISTRATION

N° 16-040R

CONSEIL GENERAL
DE L'ENVIRONNEMENT
ET DU DEVELOPPEMENT DURABLE
N° 010629-01

L'automatisation des véhicules

Annexes cahier N°2

Etabli par

Jean-François ROCCHI
Inspecteur général
de l'administration

Hervé de TREGLODE
Ingénieur général des mines

Bernard FLURY-HERARD
Ingénieur général des ponts,
des eaux et des forêts

Philippe BODINO
Chargé de mission à l'inspection
générale de l'administration

Frédéric RICARD
Ingénieur en chef des ponts,
des eaux et des forêts

- Février 2017 -

SOMMAIRE

Annexe n° 9 : La cyber sécurité

1. Les vulnérabilités informatiques des véhicules autonomes sont assurément importantes

1.1. Une large surface d'attaque et des vulnérabilités importantes

La vulnérabilité des véhicules modernes est forte. Ce que les spécialistes qualifient de « surface d'attaque » ouvre des brèches dans lesquelles s'infiltrent les délinquants.

Un véhicule automatisé et/ou connecté, présente une très large surface d'attaque informatique. En effet les technologies qu'il embarque au profit de systèmes « intelligents» sont très diverses et nombreuses. Les radars, lidars, caméras de plus en plus nombreux et nécessaires à l'automatisation fonctionnent sur la base de lignes de code informatique, et sont associés à des calculateurs (ECU : Electronic Control Unit). On trouve aujourd'hui plus de 80 calculateurs sur certains véhicules haut de gamme et leur nombre est élevé dans toutes les gammes. Ceux-ci agissent aussi sur les organes de fonctionnement classique du véhicule (moteur, freinage, gestion de l'habitacle, divertissement, localisation, direction, verrouillage centralisé, ouverture des portes et démarrage, téléphonie mains libres…). Ces calculateurs peuvent communiquer directement avec des bases à l'extérieur de la voiture. Ils sont installés en réseau par lequel transitent les données : le CAN (Controller Area Network), qui véhicule jusqu'à 60 millions de lignes de code et jusqu'à 20 Giga-octets d'échanges par heure. Ce réseau aboutit à la prise OBD (On Board Diagnostic). Celui qui s'y connecte y collecte toutes les données utiles pour réaliser les diagnostics et l'entretien des véhicules (garagistes). En outre, on trouve toutes les fonctions de GPS, et d'infotainment. Le véhicule communique aussi vers l'extérieur (plateformes, infrastructures, autres véhicules, fournisseurs, bases de données…) par diverses voies : la téléphonie, le Bluetooth, le wifi, d'autres fréquences. Enfin l'e-call sera obligatoire dès 2018 sur tous les véhicules.

C'est donc un objet connecté qui présente une large surface d'attaque informatique en tous points, et dont la cybersécurité globale ne vaut que par son point le plus faible[1]. C'est en outre un objet particulier par son usage et le fait qu'il transporte des passagers.

Selon l'ANSSI, la surface d'attaque est très importante, mais elle est cependant délimitée en petites parcelles technologiques de systèmes « propriétaires ». Cependant il existe des points de faiblesse qui peuvent concentrer les attaques : la prise OBD, le bus CAN qui canalise et mutualise les données. En outre, ce sont des « standards » qui font des ponts entre les parcelles, ce qui est un facteur aggravant. Une fois que l'on est sur le réseau, on peut tout faire et notamment upgrader ses propres fonctions d'administrateur.

L'ANSSI classe les menaces en 4 catégories, par technicité croissante[2].

- Atteinte à l'image : défiguration de sites, propagande. Le constructeur peut faire l'objet d'une attaque de ce type. Les acteurs n'ont pas besoin d'un grand niveau technique.

- Cybercriminalité : relative impunité de ceux qui conduisent les attaques (c'est le règne de l'anonymat).

[1] Exemple aux États Unis, chez les magasins Target, les données de 115 millions de clients ont été piratées via le prestataire de climatisation, dont le système est relié au « bus » central. Quand on a affaire à un « système de systèmes », c'est le point le plus faible qui compte. De nouveaux réseaux autonomes bas débit à faible consommation qui pourraient transmettre des informations simples du véhicule vers des bases arrière présentent aussi des possibilités de failles. SIGFOX et LORA (Internet Of Things) sont les plus connus qui pourraient venir sur le champ des véhicules autonomes.

[2] Le classement de l'OCSTI est un peu différent : Sécurité (déni de service (DOS) / intimidation / terrorisme (tuer les occupants ou en faire une arme par destination vers une foule par exemple))… vie privée : connaissance de la façon de conduire / vol de données personnelles / écoutes téléphoniques / vidéosurveillance / localisation… autres (financiers) : vol / reprogrammation de clé / demande de rançon (le véhicule ne fonctionne plus) / manipulation du cours de bourse du constructeur.

- Espionnage.

- Sabotage. C'est ce que l'ANSSI craint le plus et où elle concentre les efforts. Il n'y a pas d'exemple pour le moment sur les véhicules. Mais, des cas dans le domaine de l'énergie (exemple de centrales nucléaires et de stockage de gaz) font penser que les véhicules seront impactés. Par exemple, attaque de centres de services ou de plateformes de supervision ou attaque du véhicule lui-même. Le problème est aussi la multiplicité d'acteurs, y compris ceux du monde du divertissement.

En termes de sensibilisation des écosystèmes, on remarque que le top management est en général convaincu, les RSSI aussi. La difficulté semble être avec le « middle management ». On y rencontre des problèmes culturels. Par exemple les gens issus des « automatismes » sont convaincus de la sûreté de fonctionnement de leurs systèmes, car ils ont élaboré une « logique » de fonctionnement, mais ils ne tiennent pas compte de la malveillance.

Notons enfin un paradoxe pour ceux qui ne font pas de la mise à jour d'applications sensibles de peur d'ouvrir la porte à des virus ou de se rendre vulnérables. Cela conduit au fait que les systèmes les plus critiques sont les moins mis à jour. La télétransmission de mises à jour reste néanmoins une faille propice à la malveillance.

La surface d'attaque est immense mais les pouvoirs publics font confiance aux constructeurs et au marché pour la sécuriser. Il faut cependant noter un bémol dans la phase intermédiaire. Les véhicules qui vont sortir en 2017 embarqueront déjà des fonctions connectées vulnérables par ce que pas encore suffisamment bien pensées au niveau cybersécurité.

Voler un véhicule en simulant sa clé électronique, discréditer un constructeur en provoquant des dysfonctionnements, prendre le contrôle d'un véhicule pour effrayer son conducteur, créer des bouchons, tuer ses passagers, le précipiter sur une foule, etc. sont des menaces qui n'ont rien d'imaginaire. L'atteinte à l'image, la cybercriminalité, l'espionnage, le sabotage, vont assurément toucher les véhicules automatisés et leurs constructeurs.

1.2. Des cas d'atteinte à la cybersécurité sont déjà constatés

Le vol par « mouse jacking » (imitation des signaux émis par les clés) se développe en France et dans le monde[3]. Plusieurs démonstrations de prise de contrôle de véhicules ont été réalisées par des chercheurs ou des hackers parfois employés par les constructeurs dans le cadre de la recherche sur la sécurité. En outre, des attaques massives sur des sites conduisant au « déni de service » sont de plus en plus fréquentes. Elles pourraient toucher dans le futur des plateformes réservées aux véhicules automatisés. Enfin le vol de données personnelles est un problème sensible.

- **Hausse du nombre d'affaires de vol sans effraction[4]**

La sécurité des ouvertures de portes à distance de nombreux modèles de voitures serait particulièrement vulnérable. Des chercheurs en Allemagne et en Grande-Bretagne ont dévoilé une faille de sécurité qui concernerait environ 100 millions de véhicules dans le monde, rapporte la presse allemande. Une étude[5] parvient à démontrer la très grande vulnérabilité des boîtiers qui commandent l'ouverture et la fermeture des véhicules, basés sur un système de code tournant (rolling code). Les chercheurs affirment que « pour la

[3] Le taux de vols par mouse jacking serait de plus de 50 % selon la société « Traqueur».

[4] Depuis deux ans, le nombre de voitures volées est reparti à la hausse après 12 années de baisse (+2,3 % en 2015), soit plus de 110 000 véhicules volés l'an passé, un préjudice estimé à 1,2 milliards d'euros pour les compagnies d'assurance, rappelle 40 millions d'automobilistes. « Le mouse-jacking reste la pratique dominante avec 70 % des vols », commente Pierre Chasseray, délégué général de l'association.

[5] Menée par Flavio Garcia, David Oswald et Pierre Pavlidès, chercheurs de l'Université de Birmingham, en collaboration avec Timo Kasper, de la société Kasper & Oswald GmbH spécialiste des questions de sécurité informatique.

plupart des fermetures de porte, il existe des outils qui permettent de décoder la serrure pour créer une clé correspondante». En effet, les grands constructeurs automobiles, et notamment les véhicules fabriqués par Volkswagen depuis 1995, ne proposent qu'un faible nombre de combinaisons. Par ailleurs, selon les chercheurs, un pirate informatique qui aurait récupéré les algorithmes de chiffrement aurait simplement besoin d'intercepter un seul signal de la télécommande d'un véhicule pour reproduire le code de la clé de voiture.

Des problèmes de sécurité du même type ont également été identifiés par les chercheurs chez d'autres constructeurs parmi lesquels les français Citroën (Nemo, Jumper), Peugeot (207 notamment) et Renault (Clio, Twingo, etc.), l'italien Fiat (Punto, Panda...), l'allemand Opel (Astra, Corsa, etc.), le japonais Nissan (Qashqai notamment), l'américain Ford (Ka) ou d'autres marques. Ainsi, selon les chercheurs, ces failles de sécurité expliquent le nombre grandissant d'affaires de vol sans effraction que les assureurs refusent de prendre en charge.

Ces études se vérifient sur le terrain. Cela a été confirmé par l'institut de recherche criminelle de la gendarmerie nationale qui a présenté plusieurs cas à la mission, parmi lesquels le vol de soixante véhicules entre 2012 et 2015 au moyen d'une tablette modifiée qui se connecte au bus CAN. On peut aussi voir sur Youtube des publicités pour des outils informatiques frauduleux qui simulent la clé du véhicule pour s'en emparer, puis lorsque le véhicule est aux mains des voleurs, reproduire la clé électronique à partir de la prise OBD.

- **Démonstration de piratage et de contrôle à distance par les chercheurs ou les hackers**

À l'été 2015, deux chercheurs américains en informatique ont démontré qu'il était facile de prendre le contrôle d'une voiture « connectée » via des SMS. Charlie Miller et Chris Valase étaient parvenus à pirater à distance la Jeep Cherokee d'un journaliste du site spécialisé Wired. Ils avaient ainsi pu allumer la radio, faire fonctionner les essuie-glaces et couper le moteur. Ils étaient aussi parvenus à désactiver les freins.

En 2016, des chercheurs chinois en cybersécurité[6] ont révélé des failles de sécurité exploitables à distance sur une Tesla Model S. Dans une vidéo publiée sur leur blog, ils interagissent à distance avec le véhicule grâce à un ordinateur. Ils ouvrent les portes et le coffre, désactivent le panneau de bord, activent les clignotants et les essuie-glaces, sans être physiquement présents dans le véhicule. L'un des chercheurs, qui se trouve à plus de 15 km de là, déclenche les freins du véhicule alors que la Model S est en route, sans que les feux ne s'allument. Ils ont réussi à s'emparer du véhicule sans le moindre contact physique, mais « après plusieurs mois de recherche intense », selon eux. Le piratage visait l'un des systèmes internes de la Model S, le bus CAN, qui assure notamment la transmission des données entre ses différents composants électroniques. Sur leur blog, les chercheurs affirment avoir testé la procédure sur plusieurs versions de la Tesla Model S. Ils pensent « raisonnable de supposer que d'autres modèles construits par Tesla sont concernés par ces failles ». Ils ont depuis présenté leur découverte à l'entreprise américaine, qui, dans un communiqué, déclare avoir réglé le problème grâce à une mise à jour logicielle. Ce communiqué précise que si la faille existait bel et bien, elle était exploitable « uniquement quand le navigateur Internet du véhicule [situé sur le tableau de bord] se trouvait en cours d'utilisation ». De plus, Il était également nécessaire que la voiture soit connectée à un réseau Wifi non sécurisé, selon Tesla. « *Toutes les démonstrations ont été réalisées sans contact et sans modification physique sur la voiture* », explique la vidéo. Les prises de contrôle ont été réalisées sur deux modèles de Tesla S, la P85 (à l'arrêt) et la 75D (en mouvement). Cependant, les scientifiques affirment avoir testé les failles sur d'autres véhicules Tesla S avec succès. « *Il est raisonnable de supposer que les autres modèles Tesla sont aussi concernés* », précisent encore les chercheurs sur leur blog.

[6] Samuel LV, Sen Nie, Ling Liu et Wen Lu, du Keen Security Lab.

- **Travailler avec les hackers**

Les « *menaces évoluent* », avance Titus Melnyk chargé de la sécurité chez Fiat Chrysler Automobiles (FCA), qui vient de lancer un programme visant à encourager les hackers à informer le groupe des failles liées à la cybersécurité de ses voitures. Le constructeur des Jeep promet une prime pouvant aller jusqu'à 1 500 dollars par alerte. « *On ne sait jamais. Cela peut être la base d'une attaque* », défend M. Melnyk, insistant sur le fait que ce programme est « *très sérieux* ». En 2015, le constructeur Tesla avait été le premier à faire appel à des hackers après que certains d'entre eux aient révélé qu'ils pouvaient couper à distance le moteur d'une berline Model S en piratant son système multimédia. GM, qui dit recevoir et résoudre plusieurs alertes liées à de possibles cyber attaques par jour, gère un programme sur les vulnérabilités de ses voitures sur le site hackerone.com.

- **Attaque conduisant au déni de service[7]**

Le 22 septembre 2016, le blog de Brian Krebs, un chercheur reconnu en sécurité informatique, était rendu inaccessible par une attaque informatique. Le site a été visé par une attaque dite de « déni de service », qui consiste à saturer un site de connexions pour en bloquer l'accès ou faire tomber les serveurs qui lui permettent d'exister en ligne. La puissance d'une attaque de ce type se mesure en gigabits par seconde (Gbps) – le volume de trafic envoyé vers le serveur du site. Celle-ci a été estimée à 620 Gbps, ce qui en fait l'une des plus importantes de l'histoire d'Internet[8]. Le site a été rendu totalement inaccessible, malgré le système de protection dont il bénéficiait[9].

Le même jour, l'hébergeur et fournisseur d'accès français OVH était victime d'une tentative de blocage massive – une série de 26 attaques simultanées de plus de 100 Gbps. Ce qui rend ce type d'attaques difficiles à contrer, c'est qu'elles sont dites « distribuées » – l'afflux de connexions ne provient pas d'une seule source, qui pourrait alors être bloquée aisément[10].

De nombreux spécialistes affirment depuis des années que « l'Internet des objets » représente une menace importante – non pas à cause des objets en tant que tels, mais parce que de très nombreux modèles d'objets connectés vendus dans le commerce sont insuffisamment protégés et donc aisément piratables. Contrairement aux ordinateurs ou aux smartphones, ils ne bénéficient que rarement de mises à jour régulières et restent connectés en permanence à Internet ; ce qui en fait des cibles idéales pour des personnes cherchant à créer des botnets de grande envergure.

Le 24 octobre 2016, ce sont les géants Facebook et Google qui ont vu leur activité perturbée pendant une journée par le même type d'attaque.

Enfin, le vendredi 25 novembre 2016, sur les écrans des salariés de la Municipal Transportation Agency (MTA), chargée des transports en commun de San Francisco, le message suivant est apparu « *Vous avez été piraté, toutes les données sont chiffrées.* ». Même si ce piratage n'a pas perturbé la circulation des transports, il a permis aux usagers de voyager gratuitement le vendredi soir et le samedi, les portiques ayant été ouverts. Le procédé ressemble à un logiciel de racket (ransomware), qui consiste à chiffrer les

[7] Selon l'entreprise Verisign, qui a récemment publié un rapport sur le sujet, elles auraient progressé de 85 % dans le monde entre la fin de 2014 et la fin de 2015.

[8] Lorsque l'attaque dépasse la centaine de Gbps, il s'agit d'une attaque majeure – les plus grandes attaques mesurées ces dernières années atteignaient 300 Gbps.

[9] Mis en place par une filiale du géant d'Internet Akamaï, le site est revenu en ligne épisodiquement durant les deux jours suivants, avant qu'Akamaï ne jette l'éponge, expliquant qu'il pouvait protéger le site mais que cela aurait un coût – près de 200 000 dollars à l'année – une somme que M. Krebs ne pouvait pas payer. Google lui a alors proposé de fournir gracieusement son propre système de protection contre ce type d'attaque – le site de M. Krebs est depuis normalement accessible.

[10] Pour réaliser ces attaques, les assaillants ont le plus souvent recours à un *botnet*, un réseau de machines infectées qui participent toutes, à l'insu de leur propriétaire, à l'attaque. La particularité de cette attaque, qui atteint ces débits inédits, est qu'il s'agit d'un « botnet » non pas composé d'ordinateurs, mais de machines beaucoup plus simples – et notamment de caméras de surveillance. M. Klaba explique que son entreprise a repéré 145 607 caméras qui semblaient faire partie du réseau.

données présentes sur un ordinateur jusqu'à ce que la victime accepte de payer une rançon pour les déverrouiller. Le message qui s'est affiché sur les ordinateurs contenait ainsi une adresse courriel, qu'a contactée The Examiner (journal de San Francisco). Le pirate a répondu « *Nous faisons ça pour l'argent, et rien d'autre* », expliquant que le réseau de transports de San Francisco n'était pas directement visé. Selon lui, un salarié a téléchargé le logiciel malveillant, ce qui aurait suffi pour toucher l'ensemble du système. « *Notre logiciel tente d'infecter tout ce qu'il trouve* », a-t-il précisé, en réclamant 69 000 €.

- **Vol de données**

Les nouvelles technologies embarquées exposent également les conducteurs à un vol potentiel de leurs données personnelles quand ils connectent leur téléphone intelligent. En effet, des données personnelles sont stockées ou transmises à travers les systèmes multimédias des véhicules, ce qui ouvre des opportunités pour les hackers. L'une des pistes, sur laquelle s'accordent les experts, pour contrer les pirates est un partage des informations entre acteurs du secteur. Par exemple aux États-Unis, les groupes automobiles et leurs équipementiers ont obtenu en 2015 du ministère américain de la Justice de pouvoir travailler ensemble sur le sujet sans risquer des accusations d'entente.

- **Les « brouilleurs »** : déjà aujourd'hui des véhicules utilisent des brouilleurs pour ne pas être repérés. (brouilleurs de leurs propres données et de données périmétriques)

On le voit les menaces sont nombreuses et diverses. Il n'existe pas de cartographie précise des menaces et de leur évaluation. Or, la cybersécurité est un point stratégique.

2. Les acteurs de la cybersécurité

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) auprès du Premier ministre a la mission de faciliter la coordination des politiques pour la cybersécurité en France. Elle se donne pour rôle d'introduire des exigences de cybersécurité dans le dossier technique (exemple : ordonnance pour les expérimentations), de sensibiliser les constructeurs (référentiels, labellisation, qualification et agrément), de labelliser les systèmes et les composants (avec la difficulté du secret industriel), de bâtir des protocoles de tests…

La DGEC du MEEM a en charge la réglementation technique liée aux véhicules, dont la cybersécurité, y compris à l'international (notamment au WP 29[11]).

L'observatoire central des systèmes de transport intelligent de la gendarmerie nationale (OCTSI) fondé le 1er juillet 2015 a pour objectif de recueillir du terrain les données pertinentes, de les analyser, de suivre l'état de l'art et de proposer des évolutions en matière de sécurité routière (prévention des accidents) et de sûreté (prévention d'actes malveillants)[12]. C'est le seul observatoire de ce type en Europe.

Les instituts de recherche : dans le cadre du plan NFI, l'Institut VeDeCOM pilote un groupe sur les aspects relatifs à la connectivité dont l'un des thèmes est : « *permettre un contrôle à distance sécurisé et une exclusion d'un élément malveillant* ». L'IRT SystemX[13] fait de même sur les aspects relatifs à la sécurité avec pour thème : « *assurer la cybersécurité du système véhicule autonome et connecté dans son environnement* », mais les projets ne sont pas encore lancés. Très peu d'études ont été faites.

Pour les constructeurs et les industriels, c'est un gros enjeu, mais pour le moment il y a peu de partage, au motif de sécurité industrielle et d'intelligence économique.

[11] Forum d'harmonisation des règles pour les véhicules (ONU).

[12] Productions de l'OCSTI : guide pour les enquêteurs sur le mouse jacking/articles de sensibilisation sur le problème cyber/études et fiches/conférences/rapport au ministre**/**séminaire annuel/participation à la task force et au groupe inter administrations.

[13] Il y a 8 IRT en France, issus des investissements d'avenir. C'est une nouvelle façon de faire travailler ensemble les industriels et les chercheurs, et d'essayer de sortir de la logique de subvention.

Sur le cas plus spécifique des forces de l'ordre, la gendarmerie a beaucoup investi ce domaine parce qu'elle considère que le véhicule automatisé n'est pas un objet connecté comme les autres, mais aussi parce que c'est un domaine à grands enjeux[14]. Outre l'OCSTI, elle dispose du pôle judiciaire de la gendarmerie nationale notamment du plateau d'investigations véhicules[15], et de plusieurs départements de l'IRCGN[16]. La police a choisi une voie différente et n'est pas aussi présente dans ce dossier. Elle n'occupe pas pour le moment la place qui lui est réservée à l'OCSTI.

Trois principes peuvent être retenus pour structurer le dispositif de lutte contre la cybercriminalité et de renforcer les processus :

- L'approche commune police-gendarmerie, en particulier par le partage des structures (OCSTI, plateau véhicules…), des outils (GENDIAG[17]) et des méthodes (fiches réflexe, guide d'enquête) ;

- La mise en réseau est essentielle : les services doivent participer au groupe inter administrations, tisser des partenariats avec des centres de recherche, échanger des stagiaires, développer des projets communs ;

- Le partenariat d'échanges avec des constructeurs est stratégique, notamment pour le développement technologique spécifique aux besoins des forces de police, l'identification des fragilités des véhicules volés et la réponse à apporter, récupération des données des Event data recorders (EDR), etc.

Ce troisième point est fondamental aussi, pour l'ensemble des acteurs. En effet les pouvoirs publics comptent sur les constructeurs pour mettre en place des mesures efficaces de cybersécurité, car elles sont stratégiques pour eux. Il est donc essentiel que les constructeurs soient associés et s'associent à toutes les démarches relatives à cette thématique. La gendarmerie bâtit des partenariats avec les constructeurs : des conventions sont en cours avec Renault et PSA, qui organisent essentiellement des échanges d'informations.

La coordination des acteurs est néanmoins balbutiante. Elle prend notamment la forme d'un tour de table ponctuel dans le groupe de travail inter administrations et la task force, mais n'est pas organisée en mode de projet. Les constructeurs ne sont pas encore assez ouverts et associés. Il n'y a pas de coordination spécifique à la thématique de Cybersécurité. Il y a une forte prise de conscience qui génère du foisonnement. Chacun construit donc ses propres réponses, parfois en partenariat bilatéral, mais la réponse globale n'est pas encore structurée.

La cybersécurité concerne tous les véhicules, même ceux qui ne sont pas hautement automatisés. L'e-Call, obligatoire à partir de 2018, est un nouveau point d'entrée. Elle regarde tout autant d'autres moyens de transport : trains, bateaux… La coordination en matière de cybersécurité doit être élargie sur la base de ce périmètre étendu.

Il est possible de prendre exemple sur ce a été fait pour la sécurité des cartes de paiement : la mise en place d'un « observatoire » qui a débouché sur des outils concrets comme « 3D secure ». Le dialogue est indispensable entre des acteurs qui peuvent collaborer en phase de pré-industrialisation, puis devenir

[14] La lutte contre la criminalité numérique : 260 enquêteurs, 1 700 référents cyber, plus les brigades. Cette branche est a priori déjà surchargée.

[15] Qui apporte un soutien aux enquêteurs afin de les aider à identifier un véhicule qui pourrait être volé ou à le localiser (40 % de ces saisines proviennent des unités de police nationale de la préfecture de police de Paris).

[16] Véhicules (VHC) et informatique électronique (INL) qui apportent leurs expertises et le centre de lutte contre les criminalités numériques (C3N) qui assure une veille informatique pour suivre et réprimer la délinquance associée sur les réseaux et qui conduit des actions de recherche pour reproduire les attaques *(hacking*) et comprendre la capacité des *hackers* et leur niveau supposé.

[17] GENDIAG est un projet commun qui a abouti à la réalisation d'un outil permettant d'identifier tous les calculateurs d'un véhicule en se branchant sur la prise OBD.

concurrents ensuite (exemple des opérateurs téléphoniques et des banques). Une autre approche est de désigner un coordinateur thématique.

3. La réponse aux menaces

Une approche cadre a été proposée par l'ANSSI : Pour assurer la cybersécurité des véhicules connectés et automatisés, il faut rapidement tenir compte des considérations suivantes :

- le nombre des véhicules connectés augmentera de beaucoup durant la décennie à venir, même celui des véhicules connectés à bas coût, notamment en raison des équipements obligatoires à bord comme l'e-Call (appel d'urgence) ;

- la cybersécurité doit être prise en compte aussi tôt que possible en tant que domaine à traiter obligatoirement lors de la réception par type, en clarifiant et harmonisant les règles que doivent appliquer les constructeurs comme les équipementiers ;

- l'approche européenne envers la cybersécurité devra être fondée sur des règles tirées de la réglementation internationale préparée à Genève ;

- comme tout nouveau véhicule sera bientôt confronté au problème de la cybersécurité, il faudra introduire des dispositions envers la cybersécurité dans le règlement de la Commission économique pour l'Europe des Nations-Unies n° 10 (sur la compatibilité électromagnétique) ou n° 116 (sur la protection contre les usages non autorisés), ou bien bâtir une nouvelle réglementation internationale pour les catégories M (voyageurs) et N (marchandises) de ladite Commission économique ;

- les dispositions devront être fondées sur les normes existantes, notamment celles qui s'appliquent aux industries autres que l'industrie automobile ;

- les nouvelles dispositions de la réglementation automobile devront astreindre les constructeurs à installer des systèmes de cybersécurité qui devront être testés et validés avant toute mise en service ;

- il faudra répondre convenablement à la question des mises à jour par la technologie OTA (over the air) ou par des correctifs (patchs) de sécurité pour les voitures déjà en circulation.

Ainsi l'ANSSI a-t-elle été conduite à présenter les recommandations suivantes, rédigées avec la DGEC, et adressées au WP 29 :

- effectuer **une analyse de risques**, un audit de conformité et des tests d'intrusion avant toute mise en circulation d'un nouveau type de véhicule, cela pouvant constituer un nouveau chapitre dans le processus de réception (homologation) des véhicules ;

- adopter le principe de la **sécurisation dès la conception** pour les logiciels comme pour les matériels (composants, dispositifs, véhicule), cela permettant à l'ensemble des parties prenantes de mieux **sécuriser les architectures** et les réseaux en s'appuyant notamment sur la défense en profondeur (isolation des fonctions critiques), le filtrage des flux, le chiffrement des flux, etc. ;

- utiliser, s'ils existent, des **composants labellisés** (certifiés ou qualifiés par l'ANSSI[18]), par exemple pour les unités de commande électronique : ECU pour Electronic Control Units, TCU pour Telecommunication Control Unit, les passerelles (Gateways) qui isolent les fonctions sensibles) des véhicules ;

[18] L'ENISA est l'agence européenne de sécurité des systèmes d'information.

- assurer le **maintien en condition de sécurité** des véhicules via des mises à jour à distance dite OTA (Over The Air)[19] ou par le biais de la prise OBD (On Bord Diagnostic), mais en prenant garde au fait que ces mises à jour multiplient les possibilités de compromission des systèmes et doivent donc être particulièrement maîtrisées ;

- garantir la **sécurité opérationnelle** (supervision, détection et gestion des incidents) pour déceler et prévenir les attaques informatiques, le suivi global de la sécurité et la réponse aux incidents de sécurité pouvant s'appuyer sur une adaptation du SOC (Security Operations Center) à l'univers automobile ;

- tracer et journaliser les **événements informatiques** en vue d'une analyse approfondie le cas échéant ;

- prévoir un **mode dégradé ou manuel** en cas de problèmes liés à la cybersécurité ;

- mettre en place une **structure d'échange** dédiée au secteur automobile sur les menaces et les réponses à apporter aux cyber attaques à l'instar de ce qui existe dans d'autres pays ou dans d'autres domaines en France, la constitution d'un CERT (Computer Emergency Response Team) dédié à l'univers automobile étant un gage d'efficacité ;

- introduire dans les corpus **réglementaires et normatifs** relatifs à l'automobile des exigences de cybersécurité ;

- adopter une approche holistique, intégrer **l'infrastructure routière et les infrastructures de télécommunication d**ans le champ d'analyse.

Ces recommandations et les analyses de risques devront former un nouveau cadre pour l'approbation de la sécurité de tous les véhicules connectés.

Selon l'ANSSI, la réception d'un véhicule devrait être subordonnée à un audit de conformité aux nouvelles règles de cybersécurité.

C'est donc une approche réglementaire et normative[20] que préconise l'ANSSI. Les règles techniques relatives aux véhicules sont établies au niveau international (ONU et commission européenne), notamment dans le cadre du WP 29 qui reste encore très orienté vers la protection des données. La réglementation technique n'impose pas aujourd'hui d'exigence relative à la cybersécurité.

La parole de la France y est portée par la DGEC, qui a proposé les recommandations de l'ANSSI (citées plus haut) dans le groupe de travail ITS. Elles ne figurent pas toutes dans une contre-proposition concomitante germano-japonaise. Une difficulté subsiste : la France propose d'intégrer ces propositions dans la réglementation technique internationale, alors que les Allemands et Japonais veulent en faire de simples lignes directrices. Or, tous les véhicules neufs embarquent déjà des fonctions connectées insuffisamment bien conçues au regard de la cybersécurité. Le WP 29 n'a pas encore chargé l'un de ses groupes de travail

[19] L'identification du véhicule est une difficulté selon systèmX. Il faut développer une base de données de certificats qui permettent de garantir « qui vous êtes ». Il faut expérimenter les problèmes d'authentification des entités qui communiquent (VtoV ; VtoI). Il faut générer des certificats (PKI : public key infrastructures) toutes les 10 minutes ou moins… En outre, on rencontre une difficulté culturelle : dans le monde IT ont fait une mise à jour dès que l'on trouve un trou de sécurité. Le monde du transport a pour culture d'attendre car il faut ré-homologuer.

[20] L'approche normative est aussi une piste. Les normes ne sont pas toujours opposables, mais tous les constructeurs les respectent. De nombreuses normes concernent les équipements automobiles. Dans le domaine de la sécurité, l'ISO 26262 publiée en 2011 (« Véhicules routiers - Sécurité fonctionnelle») pour les systèmes de sécurité dans les véhicules routiers à moteur est largement reprise mondialement. Elle définit un cadre et un modèle d'application, ainsi que les activités, les méthodes à utiliser et les données de sortie attendues. Sa mise en œuvre permettra de garantir la sécurité fonctionnelle des systèmes électrique/électronique dans les véhicules automobiles (c'est une adaptation de la norme CEI 61508 prenant en compte les spécificités de ce secteur). L'association SAE a publié un guide de recommandations en termes de cybersécurité début 2016 (SAE J3061).

de proposer des évolutions réglementaires pour imposer le respect de règles de cybersécurité dans le processus d'homologation. Des lignes directrices pourront être utiles dans l'intervalle nécessaire à la production réglementaire.

La position américaine, se rapproche de la position allemande. Elle est traduite dans les « guidelines » publiées par le ministère fédéral des transports le 19 septembre 2016[21].

Le Parlement européen a adopté la directive NIS (Network and Information Security) le 6 juillet 2016. Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » (dont le secteur des transports) et certains fournisseurs de services numériques seront soumis à des exigences de sécurité et de notification d'incidents de sécurité.

L'Europe fixe un cap, mais ce sont les États membres de l'UE qui devront identifier les entités concernées par la directive, en déterminant quelles autorités nationales sont compétentes pour contrôler l'application de la directive, en adoptant une stratégie nationale de sécurité des réseaux et des systèmes d'information (identification des risques, prévention, gestion et réponse à incidents). Sans oublier que la sécurité des réseaux et des SI inclut la sécurité des données stockées, transmises et traitées. Chaque État membre devra désigner un ou des centres de réponse aux incidents de sécurité informatique (CSIRT), ou un centre de réponse aux urgences informatiques (CERT), pour alerter, suivre et analyser les incidents à l'échelon national.

La transposition de la directive NIS entrée en vigueur le 19 juillet 2016, doit intervenir au plus tard le 9 mai 2018. La France s'est déjà lancée (elle est en avance sur ce sujet : elle a fortement inspiré la directive, avec les allemands, et a été désignée pilote pour la transposition). Un dispositif déjà en place[22] permet d'appliquer certaines mesures aux OIV (249 opérateurs d'importance vitale, sur une liste classifiée). Le dispositif de transposition de la directive NIS, en cours d'élaboration, s'en inspire et sera formalisé en 2017.

Les premiers arrêtés encadrant la sécurité des OIV ont été publiés. Le Journal Officiel vient de publier 3 arrêtés applicables au 1er octobre 2016 fixant « les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité » pour le secteur des transports (terrestre, maritime et fluvial, aérien)[23]. L'arrêté précise les modalités de déclaration des systèmes d'information d'importance vitale (SIIV), de déclaration des incidents de sécurité, de désignation de la personne représentant l'opérateur auprès de l'ANSSI. Les règles de sécurité[24] font l'objet d'une annexe

[21] Synthèse et traduction : *« Ce domaine est un domaine en évolution et plus de recherches sont nécessaires avant de proposer une norme réglementaire. Il faut donc dans un premier temps, développer des produits robustes intégrant les menaces de cybersécurité, inclure systématiquement l'évaluation du risque. La sécurité doit être globale et par conception et le système doit être apprenant. Les constructeurs sont encouragés à concevoir leurs systèmes après avoir étudié les meilleures pratiques, notamment en prenant appui sur les principes publiés par l'institut national pour les normes et pour la technologie, la NHTSA, le SAE, l'alliance de fabricants automobiles… Le processus entier doit être documenté (les actions de changement, les choix de conception, les analyses doivent être tracées…). Le partage industriel est important. C'est le but du centre auto-ISAC : l'apprentissage de groupe. À cette fin, les entités (principalement les constructeurs) devraient rapporter toutes les fragilités, les découvertes d'incidents de terrain, les tests internes, ou la recherche de sécurité externe à auto-ISAC dès que possible indépendamment de leur adhésion au centre. Ces entités devraient envisager d'adopter une politique de révélation de vulnérabilité. ».*

[22] Article 22 de la loi de programmation militaire du 18 décembre 2013, puis décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale.

[23] Les règles ont été définies par 18 groupes de travail représentant 12 secteurs dont les transports, puis par le dialogue entre l'OIV concerné et l'ANSSI. Fruit de ces échanges, les arrêtés fixent donc un ensemble de règles strictes en matière de sécurité pour les OIV sur les systèmes d'information d'importance vitale (SIIV) identifiés comme tels, qui devront être homologués à travers un dossier et un audit. Cet audit porte sur l'architecture, la configuration, l'organisationnel et les tests d'intrusion. Il est réalisé par un prestataire qualifié par l'ANSSI ou en interne.

[24] Il s'agit des règles de politique de sécurité des systèmes d'information, homologation de sécurité, cartographie des systèmes d'information, maintien en condition de sécurité, journalisation, corrélation et analyse des journaux, détection, traitement des incidents de sécurité, traitement des alertes, gestion des crises, identification, authentification, droit d'accès, comptes

précise et exigeante. Ces règles sont contraignantes et devraient peser entre 5 et 10 % du budget de la DSI de tout OIV, selon l'ANSSI.

La philosophie de la loi de programmation militaire repose sur une assiette réduite d'opérateurs avec une exigence forte, sur la base du concept de sécurité nationale et de la notion d'opérateur d'importance vitale. La philosophie de la NIS pourrait s'appuyer sur une assiette plus large avec des exigences moins fortes, sur la base du concept de continuité du marché et de la notion d'opérateur essentiel. En France, les opérateurs d'importance vitale sont déjà listés, les opérateurs essentiels doivent l'être.

Dans l'intervalle qui nous sépare de la date limite de transposition, il peut être utile d'analyser dans quelle mesure cette directive pourrait être applicable à la problématique de la cybersécurité des véhicules autonomes. En outre, la NIS concerne des opérateurs mais pas leurs objets, et donc en l'occurrence pas les véhicules, ni les données (qui sont du domaine de la CNIL).

Cependant les règles de la NIS pourraient être appliquées aux futures plateformes de supervision, et aux réseaux de collecte et de transfert de données (vers e-call, assureurs, assisteurs, constructeurs). Une structure d'échange et de partage des alertes, des incidents de sécurité, de leur analyse et de leur traitement est en outre nécessaire, comme c'est déjà le cas aux États-Unis (auto–ISAC). Les outils mis en place par la NIS, notamment un CERT (Computer Emergency Response Team) spécifique aux véhicules connectés ou autonomes, pourraient être une solution. Ce CERT ne devrait pas être limité aux seuls constructeurs, afin de continuer à permettre les remontées d'incidents pour la connaissance de l'état de la menace. Il pourrait s'imbriquer dans l'architecture du CERT racine, aujourd'hui confié à l'ANSSI.

d'administration, systèmes d'information d'administration, cloisonnement, filtrage, accès à distance, installation de services et d'équipements, indicateurs.

Annexe n° 10 : L'état de la recherche en France et dans le monde

Les développements sur les voitures autonomes sont les plus nombreux. Ils sont particulièrement intenses en Chine (depuis peu), en Corée du Sud, aux États-Unis, en Europe (Allemagne, Espagne, France, Royaume-Uni, Suède, etc.) et au Japon. Il y en a aussi dans d'autres pays, comme en Australie, et à Singapour. Partout, ils s'appuient sur des essais (sur route fermée), des expérimentations (sur route ouverte à d'autres circulations) et des simulations numériques. Les recherches portent surtout sur les capteurs et l'intelligence artificielle. Pour tous, les trois problèmes les plus difficiles à dénouer concernent : (1) la reprise en main, (2) la mise en trajectoire de sécurité et (3) la compréhension des comportements humains alentour. Les recherches sur l'adaptation nécessaire des routes (niveau de maintenance, etc.) sont moins nombreuses, sauf pour les connexions I2V. La raison en est que l'industrie s'efforce de mettre au point, dans la mesure du possible, des systèmes qui soient capables de circuler partout, qu'il y ait une bonne signalisation routière (marquages au sol, etc.) ou non. La recherche s'intensifie autour des enjeux du développement du véhicule autonome. Les travaux portent sur les capteurs, sur la cartographie numérique, sur l'interface entre le conducteur/passager et le véhicule, et sur les aménagements de l'infrastructure (y compris la connectivité). Il s'y ajoute les travaux portant sur la sécurité des systèmes (lutte contre la cyberdélinquance). Bien entendu, les recherches consacrées à l'intelligence artificielle (notamment sur le « deep learning », ou processus d'apprentissage de l'intelligence artificielle) profitent au véhicule autonome.

I. En France

L'effort de recherche est partagé entre le secteur public et le secteur privé (en réalité, des passerelles ont été établies grâce à la NFI ou dans le cadre des Investissements d'avenir. Les principaux instituts engagés dans ces travaux sont, comme décrit dans le rapport au § 1.2.4., l'IFSTTAR, le CEREMA, l'INRIA, l'IRT SystemX, et VeDeCom.

• **L'IFSTTAR** (Institut français des sciences et technologies des transports, de l'aménagement et des réseaux, établissement public à caractère scientifique et technologique)

L'IFSTTAR est particulièrement présent sans les recherches sur le comportement.

Son Laboratoire de psychologie des comportements et des mobilités (LPC) de l'IFSTTAR a publié **un rapport important** sur le comportement des véhicules automatisés et de leurs conducteurs : « Intention to use a fully automated car : Attitudes and a priori acceptability » (publié le 9 mai 2014) de William Payre (Institut Vedecom), Julien Cestac (IFSTTAR) et Patricia Delhomme (IFSTTAR). La Mission CGEDD-IGA a été particulièrement intéressée par les résultats.

Les trois auteurs ont montré que la reprise en main sans entraînement en cas d'urgence pouvait durer en moyenne de 2 à 8 secondes. En cas d'anticipation, le système prévenant alors à l'avance de la nécessité de reprendre le contrôle de la voiture, le temps de reprise en main varie en moyenne entre 3,6 et 15,2 secondes pour la première reprise de contrôle, et en moyenne de 2,7 à 13,9 secondes pour la seconde reprise de contrôle. La reprise en main peut donc être nettement au-dessus du temps généralement considéré comme convenable, à savoir 10 secondes. Les auteurs ont conclu par trois points clefs :

- il faut apprendre aux conducteurs à se servir convenablement d'un véhicule pleinement autonome (afin de réagir convenablement lors des reprises en main),

- un haut niveau de confiance peut paradoxalement augmenter le temps de reprise en main en cas d'urgence,

- un entraînement approprié peut atténuer les conséquences fâcheuses de l'excès de confiance sur les temps de reprise en main.

• **Le CEREMA** (Centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement, établissement public administratif)

Le CEREMA est particulièrement impliqué dans les expertises sur les infrastructures, l'aide à la conduite, la signalisation. Il a travaillé sur les aspects psychologiques (développés dans l'annexe n° X sur l'acceptabilité sociale).

- L**'INRIA** (Institut national de recherche en informatique et en automatique, établissement public à caractère scientifique et technologique) est un acteur clé dans le domaine de l'intelligence artificielle, et intervient comme partenaire dans des projets de véhicules de niveau 5.

- **System X** (Institut de recherche technologique issu du programme des investissements d'avenir) :

Fort de 82 chercheurs et 34 doctorants, assisté par de nombreux partenaires (61 industriels et 14 établissements académiques), l'institut de recherche technologique (IRT) SystemX, fondé en 2012, est chargé[25] de la sécurité au titre du plan sur les véhicules autonomes de la Nouvelle France Industrielle (NFI). Sa mission porte sur la sécurité des véhicules automatisés entendue comme (1) la sûreté de fonctionnement et (2) la cybersécurité. Ses objectifs sont :

  - de « recommander les méthodes et les outils pour l'aide à la conception et la validation du VA [véhicule autonome] », et à ce dessein, de « proposer les méthodes et les outils afin de démontrer l'atteinte des objectifs de sûreté de fonctionnement », et de « recommander, proposer et partager des modèles et des formats permettant la construction d'une bibliothèque de cas tests »,

  - d'« analyser la vulnérabilité Cyber du véhicule particulier »,

  - de « coordonner et mettre à jour la feuille de route technologique « Sécurité et Sûreté de fonctionnement ».

- **VeDeCom** (institut pour la transition énergétique, issu du programme des investissements d'avenir) fédère la presque totalité des organismes français travaillant aux recherches précompétitives en matière de véhicule autonome. C'est, avec SystemX, l'organisme le plus important aujourd'hui en France, hors les centres de recherche de l'industrie automobile. Les véhicules connectés et autonomes constituent le second de ses trois domaines d'étude, à côté de l'électrification des véhicules et du thème « Mobilité et énergie partagées ». Quatre grands sujets de recherches structurent le domaine « Délégation de conduite et connectivité » :

  - véhicule à conduite déléguée,

  - robustesse des architectures et des systèmes,

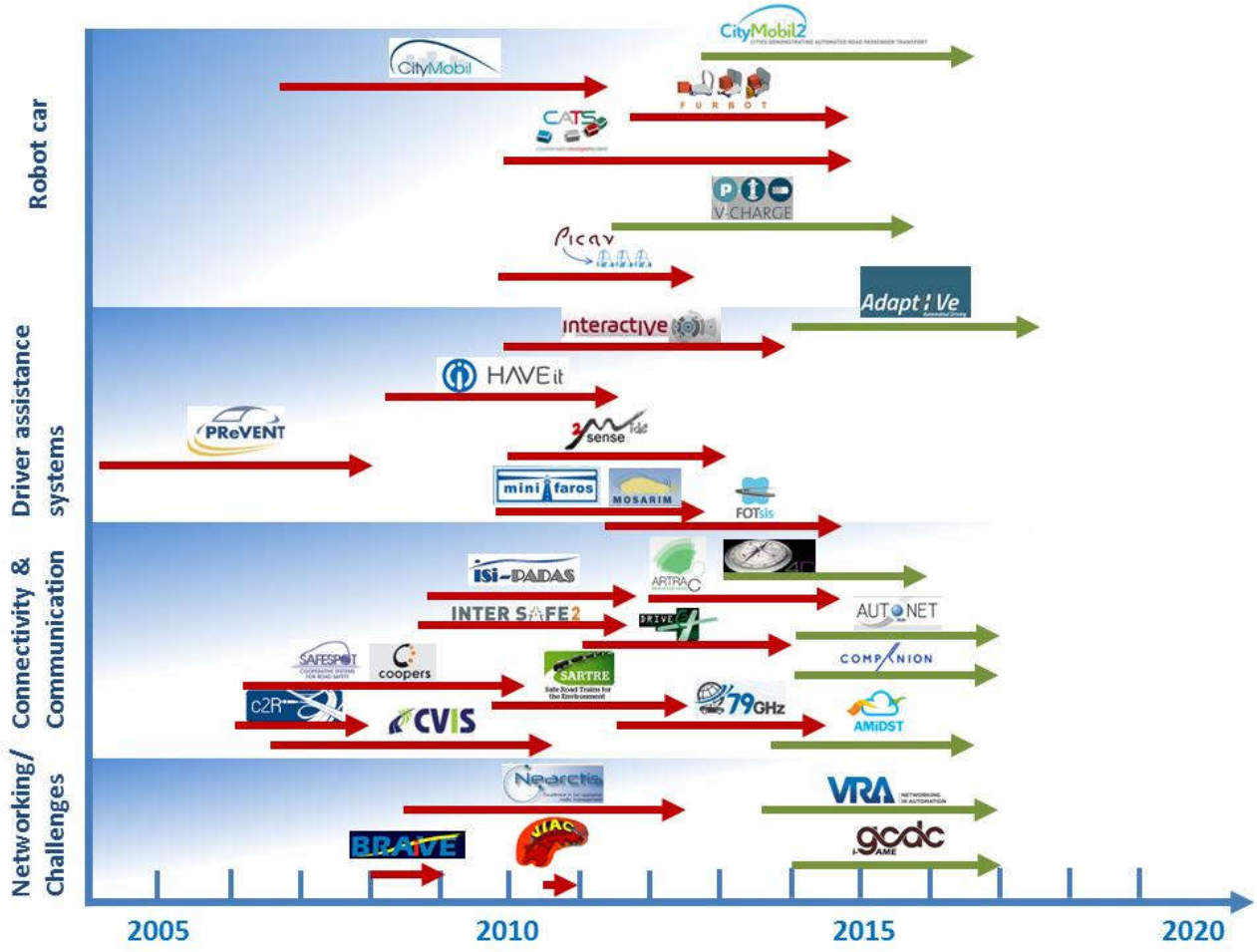
  - nouvelles communications sécurisées et sécurité coopérative,

  - évaluation des impacts sociétaux et acceptabilité de la conduite déléguée.

[25] SystemX travaille à d'autres recherches que celles relatives aux véhicules automatisés.

II. En Europe, l'Union européenne coordonne des travaux de plus en plus importants

Il y a d'assez nombreux projets de recherche et développement coordonnés par l'Union européenne. Les auteurs du rapport « European Roadmap Smart Systems for Automated Driving » (Jadranka Dokic, Beate Müller et Gereon Meyer), rapport publié à Berlin le 1er avril 2015 dans le cadre de l'European Technology Platform on Smart Systems Integration (EpoSS), ont résumé dans le graphique ci-dessous les programmes européens portant d'une manière ou d'une autre sur le véhicule autonome. Les flèches rouges ont trait aux programmes achevés, et les vertes aux programmes en cours en 2015.



Source : Commission européenne

Dans le cadre de Horizon 2020 et de son programme de travail pour 2016 et 2017 (« Smart, green and integrated transport »), la Commission européenne a publié et publiera des appels à projets comme indiqué dans le tableau ci-dessous (cf. décision de la Commission européenne C(2016) 4614 du 25 juillet 2016) :

Les appels sont les suivants :

- ART-02-2016 pour « Automation pilots for passenger cars »,
- ART-04-2016 pour « Safety and end-user acceptance aspects of roaf automation in the transition period »,
- ART-05-2016 pour « Road infrastructure to support the transition to automation and the coexistence of conventional and automated vehicles on the same network »,

- ART-06-2016 pour « Coordination of activities in support of road automation »,
- ART-01-2017 pour « ICT infrastructure to enable the transition towards road transport automation »,
- ART-03-2017 pour « Multi-Brand platooning in real trafic conditions »,
- ART-07-2017 pour « Full-scale demonstration of urban road transport automation ».

Par ailleurs, la recherche privée, chez les constructeurs et équipementiers notamment, est très importante. Le rapport précité du cabinet Strategy& relève que Bosch emploie 14 000 ingénieurs dans le domaine du software…

III. **Ailleurs qu'en Europe, l'effort est impressionnant**

1. Aux États-Unis, des programmes colossaux ont été lancés par les acteurs de l'internet (Google en tête), ainsi que par les constructeurs traditionnels.

Google a consacré des moyens importants au programme de développement de véhicules de niveau 5. À la fin octobre 2016, les véhicules en test ont accompli un trajet de 3,5 millions de kilomètres (ou 2,2 millions de miles). TESLA est également très en pointe, et des entreprises qui viennent au départ du monde du numérique, comme Nvidia, sont aussi très impliqués dans des travaux de recherche et de simulation.

2. En Asie, la Chine, la Corée du Sud et le japon soutiennent des efforts de recherche tout-à-fait significatifs. L'effort est particulièrement soutenu en Chine, avec l'appui total du gouvernement (voir le rapport de Strategy&, page 43). Les entreprises comme BAIDU visent des objectifs très ambitieux (pour BAIDU, rien moins que de dépasser les Américains), et consacrent des moyens très larges à la recherche. BAIDU a, par exemple, numérisé 6,7 millions de kilomètres de routes en Chine[26].

[26] Center for Technology innovation, at Brookings : « *moving forward : self-driving vehicles in China, Europe,Japan, Korea, and the United States* », septembre 2016

Annexe n° 11 : Les poids lourds, les navettes, les bus autonomes

Il y a bien des recherches faites sur les autocars et autobus, comme celles menées par l'entreprise Yutong en Chine ou celle de la Land Transport Authority à Singapour. En France, la RATP a aussi engagé des études, en commençant par les déplacements des autobus dans les centres bus (dépôts et ateliers dans la terminologie de la RATP). Mais la plupart se concentrent pour le moment sur les navettes de petite taille, de dix ou quinze places. Un peu partout dans le monde, des expérimentations sur routes ouvertes se déroulent ou se préparent, notamment avec les deux sociétés françaises Navya et EasyMile (Australie, France, États-Unis, Inde, Suisse, etc.), mais aussi avec d'autres sociétés : Local Motors d'Arizona, Hi-Tech Robotic Systemz d'Inde, Kamaz (avec Yandex) de Russie, etc.

Les poids lourds

Les recherches qui regardent les camions autonomes, dont les premières remontent à plusieurs décennies en Europe comme aux États-Unis, ont déjà abouti à des réalisations industrielles. Ainsi la société minière Rio Tinto a-t-elle constitué une flotte de lourds camions (pouvant transporter 320 tonnes) sans conducteur dans ses mines à ciel ouvert d'Australie-Occidentale ; elle a passé contrat avec Komatsu pour acheter au total 150 camions autonomes.

La circulation en peloton de poids lourds a été l'objet d'études avancées aux États-Unis (mise au point de la technologie Driver Assistive Truck Platooning ou DATP) comme en Europe (étude de la société néerlandaise TNO de février 2015, qui fait référence). L'IFSTTAR a lui aussi mené des études encourageantes. Dans les projets étudiés ou les expérimentations menées, les camions derrière le véhicule de tête peuvent rouler avec ou sans conducteur. Dans tous les cas, les avantages sont importants au regard de la consommation de carburant (peut-être 15 % de moins), de la sécurité routière, du confort des conducteurs en arrière, des frais de personnel si les conducteurs derrière le camion de tête sont considérés comme ne travaillant pas, ou bien sûr s'il n'y a pas de conducteurs en arrière. Il est regrettable que la France n'ait pas participé à la grande expérimentation d'avril 2016 appelée European Truck Platooning Challenge ; lorsqu'une douzaine de camions de DAF Trucks, Daimler Trucks, Iveco, MAN Truck & Bus, Scania et Volvo Group, avait alors convergé à Rotterdam en traversant cinq pays d'Europe (Allemagne, Belgique, Danemark, Pays-Bas et Suède).

Les navettes et bus

1. Deux sociétés françaises se distinguent dans le monde pour la fabrication de navettes (ou minibus) autonomes : EasyMile (implantée à Toulouse) et Navya (implantée à Paris et Lyon, employant une cinquantaine de personnes, accompagnée par le fonds d'investissement Robolution Capital).

2. Dès 2009, après une dizaine d'années de recherche et développement, dans le cadre d'IMARA (« informatique, mathématiques et automatique pour la route automatisée »), l'Institut national de recherche en informatique et en automatique (Inria) a testé dans plusieurs villes d'Europe son véhicule autonome CyCab, petite voiture à deux places. Ces essais se sont faits dans le cadre du projet européen CityMobil, dont le but était de développer des moyens intelligents de transport en commun. Le CyCab a été testé en particulier à Vantaa (Finlande) en octobre 2009. Le développement du CyCab a été poursuivi ensuite par la société Robosoft.

Deux CyCab de l'Inria
(source : Inria)

3. Le projet européen de recherches CityMobil2 regarde le développement de navettes et autobus autonomes. Fort d'un budget de 15 millions d'euros (les deux tiers provenant de l'Union européenne), exécuté sur la période 2012-2016, ce programme permettra des démonstrations et expositions de petits autobus dans dix villes d'Europe : León (Espagne, expérimentation à grande échelle), Bordeaux (France, exposition), Varsovie (Pologne, exposition), Oristano (Italie, expérimentation à petite échelle), Vantaa (Finlande, expérimentation à petite échelle avec navettes EZ10 d'EasyMile à l'été de 2015), San Sebastian (Espagne, expérimentation à petite échelle), Sophia Antipolis (France, expérimentation à petite échelle avec navettes d'EasyMile), La Rochelle (France, expérimentation à grande échelle avec navettes d'EasyMile[27]), Lausanne (Suisse, avec navettes d'EasyMile) et Trikala (Grèce, expérimentation à grande échelle avec navettes de Robosoft). Les deux constructeurs retenus à l'origine étaient français : EasyMile et Robosoft (actionnaire avec Ligier d'EasyMile). Par la suite, seule la société EasyMile continuera le développement. Sa navette, qui s'appelle EZ10, longue d'environ quatre mètres, n'a ni volant ni pédale, peut prendre douze voyageurs, est accessible aux personnes à mobilité réduite, est équipée d'un moteur électrique (batterie lithium-ion permettant une autonomie de 14 heures), se déplace normalement à la vitesse maximale de 20 ou 25 km/h, coûte aujourd'hui environ 200 000 euros, a déjà participé à cinq expérimentations.

4. Le projet City Automated Transport System (CATS) s'est inscrit dans le 7e programme-cadre de l'Union européenne. Il a duré de 2010 à 2014. Il portait sur la faisabilité et l'acceptabilité de véhicules électriques sans conducteur dans les villes d'Europe. Des essais ont eu lieu à Strasbourg (France), Ploiesti (Roumanie) et Lausanne (Suisse), avec des véhicules de la société Navya. Les conclusions ont été reprises notamment dans l'article « Pioneering driverless electric vehicles in Europe : the City Automated Transport System (CATS) » de Derek Christie, Anne Koymans, Thierry Chanard, Jean-Marc Lasgouttes et Vincent Kaufmann, publié en 2016 dans Transportation Research Procedia (volume 13, 2016).

5. Hors du programme CityMobil2, le projet WEpod a été préparé par la province de Gelderland aux Pays-Bas pour un service à l'université et centre de recherche Wageningen. Les navettes sont d'EasyMile. Le projet se poursuivra avec l'établissement d'une liaison entre cette université et la gare ferroviaire d'Ede-Wageningen.

6. Hors du programme CityMobil2, la société française Navya a vendu deux navettes appelées ARMA à la société CarPostal, entreprise publique de transport collectif en Suisse, pour une expérimentation dans les rues ouvertes (avec feux de signalisation) de la ville de Sion. La navette ARMA à moteur électrique, longue de 4,75 mètres, peut prendre quinze voyageurs et coûte environ 200 000 euros. La circulation des navettes

[27] Sans volant ni pédales, les navettes ont circulé à la vitesse maximale de 7,5 km/h sur une distance d'un kilomètre et demi. Les algorithmes de guidage avaient été préparés par Robosoft. Les navettes étaient équipées de radars à l'avant (détectant tout objet à moins de 30 mètres), d'un lidar et d'un GPS différentiel (permettant une localisation centimétrique).

sera gérée par la nouvelle société BestMile, fondée par des jeunes ingénieurs de l'École polytechnique fédérale de Lausanne (ÉPFL). Chaque navette ARMA, mue par un moteur électrique, pourra prendre neuf voyageurs et circulera à la vitesse maximale de 20 km/h ; pour agir en cas de problème, un opérateur est toujours présent à bord.

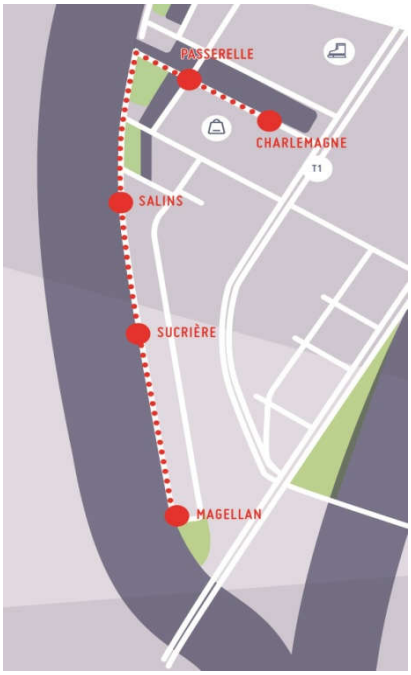
7. La société Navya a vendu six navettes ARMA à ÉDF pour sa centrale nucléaire de Civaux (Vienne). Circulant à la cadence d'un passage toutes les trois minutes sur un parcours de 2,8 kilomètres, gérées par Transdev, elles remplacent les bus à moteur thermique pour le transport des personnels sur le site de la centrale selon une cadence (souvent trop lente) d'un passage toutes les quinze minutes. En juillet 2016, les navettes devaient commencer à circuler sans opérateur à bord, les circulations étant suivies à distance par Navya dans son centre opérationnel à Lyon ; toutefois, cette phase a été repoussée. Les navettes transportent entre sept cents et mille personnes par jour. Pour la société ÉDF, les avantages sont de quatre ordres : transport écologique (sans émission de dioxyde de carbone), meilleur service de transport (cadence plus haute), vitrine technologique (véhicules tous autonomes et électriques), bonne rentabilité économique de l'investissement (absence de conducteurs).

Navette ARMA de la société Navya dans la centrale de Civaux (Vienne) en avril 2016
(source : Navya)

8. La société Navya exécute et prépare deux expérimentations importantes à Lyon et à Paris

Il s'agit d'abord, à Lyon, de circulations expérimentales (avant de devenir commerciales) entre l'arrêt de tramway T1 Hôtel de région-Montrochet et la pointe sud du quartier Confluence (près de l'immeuble de GL Events). Il y a trois arrêts intermédiaires. Les cinq stations s'appellent Charlemagne, Passerelle, Salins, Sucrière et Magellan. La distance entre les deux terminus est de 1,3 kilomètre. Accessible à tous, le transport expérimental est opéré par Navya et Keolis, avec le soutien de la métropole de Lyon, du SYTRAL et de l'ADEME. Il durera un an. Assuré par deux navettes ARMA (qui peuvent transporter jusqu'à quinze personnes, dont onze assises), commencé le 2 septembre 2016, appelé NAVLY, le service de transport, qui est gratuit, est ouvert de 7 h 30 à 19 h du lundi au vendredi, avec une fréquence comprise entre 10 et 20 minutes. La vitesse maximale est de 25 km/h ; en réalité, elle sera entre 10 et 15 km/h durant les premières semaines au moins. Conformément à l'autorisation de l'expérimentation, un agent est présent à bord pour s'assurer du bon fonctionnement de chaque navette autonome, et les voyageurs doivent s'inscrire sur un registre en montant.

Les navettes de Navya à Lyon en septembre 2016
(source : Navya-Keolis)



Les dessertes des deux navettes de Navya à Lyon
(source : Navya-Keolis)

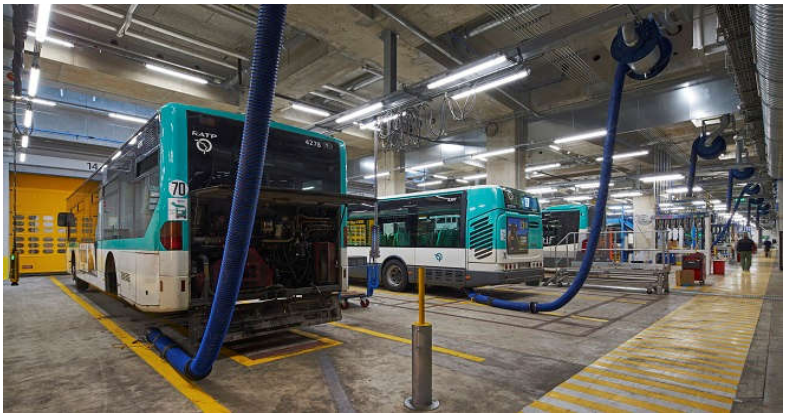
Il s'agit d'autre part de circulations expérimentales puis commerciales à Paris[28], selon un projet préparé avec la mairie de Paris, la RATP et Setec pour une liaison entre la gare de Lyon et la gare d'Austerlitz par le

[28] L'adjoint à la maire de Paris en charge de l'urbanisme, de l'architecture, des projets du Grand Paris, du développement économique et de l'attractivité, Jean-Louis Missika, s'est montré enthousiaste sur les véhicules autonomes dans l'article qu'il a fait publier (sous le titre « *Il est temps d'investir dans le transport autonome à Paris* ») dans Les Échos le 18 octobre 2016 : « *Pour réussir le pari du transport collectif autonome, nous avons besoin d'une vision partagée qui pense le court et le long terme, cette vision partagée doit être construite dans le cadre d'une conférence métropolitaine qui devrait réunir toutes les parties prenantes publiques et privées. / Cette vision doit se fixer des objectifs ambitieux, environnementaux et sociaux : la fin des émissions de particules fines avant 2025, l'objectif de neutralité carbone d'ici 2030, l'accessibilité pour tous et la complémentarité avec les mobilités actives (marche, vélos, etc.). La Ville de Paris est prête pour agir dans cette mutation, elle veut expérimenter très rapidement des liaisons en navette autonome en site ouvert, en commençant avec la RATP par une démonstration sur le pont Charles de Gaulle entre les gares de Lyon et d'Austerlitz, avant la fin de l'année. Ces navettes auront aussi un rôle à jouer pour*

pont Charles-de-Gaulle. Une « étude d'opportunité pour la mise en place d'une liaison entre les gares de Lyon et d'Austerlitz » (version 2 du 14 mars 2016) a été remise aux ministères en mars 2016. Faite avec six ou sept navettes, la liaison relierait probablement un espace de la SNCF au sud-ouest gare de Lyon au bas de l'hôtel Mercure, la rue Van Gogh, le pont Charles-de-Gaulle (avec voie particulière dans chaque sens probablement) et un espace près de la gare d'Austerlitz au débouché du pont sur l'avenue Pierre Mendès-France. La ville de Paris tient beaucoup à ce projet en raison de son caractère innovant, de l'impossibilité de trouver d'autre projet convenable pour transporter les milliers de personnes qui vont et viennent entre les deux gares chaque jour, et de son souhait de préparer des projets de véhicules autonomes dans son dossier de candidature pour les Jeux olympiques de 2024[29]. Le conseil régional d'Île-de-France soutient aussi ce projet[30].

9. Par communiqué de presse le 11 octobre 2016, la société Navya a fait savoir qu'elle procédait à une augmentation de son capital, avec une participation de 30 millions d'euros apportée par Keolis, Valeo et Group8 (société du Qatar). Ces trois actionnaires s'ajoutent aux actionnaires que sont Gravitation, Capdécisif Management et Robolution Capital (ce dernier conservant le contrôle de l'entreprise). Navya a signé un accord de distribution de ses navettes avec Group8 pour les marchés du Moyen-Orient et d'Afrique ; elle construira dans le Golfe persique une usine d'assemblage pour le marché régional.

10. Au début de 2016, la présidente de la RATP a annoncé mettre à l'étude un projet de développement de bus autonomes, d'abord pour les mouvements dans les centres de maintenance. Étudié avec le constructeur italien IVECO, le premier projet regarde le garage autonome des bus au centre bus de Lagny-Pyrénées[31] (rouvert après reconstruction en décembre 2015) dans le XXe arrondissement de Paris (projet de « garage intelligent »). Le CEA est associé à ce projet. Il est soutenu par l'Union européenne. Le but est d'équiper les bus actuels afin qu'ils descendent sans conducteur de la rue au centre bus, puis se garent.



Le nouveau centre bus de Lagny-Pyrénées (Paris) de la RATP en décembre 2015
(source : RATP)

---

développer le transport à la demande dans des zones mal desservies comme les bois parisiens, et surtout dans le périurbain. La grande couronne francilienne pourra ainsi en bénéficier pour faciliter l'accès à la demande aux gares du réseau Transilien. Des expérimentations pourraient aussi être menées sur des voies rapides réservées aux navettes autonomes. Une priorité devrait être donnée à la liaison entre Saclay et Paris pour permettre aux milliers d'étudiants qui rejoindront dès 2019 ce nouveau pôle scientifique et universitaire d'avoir une solution de transport efficace et accessible. Le temps presse, il est indispensable que tous les acteurs prennent conscience de cette révolution des mobilités, de ce qu'elle exige d'eux et des actes audacieux qu'il faut poser pour la mener à bien. ».

[29] Tokyo veut présenter des véhicules autonomes à l'occasion des JO de 2020 sur son territoire.

[30] *« Il est indispensable de se préparer à l'arrivée des futurs véhicules guidés autonomes [*sans conducteur*] annoncés entre 2020 et 2022, ou encore des futurs « trains de bus » ou RER autoroutiers. Nous sommes en train d'identifier les tronçons sur lesquels les expérimentations seront menées. Par exemple, nous étudions la création d'une ligne de navettes autonomes entre les gares de Lyon et d'Austerlitz, à Paris. »* (Valérie Pécresse, Le Journal du Dimanche, *« Mon plan anti-bouchons »*, 18 septembre 2016).

[31] Au 18 de la rue des Pyrénées.

11. Dans la commune d'Archamps (Haute-Savoie), des études sont actuellement entreprises, avec l'aide du Cerema (centre-est), pour des transports intelligents et autonomes en ville (transport du dernier kilomètre) : projet NodeTech, qui regarde plus particulièrement le parc d'activités Archamps Technopole (50 hectares, 1 800 employés).

12. Dans le nord de la Californie (États-Unis), la Contra Costa Transportation Authority (CCTA) prépare des expérimentations de navettes d'EasyMile[32] sur le site de GoMentum Station[33][34] (ancienne installation de la marine américaine, qui s'étend sur 5 100 acres ou 2 000 hectares et sur 19,6 milles de route) à Concord, puis sur le site de Bishop Ranch (grande zone d'activités industrielles et commerciales de San Francisc Bay Area, de 585 acres ou 237 hectares) à San Ramon, puis sur rues ouvertes près de Bishop Ranch. Dès 2016, deux premières navettes d'EasyMile seront testées à Bishop Ranch.

Toutes les expérimentations conduites par la CCTA participeront d'un ambitieux plan de recherche et développement (« Shared Autonomous Vehicle Testing Plan ») avec de nombreuses parties prenantes : industriels, entreprises de télécommunication, instituts de recherche, etc. Elles conduiront in fine la CCTA à définir, et mettre en œuvre dès 2020, un nouveau plan de transport du comté de Californie. Le système principal de transport collectif (Mass Transit) y sera complété par un réseau fin et complémentaire de quelque 150 petites navettes permettant les trajets terminaux des voyageurs entre domiciles et gares.

Les expérimentations de ces navettes sans conducteur ont été autorisées par une loi signée par le gouverneur de Californie le 29 septembre 2016. Cette loi était nécessaire car il est prévu que lesdites navettes traversent des routes ouvertes à la circulation.

13. La jeune entreprise américaine Local Motors (d'Arizona aux États-Unis) a développé avec la société IBM une navette autonome de douze places (assez semblable à celles de Navya), appelée Olli. Ladite navette accomplit actuellement des essais dans la capitale des États-Unis (Washington). Les navettes sont assemblées dans l'usine de National Harbor à une quinzaine de kilomètres de Washington.

Navette Olli de Local Motors dans l'atelier de National Harbor près de Washington (DC, États-Unis) en juin 2016

(source : Local Motors)

14. Mercedes-Benz travaille aussi au développement de bus autonomes. Avec sa plate-forme appelée CityPilot, dans le cadre d'un projet technologique appelé Mercedes-Benz Future Bus, la société a testé en 2016 des bus semi-autonomes (reconnaissance des feux de signalisation grâce à une connexion avec le réseau de télécommunication de la ville, des piétons, freinage automatique, etc.) à la vitesse moyenne de 43 km/h (vitesse maximale de 70 km/h) entre l'aéroport d'Amsterdam-Schiphol et la ville de Haarlem (Bus

[32] Accord conclu entre la CCTA et EasyMile en octobre 2015.
[33] *Concord Naval Weapons Station (CNWS) Test Facility.*
[34] Sur ce site, la société Honda a déjà expérimenté des voitures autonomes.

Rapid Transit de 20 kilomètres de long). Les bus sont équipés de caméras et de radars. Les bus font monter et descendre les voyageurs aux arrêts de façon autonome. Les bus restent autonomes dans les tunnels. L'intérieur des bus a été conçu pour un grand confort. Le 18 juillet 2016, la société a déclaré vouloir investir 200 millions d'euros dans le développement de ses bus autonomes.

15. En juillet 2016, la société américaine Tesla a annoncé se préparer à développer, en plus des voitures autonomes, des camions, des bus et des voitures en autopartage, tous autonomes.

16. En Chine, plusieurs expérimentations ont déjà été faites. Yutong est un constructeur d'autobus qui a expérimenté en 2015 des bus autonomes dans ses emprises de Zhengzhou (province du Henan). D'autres expérimentations vont se développer à Wuhu (ville de près de quatre millions d'habitants dans la province de l'Anhui), dans le cadre d'une coopération conclue en 2016 entre la ville et la société Baidu portant sur les bus, les navettes et les taxis robots.

Bus autonome de Yutong en expérimentation en Chine (province du Henan) en 2015
(source : Yutong)

17. En Inde, la société Hi-Tech Robotic Systemz fondée en 2004 a développé une navette de quatorze sièges à Gurgaon (au sud de New Delhi), appelée Novus Drive. C'est la première navette automatisée construite en Inde. Elle est équipée de caméras stéréo, mais aussi d'un lidar (modèle HDL-32E) vendu par la société Velodyne LIDAR Inc. de Californie.

La navette Novus Drive
(source : The Hans of India le 7 février 2016)

18. En Finlande, à la suite de l'expérimentation de Vantaa (Finlande) à l'été de 2015 (dans le cadre du projet européen CityMobil2), le projet SOHJIA, sous la coordination de l'université des sciences appliquées d'Helsinki (dite Metropolia), a été lancé le 16 août 2016 en présence du maire de la capitale (Pekka Sauri). C'est la circulation expérimentale de navettes électriques EZ10 d'EasyMile (à neuf passagers) durant un an sur route ouverte à Helsinki (août et septembre 2016), puis à Espoo (en septembre et octobre 2016), puis à Tampere (jusqu'à l'hiver).

Navettes EZ10 d'EasyMile en 2016 à Helsinki (Finlande) dans la cadre du projet SOHJIA
(source : EasyMile)

L'expérimentation cessera durant l'hiver 2016-2017 quand la neige sera abondante ; elle reprendra au printemps de 2017.

19. En Australie, une expérimentation avec des navettes de Navya a commencé le 31 août 2016 à Perth (précisément à South Perth Esplanade) sur route ouverte avec des passagers, sous l'appellation RAC Intellibus. La navette est équipée notamment de six lidars, comme dans le quartier Confluence de Lyon. Son itinéraire court sur 2,7 kilomètres le long de la Swan.

La navette de Perth en Australie achetée en 2016 par la Royal Automobile Club of Western Australia (RAC WA) *(source : Royal Automobile Club of Western Australia)*

Le parcours de la navette expérimentale de Navya près de Perth (Australie-Occidentale)
(source : Royal Automobile Club of Western Australia)

20. La première démonstration de la RATP a eu lieu sur la voie Georges-Pompidou à Paris (près du Pont-Neuf) avec une navette d'EasyMile l'après-midi du 24 et du 25 septembre 2016, sur une courte distance (130 mètres).

Une navette d'Easymile sur les berges de la Seine
(source : Easymile).

Selon le communiqué du 26 septembre 2016 de la RATP :

« *Pour la RATP, il s'agit du coup d'envoi d'une série d'expérimentations. D'ici à la fin 2016, une autre démonstration de véhicules autonomes verra le jour entre la Gare de Lyon et la Gare d'Austerlitz sur le Pont Charles de Gaulle, en partenariat avec la Ville de Paris. La RATP travaille également à une expérimentation de desserte interne du site du CEA Saclay. Les premiers tests sont prévus début 2017. Le projet, piloté par la RATP, associe le CEA List (laboratoire de recherche du CEA), Bureau Veritas, Sherpa Engineering (société d'ingénierie) et BMCP (bureau d'études et de conseil spécialisé). Le projet, labellisé par les Pôles de compétitivité LUTB « Transport et Mobility Systems » et Systematic Paris-Région est financé dans le cadre du 22ème FUI (Fonds Unique Interministériel).* ».

La RATP a acquis en 2016 deux navettes EZ10 de la société toulousaine EasyMile qui lui permettront de mener des démonstrations et des expérimentations.

Les deux navettes achetées par la RATP ont été réceptionnées par la RATP en novembre 2016. Elles seront d'abord utilisées en démonstration au premier trimestre de 2017 sur les berges de la Seine et sur le pont Charles-de Gaulle (près de la Maison de la RATP à Paris), là où, plus tard, la RATP veut expérimenter des navettes entre la gare de Lyon et la gare d'Austerlitz.

21. La RATP étudie un projet de transport par navette autonome dans les emprises du Commissariat à l'énergie atomique et aux énergies alternatives (CEA) à Saclay (Essonne). Sont associés à la RATP : l'Institut List (du CEA Tech), le Bureau Veritas, Sherpa Engineering (société d'ingénierie) et BMCP (bureau d'études et de conseil). Le projet commencera en janvier 2017, et durera trois ans. Il recevra un financement du Fonds unique interministériel (FUI).

22. En Nouvelle-Zélande, la société française Navya a vendu une navette autonome ARMA à la société australienne HMI Technologies. La navette sera acheminée en Nouvelle-Zélande avant la fin de 2016. Elle sera expérimentée dès 2017 sur des routes privées puis ouvertes à l'Aéroport international de Christchurch. L'Université de Canterbury à Christchurch travaillera aux essais. Les expérimentations seront faites sous le contrôle de la New Zeland Transport Agency et du Ministry of Transport.

L'aéroport international de Wellington en Nouvelle-Zélande, de son côté, étudie la possibilité de recourir à des navettes autonomes EZ10 d'EasyMile pour desservir ses emprises.

23. Une expérimentation d'une navette EZ10 d'EasyMile par la TCAR, société exploitant le réseau de transport en commun de Rouen (en Seine-Maritime en France), a été accomplie du 31 octobre au 23 décembre 2016 sur les voies des quais en rive droite de la Seine, entre le pont Jeanne-d'Arc et le pont Flaubert. Ces voies sur berge sont possédées par le port autonome de Rouen, mais sont exploitées par la ville de Rouen par convention de superposition de gestion avec le port. La TCAR est contrôlée par le groupe Transdev, l'autorité organisatrice des transports étant la Métropole de Rouen Normandie. L'objectif est, plus tard, d'entreprendre sur les mêmes voies de quai une exploitation commerciale de fin de ligne, là où le moyen du bus n'est plus pertinent.

Le public était autorisé à utiliser gratuitement la navette expérimentale de 12 h à 22 h chaque jour. Les voies étaient fermées à la circulation automobile, mais ouvertes aux modes doux.

24. En octobre 2016, la Land Transport Authority (LTA) de Singapour a annoncé vouloir bientôt commencer, avec l'Energy Research Institute de la Nanyang Technological University (NTU), une expérimentation d'autobus autonomes entre l'université NTU et la station voisine dite Pioneer MRT. Elle se fera avec deux autobus à moteur hybride. L'accord à cette fin entre la LTA et la NTU a été signé le 19 octobre 2016, à l'occasion de la cérémonie d'ouverture du Singapore International Transport Congress and Exhibition (SITCE).

Signature, en présence du ministre d'État pour le transport (Ng Chee Meng, debout au centre), de l'accord sur l'expérimentation de bus autonomes entre la LTA et la NTU le 19 octobre 2016 à Singapour
(source : LTA)

Schéma de principe sur l'équipement des deux autobus qui participeront à l'expérimentation de Singapour (selon la LTA et la NTU) *(source : LTA)*

25. La société russe Yandex, géant de l'économie numérique en Russie, a annoncé en août 2016 s'être associé au constructeur russe de camions Kamaz, dont sont actionnaires l'État russe, le constructeur allemand Daimler et l'institut NAMI (centre russe de recherches automobiles), pour développer des navettes électriques autonomes. Les expérimentations commenceraient en 2017.

Le prototype de navette (pour 12 passagers) de Kamaz, NAMI et Yandex, présenté à la fin d'août et au début de septembre 2016 au Moscow International Automobile Salon (MIAS) *(source : MIAS)*

Annexe n° 12 : L'impact économique et social des véhicules autonomes. L'acceptabilité sociale

I. L'impact économique et social des véhicules autonomes

1. D'après les nombreux travaux qui leur sont consacrés, les changements sur le mode de vie pourraient être très importants

De nombreux travaux font apparaître des modifications importantes qui pourraient se manifester dans les modes de vie. Certains anticipent la réduction rapide des trajets « traditionnels », et envisagent même leur disparition à terme, ce qui signifierait la fin du permis de conduire, la disparition des auto-écoles, et la perte de compétence des « conducteurs » devenus des passagers passifs. Les plus enthousiastes décrivent un futur où des enfants pourront se rendre seuls à l'école dans des navettes autonomes, et où les personnes handicapées (aveugles par exemple) pourront bénéficier d'une mobilité inédite[35].

Certains estiment que l'automatisation permettra de distendre le lien de propriété entre les utilisateurs et les véhicules, ceux-ci étant majoritairement gérés dans des « flottes » par des opérateurs de service, et étant appelés à la demande[36]. Une étude réalisée par l'Université du Michigan en 2016[37] estime que les ventes d'automobiles pourraient reculer, les ménages pouvant se contenter d'un seul véhicule, automatisé et fonctionnant sur une plage temporelle plus large.

Pareillement, des urbanistes annoncent un bouleversement de l'organisation urbaine, se traduisant par une modification des ouvrages de la voirie, et un nouveau partage de l'espace collectif, allant parfois jusqu'à l'utopie[38].

2. Les conséquences sur l'économie et l'emploi sont plus difficiles à estimer

a. Un consensus semble se dégager autour d'un transfert de la valeur vers les plateformes et les services

Selon une étude publiée en septembre 2016 par l'institut VeDeCom et la Société des ingénieurs et scientifiques de France (IESF), intitulée : « Véhicule autonome, accompagner la transition », la chaîne de valeur sera progressivement tirée par les plateformes et les services d'usage de véhicules[39].

Selon les auteurs de l'étude, « la compétition engagée au niveau mondial porte à la fois sur la maîtrise des systèmes logiciels, sur l'organisation des territoires et sur l'adaptation des usages de mobilité ».

La valeur devrait ainsi se déplacer vers les fournisseurs et les gestionnaires de logiciels, et vers les opérateurs de services liés à la mobilité. De nombreux travaux convergent en ce sens[40].

---

[35] En ce sens, parmi d'autres, un guide produit par le cabinet américain WSP à destination des décideurs publics, intitulé « *Driving towards driverless* », 2016, en particulier page 3.

[36] On pourra consulter par exemple un travail universitaire, effectué en 2014 et présenté dans un colloque à Washington : « *The travel and environmental implications of shared autonomous vehicles, using agent-based model scenarios* », par Daniel FAGNANT et Kara KOCKELMAN, publié dans *Transportation Research,* Part C, Vol. 40 (2014).

[37] Cité par David CURRY, dans « *Car saale boom to go bust with self-driving cars ?* », site Reasdwrite, 5 avril 2016.

[38] En ce sens, une étude du cabinet WSP, « M*aking better places* », 2016.

[39] Cahier IESF, numéro 23.

[40] Voir notamment : International Transport Forum, « A*utomated and autonomous driving* », OCDE, 2015, page 18 ; Etude publiée par SWISS RE et HERE en 2016 sous le titre « *The future of motor insurance* », page 21 ; Etude du cabinet KPMG, publiée en octobre 2015, sous le titre « *Marketplace of change* », notamment page 21. Voir aussi *Les Echos,* article mis en ligne le 18 août 2016 : « *la course à la voiture autonome s'accélère entre les constructeurs* ».

b. Le secteur de l'assurance sera fortement touché

Les primes d'assurance vont nécessairement évoluer parallèlement aux progrès de la technique et seront plus individualisées (voir le Livre Blanc publié par AON Risk Solutions en avril 2015 sous le titre « Quand la voiture devient autonome »).

Le dumping massif que ces mouvements sont susceptibles d'entraîner suscitent l'inquiétude d'observateurs comme Warren BUFFET : « Notre activité assurance ne sera pas à la fête quand les voitures autonomes vont arriver, même si ce moment n'est pas pour tout de suite » (in Le Monde.fr, 14 août 2016, article de Noël GHANIME, président de Mondial Assistance France).

Il est également tenu pour probable que des transferts de responsabilité pourront s'opérer dans de nombreux pays en direction des constructeurs, ce qui va modifier en profondeur le marché de l'assurance (même source). Les prévisions sur la date à laquelle ces modifications surviendront sont variables selon les auteurs. Le cabinet KPMG, par exemple, estime les transformations interviendront assez rapidement (« Marketplace of change : automobile insurance in the era of autonomous vehicles », octobre 2015, page 20). De manière provocatrice, le journaliste David CURRY a intitulé un article mis en ligne sur le site Readwrite le 5 mai 2016 : « Could autonomous cars destroy the auto insurance industry? » (« Les véhicules autonomes peuvent-ils détruire l'industrie de l'assurance ? »). L'auteur estime que le doute est permis, car l'utilisation plus intensive des véhicules pourrait produire une plus grande usure des matériels, et donc avoir un impact significatif sur les besoins en nouvelles réparations.

Une étude portant sur le marché européen de l'assurance, réalisée par le cabinet DELOITTE (« Étude européenne sur le marché de l'assurance automobile connectée », novembre 2016) donne une idée des changements qui se préparent : 28 % des clients interrogés dans onze pays disent accepter de partager leurs données avec leur assureur, ce que le cabinet interprète comme l'indice qu'ils envisagent éventuellement d'aller vers un assureur qui leur propose ce service. DELOITTE estime que, dans un marché où les clients seront de plus en plus démarchés, la connectivité (qui est liée à la montée en charge des automatismes) constitue « une opportunité de se différencier sur un marché toujours davantage fluide et standardisé ».

c. Les autres secteurs économiques n'ont pour le moment qu'une idée assez imprécise des transformations à venir

Il existe très peu de travaux prospectifs portant sur des activités comme les transports collectifs, le transport de marchandises, l'agriculture, les taxis (ou assimilés). Les responsables interrogés par la Mission CGEDD-IGA sont très prudents dans leurs anticipations, et estiment en général que les mouvements seront graduels et qu'un partage durable du parc entre véhicules classiques et véhicules automatisés est une probabilité.

La même incertitude prévaut pour les conséquences à attendre sur l'emploi. En l'absence d'étude sérieuse portant sur ces aspects, la plus grande prudence s'impose. La Mission CGEDD-IGA n'a pas eu la possibilité d'étudier en détail ces questions.

II. L'acceptabilité sociale

Les études qui ont été réalisées dans plusieurs régions du monde indiquent que le public exprime un fort intérêt pour les véhicules automatisés. Les plus enthousiastes sont dans les pays industriellement les plus jeunes, comme la Chine. Toutefois, beaucoup, dans les pays les plus riches surtout (États-Unis, France, Allemagne, etc.), attendent de voir ce que seront vraiment les avantages de ces véhicules, surtout au regard de la sécurité routière.

1. **En France, l'intérêt des consommateurs est soutenu, mais il reste encore pour le véhicule autonome à convaincre**

a. Dans le cadre de VeDeCoM, de l'IFSTTAR, et de l'Université de Paris VIII, William Payre, Julien Cestac et Patricia Delhomme ont publié en 2015 un rapport intitulé : « Intention to use a fully automated car: attitudes and a priori acceptability ». L'étude a été faite sur la base d'entretiens individuels (5 personnes), d'une étude pilote (45 personnes) et d'un questionnaire en ligne (421 personnes). Les entretiens individuels ont montré un intérêt certain pour la conduite autonome, un sentiment de responsabilité et une intention d'usage et d'achat. L'étude pilote a montré une acceptabilité dans certains contextes (conduite ennuyeuse, par exemple) et un intérêt certain en cas de facultés dégradées (fatigue).

L'étude en ligne a montré que 52 % des personnes étaient plutôt favorables à l'utilisation d'un véhicule autonome et que 78 % seraient prêtes à en acheter un. De plus, 75 % seraient intéressées par la conduite autonome si leurs facultés étaient diminuées. Enfin, les personnes interrogées seraient prêtes à dépenser en moyenne 1 899 euros de plus pour avoir un véhicule autonome ; le surcroît de la dépense d'achat par rapport à un véhicule manuel varie de 0 (pour 22 % des gens) à 10 000 euros.

Les auteurs ont conclu en trois affirmations (cf. présentation au séminaire du GERI USACT le 26 juin 2015) :

- « Les attitudes sont globalement positives à l'égard de la conduite autonome et les participants sont majoritairement favorables à ce type de véhicule. Toutefois ils émettent des réserves en ce qui concerne la sécurité. » ;
- « La conduite autonome serait utilisée principalement pour des trajets monotones (autoroutes, embouteillages, créneaux), et moins en ville. » ;
- « Il existe un risque d'usage détourné [par exemple conduite en état d'ivresse] qui devrait être pris en compte par les constructeurs (monitorage du conducteur ?). ».

b. Le cabinet Deloitte a rendu en septembre 2016 les résultats d'une enquête sur l'intérêt des Français pour le véhicule autonome

- « 77 % des Français préfèrent les véhicules bien équipés, facilitant la conduite aux véhicules totalement autonomes » ;
- « Les Français expriment des besoins d'automatisation et de technologies moindres : 61 % recherchent un niveau d'automatisation standard, 52 % un niveau avancé, 36 % une conduite autonome limitée à certaines conditions de trafic et, enfin, 30 % une conduite autonome totale pour réaliser des trajets complets ».

Le cabinet conclut : « Si les Français apparaissent avoir une assez bonne connaissance des voitures autonomes, 72 % des consommateurs français interrogés pensent qu'elles ne seront pas une réalité commerciale en France dans les vingt prochaines années. Ils sont 44 % à penser que ce sont les acteurs non traditionnels qui permettront l'avènement de la voiture autonome ».

c. Une étude faite pour VeDeCoM en 2016 a montré une certaine perplexité des Français envers la voiture autonome

Réalisée par l'Observatoire des mobilités émergentes (ObSoCo_Chronos) pour le compte de VeDeCom, cette étude a été présentée le 22 septembre 2016 à la Mission CGEDD-IGA. Elle fait apparaître, à partir des réponses de 4 000 personnes (recueillies avant que ne soit connu l'accident de la TESLA dévoilé en juin 2016) que :

- 60% des personnes interrogées sont « favorables au véhicule autonome » et 40 % s'en inquiètent ;
- À la question : « Seriez-vous prêts à utiliser un tel véhicule ? », 51 % répondent oui et 49 % non.
- Parmi les thèmes cités, l'avantage principal tient à la réduction des accidents, tandis que la préoccupation première est celle du dysfonctionnement et du piratage.

2. Ailleurs dans le monde, les attentes sont variées

a. Aux États-Unis, de manière apparemment paradoxale, le niveau de scepticisme est relativement élevé

Une étude a été publiée en septembre 2016 par le cabinet de consultants spécialisé Kelley Blue Book (KBB) sur l'acceptabilité des véhicules autonomes par les Américains. KBB a mis en ligne le 28 septembre 2016 sur son site une restitution de cette étude, sous le titre : « KBB study finds American drivers still prefer a hands-on approach » (« une étude de KBB démontre que les conducteurs Américains préfèrent la conduite manuelle »). Ce travail fait apparaître une réticence des automobilistes aux États-Unis pour se lancer dans la conduite en mode autonome.

Le scepticisme des personnes qui répondent (hormis ceux dont l'âge est compris entre 12 et 15 ans) envers les véhicules dotés d'une forte autonomie est élevé : 64 % disent qu'ils préfèrent avoir en permanence le contrôle de leur véhicule et 80 % n'acceptent le mode autonome que s'ils peuvent l'actionner volontairement à leur gré. L'étude portait sur un échantillon de 2 264 personnes entre 12 et 64 ans.

b. Pour le monde entier, les chiffrent varient fortement selon les régions

L'Observatoire Cetelem a publié en 2016 une comparaison internationale sous le titre « Cetelem 2016 – Voiture autonome : les automobilistes prêts à lâcher le volant pour la Silicon Valley ».

Cette étude montre des niveaux d'acceptation très variables selon les pays abordés.

- De manière générale, la voiture connectée semble être plébiscitée :

« Pour 73 % des personnes interrogées, la voiture connectée est tout simplement la voiture idéale, synonyme de progrès en matière de confort (83 %), de gain de temps (81 %) et de sécurité (77 %). Pour autant, 78 % jugent qu'elle rime avec cherté. Ce sont les Mexicains et les Brésiliens qui se montrent les plus enthousiastes. On pointe là une dichotomie structurante pour l'ensemble de l'étude avec, d'une part les pays dits émergents totalement favorables à la voiture autonome et tout ce qu'elle apporte, et d'autre part les pays automobiles natifs plus méfiants quant à son développement ».

- Et la future voiture autonome est attendue :

« De la voiture connectée à la voiture autonome, il y a bien plus qu'une différence sémantique. Une véritable (r)évolution qui suscite de nombreuses interrogations, la première étant la probabilité de sa construction. Pour 3 personnes sur 4, pas de doute, la voiture autonome sera une réalité. Une réalité très proche puisque 81 % espèrent son arrivée avant 10 ans et 52 % avant 5 ans. Une fois encore, les pays « traditionnels » se montrent les plus prudents, 70 % des Allemands ne voyant pas de voitures autonomes sur les routes avant 2020 alors que 74 % des Mexicains l'escomptent avant 5 ans ».

« Mieux encore, plus de 1 automobiliste sur 2 a envie de se retrouver à l'intérieur, à défaut d'y être vraiment au volant. C'est en Chine où l'enthousiasme est le plus manifeste (91 %) alors que les Américains et les Britanniques sont les plus attachés à leur automobile's way of life traditionnel. Mais cette nouvelle voiture autonome n'est pas seulement imaginée vraiment comme une… voiture. 48 % des personnes

interrogées la voient comme un espace de divertissement, les Chinois étant une fois encore les plus excités par cette idée, suivis par les Turcs et les Portugais (respectivement 70 %, 57 % et 56 %). On la projette aussi comme un lieu de repos et détente et même, pour le quart des automobilistes, comme un lieu de travail ».

- L'attente est d'autant plus forte que les automobilistes se sont déjà accoutumés aux nouveaux outils :

« Qui dit voiture connectée, dit aide à la navigation totalement banalisée. 86 % des personnes interrogées se servent déjà de cette aide pour préparer ou guider leurs déplacements. C'est particulièrement le cas en Chine ou au Brésil, contrairement au Japon où elle est relativement peu employée. Notons aussi qu'en matière de géolocalisation, le smartphone est plébiscité par 69 % des automobilistes mondiaux. L'emploi de cet outil et des autres systèmes de navigation aura d'abord servi à optimiser le temps de parcours (80 %) et à réduire le nombre de kilomètres parcourus (70 %) ».

« La géolocalisation avec tout ce qu'elle transporte (publicité contextualisée mais aussi offre de services personnalisés divers et variés sur le trajet) reçoit un assentiment majoritaire (57 %). Alors que 87 % des Chinois sont demandeurs d'offres commerciales personnalisées, 35 % des Français ou des Américains se montrent très réservés ».

- Pour autant, les conducteurs veulent être rassurés :

« (…) la voiture connectée suscite des craintes, notamment en termes de contrôle du véhicule, pour 37 % des personnes interrogées. C'est surtout vrai aux États-Unis (54 %) ou encore en France (46 %). De fait, priorité est accordée à une sécurité tous azimuts. 89 % sont pour les systèmes de sécurité en cas de vol, 86 % particulièrement favorables aux systèmes de détection piétons/obstacles. Des solutions pour lesquelles les automobilistes seraient prêts à payer plus cher leur véhicule.

« De la voiture connectée à la voiture autonome, il y a bien plus qu'une différence sémantique. Une véritable (r)évolution qui suscite de nombreuses interrogations, la première étant la probabilité de sa construction. Pour 3 personnes sur 4, pas de doute, la voiture autonome sera une réalité. Une réalité très proche puisque 81 % espèrent son arrivée avant 10 ans et 52 % avant 5 ans. Une fois encore, les pays « traditionnels » se montrent les plus prudents, 70 % des Allemands ne voyant pas de voitures autonomes sur les routes avant 2020 alors que 74 % des Mexicains l'escomptent avant 5 ans.

« Mais la méfiance est cependant de mise, 28 % déclarant souhaiter conserver un œil sur la route, au cas où… Des suspicieux que l'on retrouve surtout aux États-Unis, en Italie ou en Pologne ».

L'étude fait aussi apparaître que ce sont les constructeurs traditionnels dans lesquels les automobilistes placent la confiance la plus forte, même si les nouveaux entrants du monde de l'internet intéressent les habitants de certains pays émergents.

3. **Les aspects humains sont jugés déterminants**

- D'abord, le prix sera une variable qui pèsera lourd :

L'attractivité envers les nouvelles technologies est avérée. Mais pas à n'importe quel prix : 191 euros, ce serait le budget « technologie » que les Français seraient prêts à dépenser pour l'achat d'un nouveau véhicule automatisé, contre 551 euros en 2014.

- Ensuite, les comportements routiers seront probablement déterminants :

Les véhicules autonomes circuleront d'autant mieux qu'il y aura moins de véhicules à conduite manuelle qui transgressent les règles du code de la route. Ainsi le président-directeur général de l'Alliance Renault-Nissan (Carlos Ghosn) a-t-il expliqué le 6 octobre 2016 en France :

« *Il faut […] que les règles de conduite soient respectées, parce que les voitures autonomes respectent les règles. […] Et les voitures autonomes vont s'arrêter aux feux rouges, quoi qu'il arrive. Ce sont des ordinateurs. Si elles sont les seules voitures à s'arrêter, vous pouvez imaginer le nombre d'accidents qu'il va y avoir au Brésil ! […] [En Inde, à Bombay notamment,] les gens ne respectent pas toujours le code de la route. Certains prennent les ronds-points à l'envers. On ne peut pas placer de voitures autonomes sur la route dans de telles conditions.* » (cité par Charles Gauthier, Le Figaro.fr, 2 octobre 2016).

Enfin, la psychologie des conducteurs sera un élément à prendre en compte dans les modèles d'acceptabilité : selon le CEREMA (Mme Stéphanie BORDEL, laboratoire de Saint-Brieuc, spécialiste des ADAS, qui a travaillé dans le cadre des projets Archos et SCOOP@F), les nouveaux outils rencontrent un frein dans l'image que s'en font les gens. « Le bon conducteur est celui qui garde la main ». Selon le CEREMA, les conducteurs -particulièrement français- préfèrent avoir un renfort d'informations qu'une assistance à la conduite. Le conducteur n'accepte de lâcher une partie de son pouvoir de conduire que s'il reçoit une bonne contrepartie. Les régulateurs de vitesse n'ont finalement été acceptés que parce qu'ils permettent de maîtriser sa vitesse face au risque d'être pris par un radar.

Les obstacles à l'acceptabilité de la voiture autonome sont au moins au nombre de quatre :

- La supervision est un acte pénible, moins gratifiant et moins agréable que la conduite[41].

- L'incertitude juridique est un gros obstacle. Qui est responsable ? La perception qu'a le citoyen de ce que sont la responsabilité et la culpabilité s'oppose souvent à ce qui est défini par la loi. Ainsi des personnes voudront-elles utiliser le système de conduite autonome pour se débarrasser de leur responsabilité (« c'est la voiture qui conduit »), alors que peut-être, ce seront toujours elles qui seront jugées responsables de la conduite, et donc d'un acte qu'elles n'auront pas, à leur sens, commis.

- L'optimisme comparatif est aussi un sérieux obstacle. C'est une caractéristique de l'esprit humain qu'on peut définir ainsi : chacun pense qu'il aurait fait mieux qu'un autre dans la même situation. Même si la machine accomplit une tâche plutôt répétitive mieux que l'homme en moyenne, cela ne suffit pas à convaincre le conducteur qu'il y gagne en abandonnant la conduite. Il faut que le gain de sécurité soit vraiment fort pour que l'homme consente à laisser la machine conduire à sa place. Le conducteur alcoolisé qui se sait diminué laisserait plus volontiers le volant à la machine… mais ferait un mauvais superviseur !

- Le temps de reprise du véhicule inquiète. Une étude de l'Université de Leeds en Angleterre indique qu'il faut au moins dix secondes, et que ce temps peut monter jusqu'à une minute.

Toujours pour le CEREMA, pendant la période intermédiaire (véhicule de niveau 2 ou 3), un autre trait de l'être humain qui fait problème est l'homéostasie du risque. Lorsque des moyens permettent une diminution du risque (par exemple les airsbags), certains conducteurs prennent plus de risques pour compenser la baisse, et rester au même niveau de risques (on ne boucle plus sa ceinture de sécurité, etc.). Or, quelques accidents à fort retentissement médiatique retarderaient l'arrivée du véhicule autonome.

En revanche, le transfert d'information vers les constructeurs ne poserait pas de problème au public, l'habitude de transférer de l'information personnelle par le smartphone ou l'ordinateur ayant déjà été prise.

[41] cf. thèse de William Payre sur l'acceptabilité du véhicule autonome

Le CEREMA ajoute que, sur l'aspect économique, les constructeurs ont du mal à vendre des systèmes en supplément, et, sur le sujet de l'éthique, que les personnes n'ont pas le même point de vue en tant que victime potentielle ou en tant que responsable potentiel.

III. **Éthique des véhicules autonomes ou le problème du choix**

La question de l'éthique des véhicules autonomes revient régulièrement parmi les sujets qui font couler beaucoup d'encre dans les livres et les gazettes. Mêlant des aspects techniques, philosophiques à des paradoxes de science-fiction (cf. les trois lois de la robotique de l'écrivain Isaac Asimov[42]), elle amène avec elle une aura de soufre et de mystère qui fait frémir le lecteur, enflamme les débatteurs et fait hésiter le législateur.

Le point de départ le plus prisé de ces réflexions est le paradoxe du tramway qu'on peut énoncer ainsi : un tramway privé de freins se dirige de façon inéluctable vers cinq hommes qu'il va tuer. La seule action possible est d'actionner un aiguillage qui enverrait le tramway écraser un homme seul qui est attaché sur cette voie. Autrement dit faut-il s'abstenir d'agir et laisser mourir cinq personnes ou bien agir et tuer volontairement une personne pour en sauver cinq autres ?

Appliqué au véhicule autonome le paradoxe du tramway donne naissance à bon nombre de questions : face à des piétons ou cyclistes imprudents qui coupent sa trajectoire le véhicule autonome doit-il accepter de les percuter et de les tuer ou doit-il se jeter sur un mur au risque de tuer ses passagers ? Doit-il pour cela comparer le nombre de piétons et de passagers ? Doit-il privilégier les personnes a priori vulnérables ou ses passagers a priori plus protégés ? Comment le véhicule juge-t-il de la vulnérabilité des autres personnes ? Un acheteur potentiel acceptera-t-il d'acquérir un engin qui est prêt à le tuer volontairement dans certaines situations ? Etc.

Derrière ces questions se cache un problème technique pour les logiciels et les algorithmes qui les définissent. Lorsque l'environnement extérieur sort de ce qui est prévu dans sa programmation un logiciel peut donner des réponses totalement inadaptées : par exemple, lorsque la bourse baisse trop brusquement il est arrivé que des logiciels de trading automatique amplifient la chute des cours voire ne créent un krach en voulant brader à tout prix leurs produits financiers.

La solution la plus évidente consiste à interrompre le système informatique lorsque la situation est en dehors des plages habituelles de fonctionnement et à rendre la main à un être humain. Pour les véhicules autonomes c'est aussi cette solution qui est choisie le plus souvent : néanmoins elle n'est pas applicable lorsque la réaction doit être immédiate, lorsque le « surveillant humain » ne veut ou peut reprendre la conduite ou tout simplement lorsque le véhicule sera censé être complètement autonome (niveau 5).

La NHTSA dans ses directives publiées en septembre 2016 aborde les considérations éthiques : elle demande que les concepteurs des véhicules décrivent de façon consciente et explicite les décisions que le véhicule va prendre lorsqu'il est mis face à des situations de conflit. Elle cite le cas où un véhicule est bloqué derrière un autre garé en double-file et qu'il ne peut passer sans franchir une ligne continue. Un conducteur humain s'autorise à le faire si rien ne vient en face : que ferait le véhicule autonome ? Elle cite aussi le dilemme de la protection des personnes vulnérables par rapport à celle de ses passagers.

[42] Un robot ne peut porter atteinte à un être humain, ni, en restant passif, permettre qu'un être humain soit exposé au danger ; un robot doit obéir aux ordres qui lui sont donnés par un être humain, sauf si de tels ordres entrent en conflit avec la première loi ; un robot doit protéger son existence tant que cette protection n'entre pas en conflit avec la première ou la deuxième loi. Converties plus tard par Asimov, pour les outils : un outil doit pouvoir être employé de manière sûre ; un outil doit accomplir sa fonction efficacement sauf si cela peut blesser l'utilisateur ; un outil doit rester intact durant son utilisation, sauf si sa destruction est requise pour son utilisation ou sa sécurité.

Ce que la NHTSA refuse c’est que des choix implicites et masqués ayant des conséquences graves soient camouflés à l’intérieur des programmes sans que l’administration ni les parties prenantes ne puissent en discuter.

Parce que l’éthique des véhicules reflète en réalité l’éthique de ses concepteurs et parce que leurs choix auront des conséquences pour la société dans son ensemble il est nécessaire que celle-ci puisse donner son avis et décider ce qui est moralement acceptable.