Enjeux numériques – N°7 – septembre 2019 – © Annales des Mines

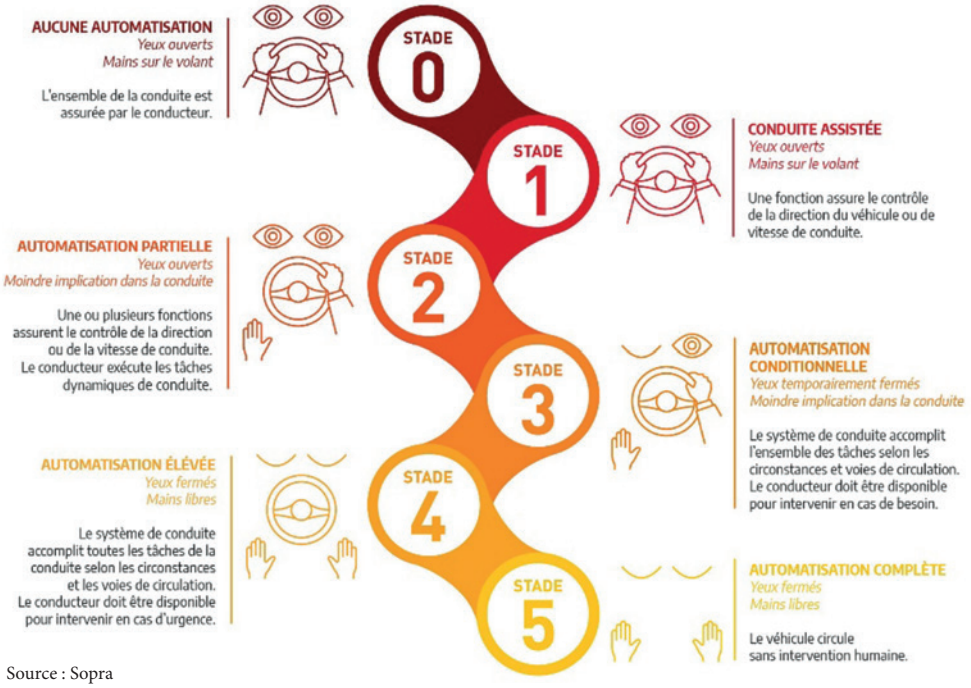
Sécurité routière, gestion des données et libertés individuelles à l'heure des véhicules autonomes et connectés

Par **Floran VADILLO**
Docteur en science politique
Chercheur associé au CMRP (Université de Bordeaux)
Directeur conseil sécurité chez Sopra Steria (1)

Objet longtemps réservé aux exercices de science-fiction, le véhicule autonome (VA) s'apprête à investir notre réalité. En effet, les initiatives se multiplient, portées notamment par Google, Tesla, Citroën ou Valeo, permettant de donner corps à ce qui paraissait utopique, si bien que l'interrogation porte désormais moins sur les potentialités que sur le rythme d'introduction des VA sur nos routes : les scénarios de diffusion lente (fondés sur le taux de remplacement annuel des véhicules) évoquent l'horizon 2040-2050, tandis que ceux basés sur des hypothèses d'une pénétration rapide du marché avancent l'horizon 2020-2030 (2). Cette dernière projection semble ambitieuse au regard des revirements de certains constructeurs (à l'instar de PSA qui a récemment renoncé à produire des véhicules entièrement autonomes), même si fleurissent déjà de nombreuses expériences en matière de transport collectif urbain (à La Rochelle, Lyon, etc.) et même si les pouvoirs publics affichent une claire volonté d'accompagnement (3). D'ici là, les véhicules, sans être autonomes, vont intégrer toujours plus d'éléments connectés afin d'assister voire de suppléer le conducteur (ce qui justifie le recours au terme générique de « véhicule autonome et connecté » [VAC] qui subsume les différents stades d'évolution des véhicules, cf. schéma ci-après).

Au-delà d'adaptations des règles de conduite ou des missions des forces de sécurité intérieure (FSI) et des administrations de la sécurité routière, une réflexion peut se nouer autour du rôle du VAC lui-même comme acteur de la sécurité routière, parfois indépendamment de son conducteur/passager. En effet, la technologie permet d'élargir le champ des possibles et notamment d'envisager de nouvelles interactions avec les FSI. Toutefois, cet horizon doit être pondéré par des considérations juridiques et sociales, elles aussi évolutives sous certaines conditions. Car la voiture ne se résume ni à un simple moyen de locomotion, ni à un outil : elle constitue un objet économique et social aux très fortes implications.

(1) Cette contribution reprend les principaux éléments d'une note publiée par DE MARICOURT A. et VADILLO F. (2019), « Les défis du véhicule autonome et connecté pour la sécurité intérieure et routière (1) : Le VAC au service des forces de sécurité ? », *Idées et prospective*, n°2, Sopra Steria, février.
(2) Cf. PAVEL I. *et al.* (2016), « Les enjeux économiques et industriels du véhicule connecté et automatisé », *Annales des Mines - Réalités industrielles*, mai 2018, p. 19. France Stratégie a également détaillé divers scénarios, cf. JANIN L. *et al.* (2016), « La voiture sans chauffeur, bientôt une réalité », note d'analyse n°47, avril.
(3) Volonté traduite tant par le décret n°2018-211 du 28 mars 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques que par l'article 125 de la loi n°2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises.



Source : Sopra

De nouvelles modalités pour un contrôle classique : un VAC obtempérant ?

En raison de la cohabitation plus ou moins temporaire qui ne manquera pas de s'instaurer entre VA, véhicules connectés et véhicules ordinaires, les FSI devront pouvoir durablement procéder à des contrôles classiques des flux routiers (identité, alcoolémie, documentation du véhicule, etc.). Si l'on peut supposer qu'aux stades 3 et 4 les conducteurs pourront reprendre le contrôle du véhicule pour obtempérer à une demande d'arrêt, qu'en sera-t-il pour un VA de stade 5 ? De même, en cas de refus d'obtempérer (passible d'une peine d'amende et de prison en application de l'article L. 233-1 du Code de la route, CR) ou d'un délit de fuite (L. 231.1 du CR), les forces de l'ordre pourraient-elles prendre la maîtrise d'un VAC et l'arrêter de leur propre initiative [4] ?

Juridiquement, en dehors de considérations de proportionnalité qu'appréciera le Conseil constitutionnel, rien ne semble s'y opposer puisque ne pas obéir à une injonction des FSI ou prendre la fuite relève aujourd'hui du délictuel et que des dispositifs d'arrêt physique (herses) ou de blocage du moteur sont déjà mis en œuvre dans le cadre d'opérations de contrôle des flux routiers ou contre des « go fast » par exemple.

Plus trivialement, les forces de l'ordre pourront-elles prendre la maîtrise d'un VAC pour le conduire à la fourrière ? Une nouvelle fois, rien ne semble s'y opposer d'un point de vue juridique puisque

(4) IDRAC A.-M., « Développement des véhicules autonomes : Orientations stratégiques pour l'action publique », *Rapport remis aux ministres de l'Intérieur, de l'Économie et des Finances, des Transports ainsi qu'au secrétaire d'État chargé du numérique*, mai 2018, p. 44, signale sans développer le sujet : « La France demandera à ce que des exigences soient développées dans la réglementation technique internationale, afin que les véhicules dont les systèmes de conduite sont totalement délégués au véhicule soient dotés de la capacité d'appliquer un ordre d'arrêt par les forces de l'ordre, et ce en toute sécurité. »

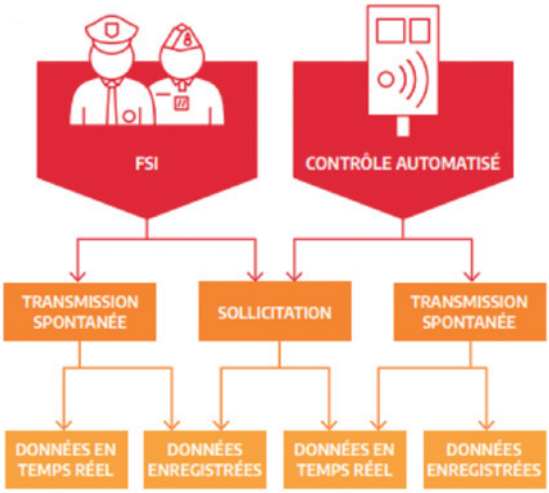
l'article L. 325-1 CR pose la capacité d'opérer « sans l'accord du propriétaire » et que l'article L. 325-2 autorise à « ouvrir ou faire ouvrir les portes du véhicule, manœuvrer ou faire manœuvrer tous appareils. [Les forces de l'ordre] peuvent conduire le véhicule ou le faire conduire, en leur présence, vers le lieu de mise en fourrière en utilisant, le cas échéant, les moyens autonomes de propulsion dont le véhicule est muni ».

Néanmoins, cette capacité de prise de contrôle interroge : les policiers et gendarmes disposeront-ils d'une « clé universelle » ou de capacités de « hacking » légal ? Il ne s'agirait pas alors de conduire le véhicule mais de le contraindre à opérer une manœuvre intégrée dans l'algorithme et opérée dans les meilleures conditions de sécurité.

Les deux solutions exposent les véhicules à des risques « cyber » accrus mais aussi à des stratégies criminelles de parade. Pourtant, si elles devaient être rejetées, demeurerait la question des modalités d'arrêt d'un VAC sur ordre des FSI, notamment pour le cas où il serait vide d'occupant. Comment dès lors prévenir les risques criminels (attentat, voiture bélier) ou de défaillance mettant en danger la vie d'autrui ? Le sujet s'avère stratégique si l'on considère que les VAC sans occupants vont sans doute se multiplier (taxis autonomes, voiture allant se garer ou chercher un occupant, livraisons, etc.).

Une nouvelle génération de constat des infractions ?

Sans même capitaliser sur la « peur du gendarme », le déploiement des VAC aura pour principale conséquence la réduction drastique d'une série d'infractions aux règles de conduite (distance de sécurité, vitesse, signalisation, etc.) en automatisant leur respect et en diminuant la part d'intervention humaine. Il s'agit d'ailleurs du principal argument mis en exergue par ses promoteurs. Toutefois, il n'empêchera pas la commission de certaines infractions liées par exemple à une non-prise en compte des indications du VAC (aux stades 3 et 4), à un défaut de vigilance, à une imprudence, à de la négligence ou à de la tromperie [5]. Mais, dans ces cas, la constatation d'infractions pourrait se trouver facilitée par la transmission de données inhérentes au dialogue permanent et nécessaire au fonctionnement du véhicule.



Source : Sopra Steria

(5) Pour de plus amples développements, se reporter à DE MARICOURT A. et VADILLO F. (2019), « Les défis du véhicule autonome et connecté pour la sécurité intérieure et routière (1) : comment gérer la mixité du trafic automobile ? », *Idées et prospective*, n°1, Sopra Steria, janvier 2019.

Celle-ci pourrait s'opérer selon deux principaux paramètres :

- sur sollicitation ou à l'initiative du VAC au bénéfice des dispositifs de contrôle automatisé (classiques ou désormais intégrés dans l'infrastructure routière avec laquelle échange le véhicule) ou des forces de l'ordre ;
- en temps réel (contrôle classique) ou *a posteriori* (contrôle de l'historique de conduite). Cette dernière hypothèse se rapproche fortement de la technologie des enregistreurs de données d'événements de la route (EDR) ou du boîtier télématique électronique (BTE) dont certaines entreprises équipent leurs flottes de véhicules afin de gérer en temps réel les déplacements de leurs collaborateurs (position géographique, parcours réalisé, distance parcourue – et donc vitesse moyenne –, temps de conduite et d'arrêt, etc.) ou encore des chronotachygraphes obligatoires pour les véhicules de transport routier et auxquels les forces de l'ordre ont légalement accès (article L. 130-6 du Code de la route). Sur un plan connexe mais prometteur, Michelin a lancé l'initiative « better driving » qui suppose l'installation d'un boîtier connecté permettant le partage des données de conduite.

La collecte de données pourrait également concerner les infractions relatives aux comportements des conducteurs/passagers à l'intérieur du VAC grâce à un dispositif de contrôle interne au véhicule. Celui-ci pourrait contribuer, *a minima,* à « la mise en place d'indicateurs de l'activité du conducteur pour s'assurer de sa capacité à reprendre les commandes et assurer la supervision du système ; le maintien des capacités de conduite des conducteurs malgré une pratique réduite de l'activité de conduite ; les problèmes de distraction dus à l'usage de systèmes lors de la conduite [(6)] ». Ce contrôle pourrait être étendu aux autres comportements en infraction avec le Code de la route grâce à des mécanismes de contrôle intégrés (éthylotest, antidémarrage, etc.) ou le recours à l'intelligence artificielle (analyse comportementale, interprétation d'images, etc. [(7)]). Il est d'ailleurs à noter que la constatation automatique est déjà autorisée par l'article R. 130-11 du Code de la route pour le port de la ceinture, l'usage du téléphone au volant et le défaut d'assurance ; l'intégrer au véhicule s'inscrirait dans la même logique.

Cependant, en l'état actuel du droit, ces développements semblent impossibles. En effet, l'article L. 311-2 du Code de la route prévoit que « les informations et données embarquées du véhicule autres que celles [relatives à l'identification et à la conformité du véhicule et de ses composants] ne peuvent être utilisées comme preuve de la commission d'autres infractions prévues par le présent code ». En cela, cet article s'inscrit dans la philosophie du droit à ne pas s'auto-incriminer notamment consacré par la Cour de cassation.

La démarche interroge également du point de vue de la proportionnalité des moyens conférés aux FSI pour accomplir leur mission (la fameuse « conciliation nécessaire entre le respect des libertés et la sauvegarde de l'ordre public » mise en exergue par le Conseil constitutionnel). Ce point s'avère d'autant plus prégnant que le véhicule bénéficie des mêmes protections que le domicile et que pareille ingérence (en particulier pour la surveillance des comportements dans l'habitacle) peinerait à se justifier par un principe supérieur au respect de la vie privée. Dans le même ordre d'idées, elle se heurterait au principe de protection des données personnelles (en particulier au regard du RGPD).

Au demeurant, l'hypothèse soulève la question de son acceptabilité par l'opinion publique, d'autant que les véhicules actuels pourraient déjà être équipés de BTE ou de chronotachygraphes, les moteurs pourraient être bridés, etc., si la sensibilité des citoyens sur ce sujet ne disqualifiait ces moyens de contrôle.

(6) HAUTIERE N. *et al.* (2017), « Véhicules connectés et autonomes : quels enjeux technologiques, juridiques et de sécurité routière ? », *Hygiène et sécurité du travail*, n°246, mars, p. 101.
(7) Il semble néanmoins douteux que pareil dispositif discrimine par exemple les passagers exemptés de port de ceinture en raison d'un certificat médical ou de leur morphologie, comme le prévoit pourtant le Code de la route.

Des enquêtes facilitées ?

Les enquêtes liées aux accidents

En cas d'accident, les enquêtes conduites pourraient se trouver facilitées par l'enregistrement des données de conduite. À ce titre, il importera que les forces de l'ordre puissent disposer de systèmes d'information interopérables avec les futurs EDR afin d'accéder aux données à valeur judiciaire.

Mais avant cette évolution majeure, les FSI ont besoin d'accéder à des données plus fiables de localisation des accidents. Le dispositif eCall, promu par la Commission européenne et qui permet d'établir un contact avec les forces d'intervention en cas de nécessité, œuvre en ce sens. De même, il semble important de sécuriser et de fiabiliser la Base de Données Accidents corporels de la Circulation (BAAC). À titre d'exemple, l'interconnexion avec le SIV (Système d'Immatriculation des Véhicules) et avec le fichier des permis de conduire permettrait aux forces de l'ordre d'intégrer dans la procédure et le BAAC des informations valides concernant le numéro technique du véhicule et l'état des droits à conduire.

Néanmoins, l'ensemble de ces évolutions suppose que les enquêteurs se dotent de capacités de traitement et d'analyse [8], technologie encore à ses balbutiements en France. De fait, le renforcement du Bureau d'Enquêtes sur les Accidents de Transport terrestre (BEA-TT) du ministère des Transports pourrait faciliter la concentration des moyens techniques et de l'expertise, mais aussi permettre de faire face à un éventuel éparpillement des données produites et échangées.

De même, ces enquêtes devront conduire au développement de compétences « cyber » dans la mesure où les risques de malveillance en ce domaine se trouveront accrus par la généralisation du VAC.

Les enquêtes judiciaires ou administratives

En dehors des enquêtes liées aux accidents, les activités de police judiciaire ou de renseignement pourront grandement profiter de l'arrivée du VAC sur les routes. En effet, les services de renseignement ou de police judiciaire pourront par exemple solliciter un accès aux données de géolocalisation dans le cadre prévu par le Code de procédure pénale [9] (CPP) ou le Code de la sécurité intérieure [10] (CSI) (une modification législative sera alors nécessaire pour faire figurer l'entité de centralisation des données du VAC – les constructeurs ou les loueurs automobiles par exemple – aux côtés des opérateurs de communications électroniques). De même, la pose de balises [11] et la sonorisation de l'habitacle [12] prévues par les mêmes codes pourront s'avérer opérationnellement beaucoup plus aisées à distance (« hacking [13] » ou par le biais de l'entité de centralisation des données ; dans ce dernier cas, une modification législative sera à nouveau nécessaire).

Enfin, un régime d'obligation de déclaration de soupçon des infractions les plus graves révélées par les données que collectent les entités de centralisation des données (constructeurs, loueurs ou sociétés d'assurance) pourrait être créé sur le modèle de celui appliqué aux banques dans le cadre de la lutte contre le blanchiment [14] et le terrorisme. Cela supposerait néanmoins que la sécurité routière soit interprétée par le Conseil constitutionnel comme un objectif supérieur aux divers

(8) Constat partagé par DE LA FORTELLE A. (2014), « La conduite automatisée : simple buzz, ou réalité industrielle ? », *Annales des Mines - Réalités industrielles*, mai, p. 88.
(9) Cf. le III de l'article L. 34-1 du Code des postes et des communications électroniques actionné par les articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale.
(10) Article L. 851-4 du Code de la sécurité intérieure.
(11) Article 230-32 du Code de procédure pénale et suivants ou L. 851-5 du CSI.
(12) Article 706-96 du CPP et suivants ou L. 853-1 du CSI et L. 853-3.
(13) Article 706-102-1 du CPP et suivants ou article L. 853-2 du CSI.
(14) Article L. 561-15 du Code monétaire et financier.

secrets professionnels et au moins équivalent au respect de la vie privée pour être mise en balance avec celui-ci. D'une manière générale, l'ensemble de ces questionnements souligne l'acuité du statut de la donnée produite et de sa gestion.

L'épineux droit d'accès aux données

Au-delà de la question de données spécifiquement générées et collectées à des fins de sécurité, celle de l'exploitation des données spontanément produites par l'usage d'un VAC revêt un caractère éminemment stratégique. En effet, le VAC sera, par nature, un producteur et un récepteur de données. Dans ces conditions, si certains auteurs prennent en considération la nécessité de penser dès à présent l'accès aux données et son contrôle [(15)], leur perspective s'avère principalement économique : reconstitution collaborative de l'environnement de conduite, gestion des infrastructures, alertes de sécurité routière ou de trafic, mais aussi amélioration des algorithmes utilisés par leur entraînement à grande échelle.

Ces données seront-elles centralisées ? Le cas échéant, par quelle entité ? Le constructeur, ses fournisseurs, les entités administrant les infrastructures ? Des loueurs devenus omnipotents ? Car l'acquisition d'un VAC pourrait perdre de l'intérêt (économique, au regard du risque d'obsolescence ou du coût, mais également social, avec la modification des représentations attachées à la voiture) ; dès lors, la location ou le *leasing* pourraient connaître un essor considérable. De ce fait, les loueurs centraliseraient les données produites ou collectées qui bénéficieraient d'un potentiel économique inégalé. Il semble nécessaire que la loi vienne aider à régler ces questions sous peine de laisser le citoyen désemparé face à des logiques économiques majeures.

D'ailleurs, les constructeurs ont proposé des principes d'accès différencié à plusieurs types de données (sécurité routière, services multifournisseurs, services personnalisés, données commerciales et suivi des composants) qui supposent un accès soit à des données anonymisées, soit contractuel entre acteurs, soit contractuel avec le conducteur [(16)]. De même, une réflexion existe autour de l'idée de conférer un statut d'intérêt général à certaines données (sécurité routière, gestion des trafics et des infrastructures). Or, l'insistance sur le cadre contractuel et sur l'anonymisation n'est pas anodine. En effet, les données collectées fourniront des indications sur l'identité des conducteurs, leur localisation, leurs habitudes de déplacement, leur type de conduite, le nombre de passagers transportés, etc. Dans tous les cas de figure sera nécessaire une évolution de l'actuel article L. 330-5 du Code de la route qui prévoit le traitement et la transmission de certaines données à des fins statistiques, commerciales ou technologiques.

On le constate, l'arrivée du VAC sur nos routes, voire sa généralisation, soulève de nombreux enjeux juridiques, technologiques ou humains. Ces enjeux exacerbent même la relation parfois conflictuelle entre le droit, les libertés individuelles et la technique. Ils posent par conséquent une triple exigence : la première réside dans la réaffirmation du statut de régulateur assumé par la puissance publique face aux acteurs économiques ; la deuxième suppose d'œuvrer à une acceptabilité sociale des évolutions normatives ; la troisième, sans doute la plus importante, impose aux législateurs et aux juristes une montée en généralité pour éviter l'obsolescence programmée de la norme elle-même ; car si nos outils évoluent, les principes doivent bénéficier d'une certaine intangibilité.

(15) JANIN L. et al. (2016), « La voiture sans chauffeur, bientôt une réalité », *France Stratégie*, note d'analyse n°47, avril, p. 4 ou IDRAC A.-M. (2018), « *Développement des véhicules autonomes : Orientations stratégiques pour l'action publique* », *Rapport remis aux ministres de l'Intérieur, de l'Économie et des Finances, des Transports ainsi qu'au secrétaire d'État chargé du numérique*, mai.
(16) IDRAC A.-M., l*oc. cit.*, p. 65. L'autrice insiste sur l'importance d'un consentement éclairé dans le cadre du RGPD.