TOUS FLIQUÉS

CAMÉRAS, CAPTEURS, GPS, RADARS... QUAND LA TECHNOLOGIE SE RETOURNE CONTRE LES CONDUCTEURS

LIGUE DE DÉFENSE DES CONDUCTEURS
STOP À LA RÉPRESSION ABSURDE, OUI À LA CONDUITE RESPONSABLE

NOVEMBRE 2024

LIGUE DE DÉFENSE DES CONDUCTEURS

STOP À LA RÉPRESSION ABSURDE, OUI À LA CONDUITE RESPONSABLE

Créée en 2006, la Ligue de Défense des Conducteurs est une association loi 1901 qui réunit 1 million de sympathisants, ralliés derrière la devise « *Stop à la répression absurde, Oui à la conduite responsable* ». La Ligue de Défense des Conducteurs, indépendante de tout organisme public, de toute formation politique, syndicale ou professionnelle, est intégralement financée par les dons de ses membres.

Notre association a pour but de réunir le plus grand nombre de conducteurs raisonnables et de faire entendre leur voix, pour en finir avec cette répression absurde et passer à une politique efficace de sécurité routière. Nous agissons en produisant et en décryptant l'information, mais aussi en organisant des campagnes de mobilisation auprès des élus et du gouvernement, pour faire évoluer les politiques et les moyens mis en œuvre afin de garantir notre sécurité sur les routes. Au-delà des dérives de la répression routière, nous nous appliquons également à dénoncer la stigmatisation dont les conducteurs font l'objet aujourd'hui, simplement parce qu'ils utilisent leur véhicule au moins régulièrement, si ce n'est quotidiennement. Les problématiques de transition écologique ou d'hyperfiscalité automobile se sont ainsi ajoutées à nos nombreux sujets de mobilisation, car elles constituent elles aussi des contraintes et des menaces pour la mobilité individuelle des Français.

L'exploitation des données personnelles générées par nos voitures connectées et les perspectives quasi infinies qu'offre la technologie numérique à la répression automatisée sont de nouveaux sujets de préoccupation, auxquels nous consacrons cette première étude.

TOUS FLIQUÉS

CAMÉRAS, CAPTEURS, GPS, RADARS... QUAND LA TECHNOLOGIE SE RETOURNE CONTRE LES CONDUCTEURS

SOMMAIRE

I- LA VOITURE, MINE D'INFORMATIONS ..... p. 6

A- Connectée ne veut pas dire branchée ..... p. 6
B- Des caméras partout ..... p. 7
C- Après le flicage, l'espionnage ? ..... p. 9
D- Les mouchards que sont les cartes SIM et les EDR ..... p. 10

II- DU FLICAGE POUR GÉNÉRER DE NOUVEAUX REVENUS ..... p. 11

A- Maintenance « *over-the-air* » et options à la demande pour les constructeurs ..... p. 11
B- Quand la transgression des règles règne en maître ..... p. 13
C- La juteuse revente de la donnée déjà intégrée dans le business plan des constructeurs ..... p. 13
D- Les assureurs en embuscade ..... p. 14

III- LES NOUVELLES TECHNOLOGIES, PRÉCIEUSES ALLIÉES DES FORCES DE L'ORDRE ..... p. 16

A- Un budget et des radars qui ne mollissent pas ..... p. 16
B- Les drones pour surveiller la sécurité routière ..... p. 16
C- Une vidéoverbalisation devenue aussi banale qu'injuste ..... p. 17
D- La vidéoverbalisation pour sanctionner bientôt dans les Zones à faibles émissions ..... p. 17
E- Les lettres et SMS envoyés aux « mauvais conducteurs » de l'État de Washington ..... p. 18
F- Le système ougandais, une inspiration pour nos pouvoirs publics ? ..... p. 18

AVANT-PROPOS

Il fut un temps, une automobile c'était un châssis, un moteur, quatre roues et un volant. Pas de question à se poser, il n'y avait guère que le bricoleur et le mécanicien du garage qui pouvaient lire l'histoire que chaque automobile avait à raconter. Mais depuis quelques années, ces histoires sont devenues bien plus complexes. De mutiques, nos voitures sont devenues extrêmement bavardes, pourvu que l'on sache les comprendre. Pour être si disertes, elles intègrent aujourd'hui des colonies de capteurs en tout genre, ainsi que des moyens informatiques pour collecter, interpréter et – de plus en plus - transmettre les informations recueillies. Une voiture moderne ne s'arrête désormais jamais de parler.

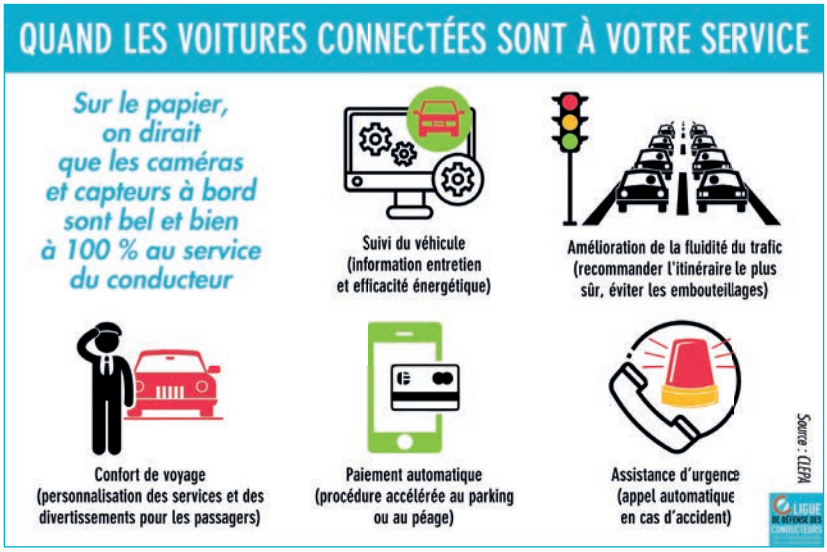
Malgré les apparences, la collecte de données par l'automobile n'est en réalité pas si récente. C'est en effet en 1969 que Volkswagen installe pour la première fois un ordinateur embarqué rudimentaire pour surveiller le système d'injection de la VW 1500, suivi au milieu des années 1970 par le japonais Datsun.

Puis, au début des années 1980, l'industrie automobile américaine commence à poser les bases de véritables outils de diagnostic embarqué, avec par exemple la surveillance de l'état du moteur en temps réel. Pour l'utilisateur, ces dispositifs se résument alors généralement à un inquiétant voyant qui s'allume, voire clignote, au tableau de bord. Le décodage du défaut reste la prérogative du mécanicien et chaque constructeur développe ses propres codes et outils d'analyse.

En 1988, l'agence pour la qualité de l'air de l'État de Californie (la fameuse structure publique à l'origine du scandale industriel du « *dieselgate* » qui, en 2015, révèle les tricheries de Volkswagen, puis d'autres marques, en matière de déclarations d'émissions de CO_2 et d'oxydes d'azote) impose à tous les constructeurs d'installer des outils de diagnostic embarqué, plus connus sous le nom d'OBD (pour On-Board Diagnostic). En 1996, cette même agence américaine écrit les spécifications dites « OBD-II », avec un connecteur et des codes de défaut standardisés qui seront imposés dès 1998. En Europe, une déclinaison appelée EOBD devient elle aussi obligatoire à partir de 2001 pour certains types de véhicules, obligation étendue à l'ensemble de la production en 2004. L'automobile entre alors dans l'ère de la production de masse de données. Désormais, tout ce qui se passe dans un moteur est capté et enregistré dans l'unité centrale de la voiture, puis restitué à la demande sous forme de codes de défaut standardisés, ou DTC (pour *Diagnostic Trouble Codes*). Si vous possédez une Renault, n'importe quel mécanicien, même chez Citroën ou Fiat, peut ainsi identifier la plupart des pannes ou défauts simplement en branchant sa fameuse « valise diagnostic » à la voiture. Mais ce n'est là que l'un des innombrables débouchés pour ces données.

Quoi qu'il arrive, que vous le vouliez ou non, votre véhicule neuf dispose aujourd'hui d'immenses capacités de connexion (selon la PFA-Plateforme Automobile, le nombre de lignes de code dans une voiture était de 100 millions en 2022, et atteindra 1 milliard en 2030 !). Et c'est vous, conducteurs, qui générez des données dont vous êtes, sur le papier, propriétaires. Sauf qu'en signant votre contrat d'achat, vous consentez la plupart du temps à ce que le constructeur les exploite... sans forcément que votre vendeur vous ait pleinement informés de ce que cela implique. Entendons-nous bien : comme le montre l'illustration ci-dessous, l'utilisation de vos data peut évidemment se faire à votre bénéfice, ne serait-ce que dans le cadre de la maintenance de votre véhicule, votre confort de voyage ou l'assistance d'urgence. Mais les champs d'application sont tellement immenses, les entreprises alléchées par l'extraordinaire potentiel que représente l'identification de vos déplacements ou de vos petites habitudes en voiture, les débordements et dérives liés aux failles informatiques ou aux actes malveillants des hackers tellement inquiétants qu'à la Ligue de Défense des Conducteurs, il nous a semblé primordial de tirer la sonnette d'alarme.

Cette présente étude a pour objectif d'informer et d'alerter tous les conducteurs des perspectives quasi infinies que leurs données offrent à l'État et aux entreprises privées, lesquels s'appuient aussi sur des technologies de flicage toujours plus prometteuses. Que ce soit en matière de business... ou de contrôle. ■



I. LA VOITURE, MINE D'INFORMATIONS

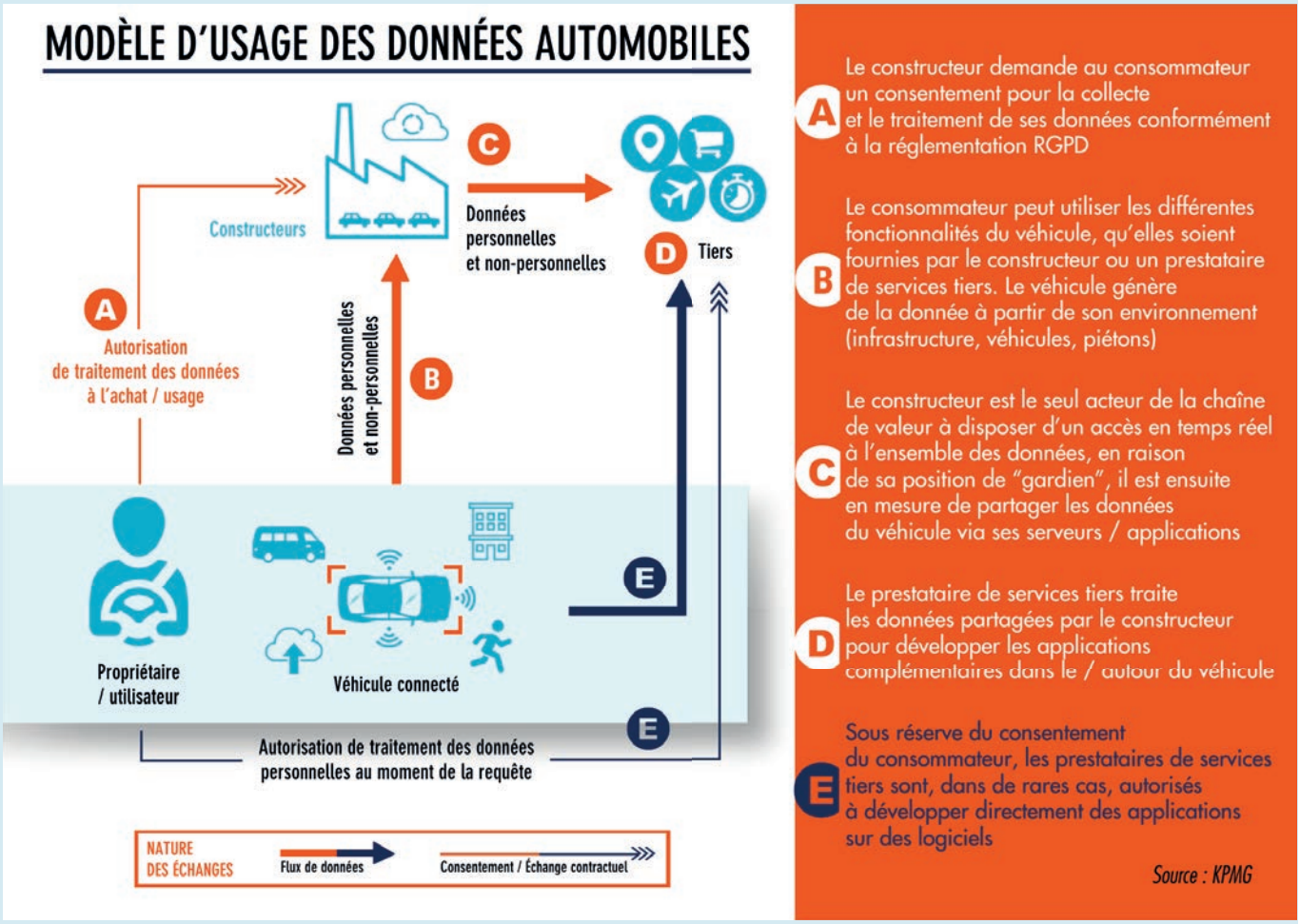
A. Connectée ne veut pas dire branchée

Une « voiture connectée » est une auto moderne, fabriquée à partir des années 2000 ; « connectée » ne signifie nécessairement pas que le véhicule propose Internet ou des fonctionnalités similaires à bord. Cela désigne plutôt une voiture dont les différents éléments et systèmes sont capables d'interagir entre eux. Pour communiquer, les appareils utilisent ce que l'on appelle le « bus Can » : « *Le bus Can sert en quelque sorte d'autoroute de données* », explique un document de formation interne du groupe Volkswagen, il « *permet l'interconnexion de groupes d'organes électroniques* ». Or, cette autoroute est déjà proche de l'état de saturation, d'après une étude du cabinet

EXPLOITATION DE VOS DONNÉES : TOUT COMMENCE AVEC VOTRE AUTORISATION

Avez-vous bien lu le contrat d'achat de votre nouvelle voiture neuve ? Si oui, vous aurez compris que la marque que vous avez choisie se révèle très intéressée par les données que vous allez générer une fois au volant... Et tout comme vous acceptez nonchalamment les « cookies » en arrivant sur un site internet, tout comme vous affichez, généralement, une très grande décontraction vis-à-vis des infos auxquelles vous laissez libre accès lorsque vous surfez, vous avez signé. Vous avez donc donné votre accord pour que votre « data » personnelle soit exploitée.

Le schéma ci-dessous, réalisé par le cabinet de conseil KPMG, explique très clairement comment la « machine » fonctionne.



Dans sa note de synthèse (juin 2023), KPMG explique : « *Les données créées par les véhicules connectés peuvent être caractérisées* ***selon leur cible*** », à savoir le conducteur (préférences, âge, adresse, etc.), le véhicule (vitesse, localisation...) ou son environnement (météo, feux de circulation, piétons, etc.). Ou alors, « ***selon leur fréquence de mise à jour*** » (inférieure à 1 mois, inférieure à 1 heure, inférieure à 1 minute et inférieure à 1 seconde).

de conseil KPMG : « *Un véhicule connecté génère en moyenne un volume de 25 giga-octets de données par heure d'usage, soit plus de deux mois de navigation sur le web. Ce volume est en constante augmentation ces dernières années* », indiquent les auteurs, car « *le nombre de capteurs par véhicule a plus que doublé en dix ans via le développement de l'électronique embarquée* ». Toujours selon l'étude du cabinet de conseil, la voiture connectée utilise les instruments suivants pour collecter des données : radars (mesure de la vitesse), GPS (géolocalisation), capteurs à ultra-sons (pour localiser les objets à proximité de l'auto), caméras en trois dimensions (lecture des feux rouges), lidar (lecture de la signalisation) et caméras infrarouges, afin de voir la nuit. En interrogeant le bus Can, il est donc possible de connaître tout ce qui se passe –ou s'est passé- à bord d'une voiture : niveau de carburant restant, position enclenchée sur les essuie-glaces, condamnation ou non des portes, distance parcourue depuis le démarrage... La liste des possibilités est quasi infinie. Ce sont 10,7 millions de voitures connectées qui circulent actuellement en France (228 millions dans le monde, toujours selon KPMG).

B. Des caméras partout

À l'instar des smartphones, les voitures sont devenues des studios de cinéma ambulants. À l'intérieur du véhicule, la star, c'est vous désormais. Une caméra peut scruter vos yeux en permanence : il s'agit d'un système de surveillance du conducteur. L'équipementier Valeo parle de « *détection de la somnolence et de la distraction* ». Si la paupière de la personne au volant devient lourde, si ses battements se font de plus en plus fréquents, le véhicule est désormais capable de vous indiquer qu'il est temps de faire une pause. Parfois, sous la forme d'une tasse à café apparaissant sur le tableau de bord.

© Mercedes

Si les caméras pour prévenir la somnolence ont d'abord été l'apanage des Mercedes et autres marques premium, ce n'est plus du tout le cas aujourd'hui. Certains utilitaires Peugeot proposent des caméras similaires en série depuis 2018. Et si les caméras montées en série ne suffisent pas, il y a toujours moyen d'en installer *a posteriori*. Les chauffeurs-livreurs d'Amazon sont ainsi filmés en permanence aux États-Unis. Non seulement leur conduite est constamment surveillée, mais aussi leur aptitude physique. Divers articles de la presse américaine font état de chauffeurs harcelés par ce contrôle permanent, qui les a contraints à signer des formulaires « de consentement biométrique ». De la même manière, les VTC d'Uber aux États-Unis sont désormais richement dotés en caméras. L'objectif est officiellement de lutter contre la recrudescence d'agressions sexuelles dont ont été victimes certaines clientes... Mais le constructeur champion des caméras demeure toutefois Tesla.

La marque d'Elon Musk installe des caméras à bord de ses véhicules depuis 2021. Celles-ci ne poursuivent pas d'autres objectifs que de scruter en permanence le conducteur. Selon l'ouvrage « *Elon Musk* » rédigé par le journaliste Walter Isaacson et sorti en septembre 2023, le patron de Tesla aurait souhaité qu'une caméra intérieure se déclenche systématiquement lorsque le mode « Autopilot » est activé. Ce pseudo-mode de conduite autonome fait en effet couler beaucoup d'encre, car il aurait été responsable d'accidents aux États-Unis. Or, d'après l'ancien journaliste de CNN, l'idée de monter des caméras en lien avec l'Autopilot viserait précisément à prouver que si accident il y a eu, c'est en raison de la distraction du conducteur et non d'un défaut de fonctionnement de l'Autopilot : les images pourraient le prouver ! Et le premier intéressé pour visionner les images n'est pas forcément le constructeur, mais bel et bien la NHTSA (la Sécurité Routière aux États-Unis), qui peut ainsi disposer d'éléments fiables pour déterminer les responsabilités dans le cadre d'un accident. Toutefois, la quintessence de la caméra intérieure semble aujourd'hui être atteinte par un produit proposé par l'équipementier Bosch. La caméra balaie en permanence l'habitacle du véhicule. Elle peut donc repérer une ceinture mal attachée, et grâce à l'intelligence artificielle, elle peut aussi imposer des décisions au véhicule. Ainsi, en cas de choc, la caméra peut par exemple décider de ne pas déclencher d'airbag à tel ou tel endroit parce qu'elle y avait détecté un siège auto, ce qui représenterait un trop grand risque pour l'occupant.

L'omniprésence des caméras intérieures a mené le sénateur américain Bill Dodd à imaginer une loi qui a été approuvée par le gouverneur de Californie le 13 octobre 2023 : « *Mon projet vise à empêcher la prise de vidéos non désirées par les caméras embarquées et à donner au consommateur un meilleur contrôle de ses informations personnelles* », explique le sénateur dans les motifs qui l'ont poussé à légiférer. Car comme il l'indique un peu plus loin, « *il semble que quel que soit l'endroit où l'on se rend aujourd'hui, on est enregistrés ou surveillés sans la moindre idée de comment ces images sont exploitées. Cette brèche dans notre vie privée arrive maintenant jusqu'à l'intérieur de nos propres voitures.* » Le sénateur Dodd est ainsi parvenu à faire voter une obligation d'information de présence de caméras à bord des voitures, ainsi que le fait que les images ne peuvent être transmises à des tiers sans consentement du propriétaire de l'auto au préalable.

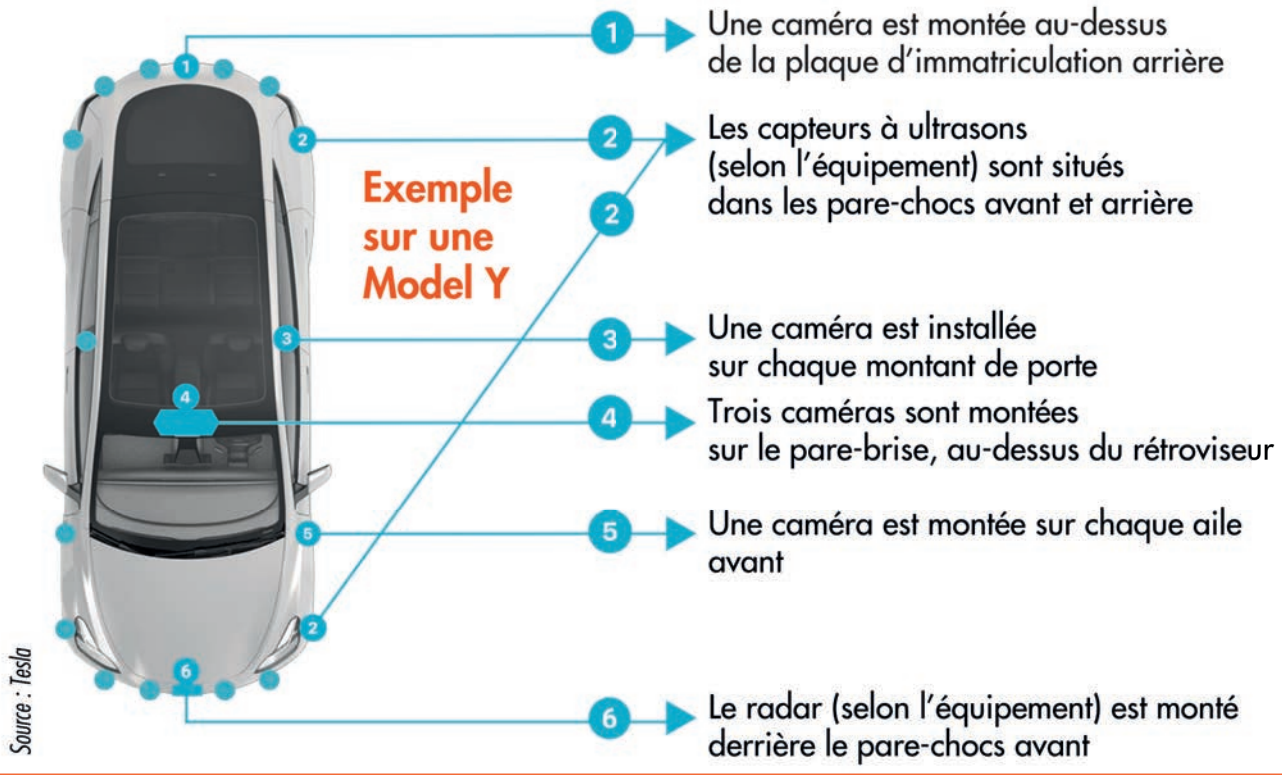
IL SEMBLE QUE QUEL QUE SOIT L'ENDROIT OÙ L'ON SE REND AUJOURD'HUI, ON EST ENREGISTRÉS OU SURVEILLÉS SANS LA MOINDRE IDÉE DE COMMENT CES IMAGES SONT EXPLOITÉES

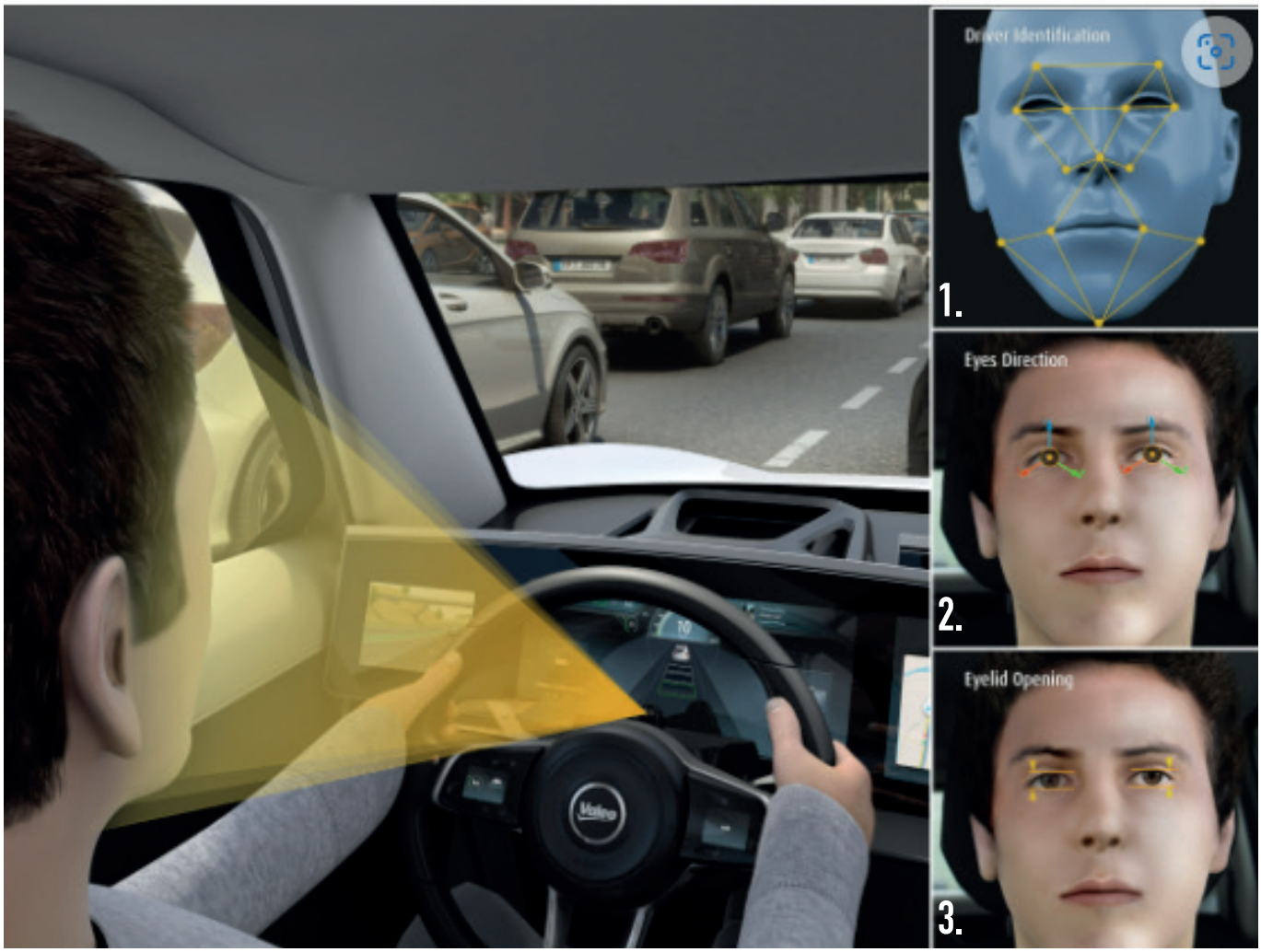
Voilà pour les caméras intérieures. Qui ne sont que peu de choses à côté des caméras extérieures. BMW appelle par exemple cela le système « *Advanced Car Eye* » : une caméra surveille tout ce qui se passe aux abords du véhicule et enregistre le moindre fait qui lui semble anormal. Le propriétaire de la BMW peut ensuite regarder tout cela sur son smartphone ! C'est cependant une nouvelle fois chez Tesla que la caméra extérieure est élevée au rang d'art. Avec le mode « sentinelle », un œil scrute en permanence tout ce qui se passe autour de la voiture, à l'image du système de BMW. Mais les Tesla possèdent des caméras tellement perfectionnées que celles-ci permettent d'identifier des personnes qui se trouvent à plusieurs mètres de la voiture. Ces images sont censées ne jamais sortir du véhicule, sauf en cas de nécessité absolue. Or, en avril 2023, un mini-scandale a été dévoilé aux États-Unis. Neuf anciens employés de Tesla se seraient amusés, entre 2019 et 2022, à collecter des images issues des caméras sentinelles pour n'en garder que des morceaux choisis : un homme qui arrive tout nu jusqu'à sa Tesla, l'intérieur du garage personnel d'Elon Musk, mais aussi, beaucoup plus grave, les images d'un enfant renversé… Comme la définition des images est plutôt bonne, la police fédérale américaine avoue même utiliser régulièrement des images issues des Tesla environnantes lorsqu'un méfait est commis. Cela aurait déjà permis d'identifier des malfrats ! Ces images captées par les caméras en mode sentinelle ont mené l'association de défense des consommateurs allemands VZB à porter plainte en 2022. Celle-ci considère en effet, à juste titre, que puisque tout le monde est filmé par une Tesla, il convient donc de recueillir le consentement écrit de chacun. Pas naïve, l'association fait remarquer que pour que les Tesla aient été homologuées en Allemagne malgré des dispositifs embarqués non conformes à sa législation, c'est la preuve de sérieux dysfonctionnements administratifs !

Le tableau ne serait toutefois pas complet sans parler de la nouvelle mode des « dashcams », c'est-à-dire des caméras de tableau de bord. Celles-ci, généralement fixées contre le pare-brise, permettent de déterminer les responsabilités lors d'une collision. La chaine de centres autos Autobacs en a fait la promotion récemment : « *Le nombre de conducteurs équipés d'une dashcam a plus que doublé par rapport à 2020 et est désormais supérieur à 70 000* », se satisfait le groupe japonais. « *Certains modèles ont aussi des modes de surveillance en stationnement, bien pratiques pour protéger le véhicule, y compris en l'absence de son propriétaire* ». Imparable !

Le non-respect chronique de la vie privée des gens par les caméras embarquées risque hélas d'encourager des comportements délictueux. Un site Internet de propagande anarchiste encourage désormais à s'en prendre aux Tesla en France. Pour ce faire, il a même édité une « note d'attaque », afin que l'assaillant sache opportunément cacher son visage aux caméras lors d'un raid sur une Tesla…

COMMENT TESLA ÉPIE SON ENVIRONNEMENT (PAS SI) IMMÉDIAT





© Volvo

Depuis le tableau de bord, une caméra scanne littéralement votre visage et « mesure » votre degré de concentration ou d'éveil.

1. Identification du conducteur
2. Orientation des yeux
3. Ouverture des yeux

C. Après le flicage, l'espionnage ?

Le président des États-Unis Joe Biden aime les *muscle cars* et l'odeur de la gomme brûlée : normal pour ce fils de concessionnaire qui a baigné dans l'automobile dès l'enfance. L'auto est donc un dossier de prédilection pour le président, qui peut se targuer de faire partie des rares chefs d'État à y entendre quelque chose. Il n'est donc pas étonnant que l'alerte soit directement venue de la Maison-Blanche : « *La Chine est déterminée à dominer l'avenir du marché de l'automobile, notamment en recourant à des pratiques déloyales* », a fait savoir le président démocrate dans un communiqué. La secrétaire au Commerce Gina Raimondo se fait plus précise en février 2024 : « *Ces véhicules sont connectés à Internet. Ils collectent d'énormes quantités de données sensibles sur les conducteurs –informations personnelles, informations biométriques, déplacements de la voiture [...] Il ne faut pas beaucoup d'imagination pour comprendre comment un pays adversaire comme la Chine, ayant accès à ce type d'informations à grande échelle, pourrait représenter un risque sérieux pour notre sécurité nationale et la vie privée des citoyens américains* », fait-elle alors savoir à la presse. Gina Raimondo enfonce le clou : « *Imaginez qu'il y ait des milliers ou des centaines de milliers de véhicules connectés en Chine sur les routes américaines qui pourraient être immédiatement et simultanément mis hors service par quelqu'un à Pékin* ». Cette situation, « *effrayante* » pour la secrétaire au Commerce, pose de vrais problèmes « *en matière d'espionnage* », insiste-t-elle encore.

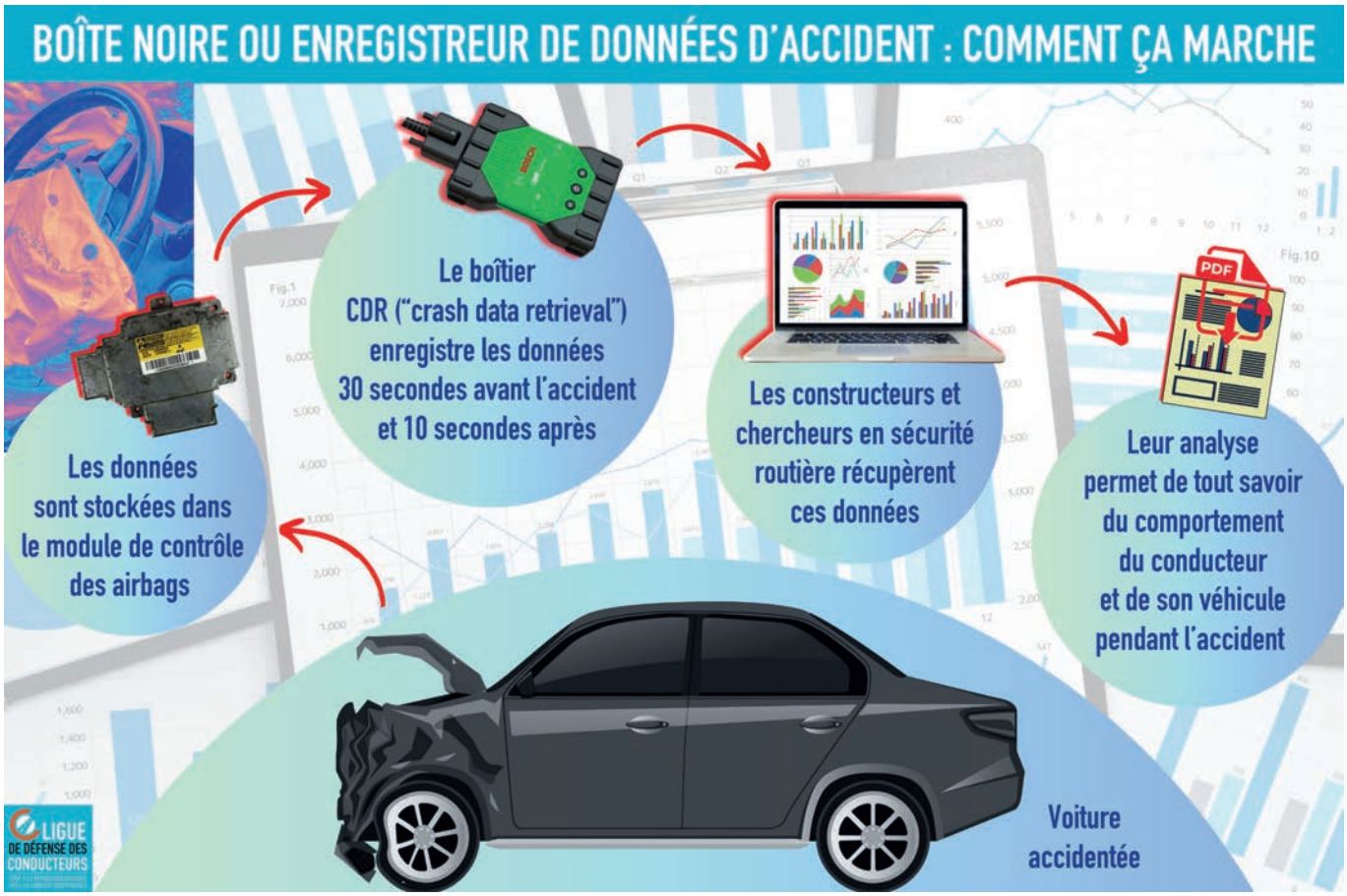
Si l'offensive de Joe Biden a sans doute une visée économique plus que sécuritaire (il s'agit surtout d'enrayer les ventes de voitures chinoises, qui se font au détriment des américaines), le président voit tout de même juste. Les modèles chinois de dernière génération sont effectivement capables de tout voir et entendre, à l'image des Tesla. D'ailleurs, en Chine, les voitures de la marque américaine sont interdites de circulation sur certains sites gouvernementaux ou militaires : elles seraient bien trop curieuses ! Joe Biden ne fait donc que confirmer que dans un pays comme dans l'autre, les soupçons sont fondés.

D. Les mouchards que sont les cartes SIM et les EDR

Quasiment toutes les voitures récentes sont géolocalisées. Ce qui ne signifie pas que toutes le sont régulièrement, loin de là même : le traitement des données coûte cher, il convient donc de tracer les véhicules pour une bonne raison. Le dispositif « eCall » en est un bon exemple : devenu obligatoire en avril 2018, ce service d'appel d'urgence se déclenche automatiquement s'il détecte un accident grave via le déploiement des airbags et appelle le 112 (numéro européen d'urgence). BMW et Stellantis (ex-PSA) avaient pris de l'avance sur le sujet, dotant leurs modèles de ce système dès 2004 pour le premier et 2007 pour le second. Qui dit appel d'urgence en série dit présence d'une carte Sim à bord, à l'image de celle présente dans les téléphones. Ce qui constitue une véritable chance pour les services de police. Habitués à réaliser des « fadettes », c'est-à-dire des relevés d'appels téléphoniques pour confondre des suspects, la police peut en réaliser pour des voitures, désormais. À l'image d'un téléphone, une voiture avec une carte Sim envoie en effet régulièrement ses informations à son opérateur. Les forces de l'ordre réalisent donc d'ores et déjà des fadettes issues des données d'un véhicule pour prouver qu'il a démarré à telle heure, à tel endroit !

Un nouveau mouchard est en outre apparu dans les voitures européennes. Il s'agit de l'EDR, pour « *Event data recorder* » ou enregistreur d'événements (c'est-à-dire de données d'accident). Assimilé à une boite noire, ce système est obligatoirement monté de série sur tous les véhicules neufs depuis juillet 2024. L'EDR ne fonctionne pas en permanence : l'enregistrement des données, générées en continu, ne se déclenche en effet que si une accélération ou un freinage considérés comme trop brutaux sont détectés. En règle générale, l'EDR « retient » les 30 secondes précédant un impact et les 10 secondes suivantes. L'EDR peut aussi se mettre en service si un prétensionneur de ceinture ou un airbag déclenche sa mise à feu. Et qu'est-ce qui est enregistré par l'EDR ? Absolument tout : état d'enfoncement de la pédale d'accélérateur, position de l'auto sur la chaussée, roulis du véhicule, présence des phares ou pas… : « *Les données aideront à mieux comprendre dans quelles circonstances se déroulent les accidents et les blessures et, ainsi, faciliteront la conception de véhicules plus sûrs* », indique le règlement de l'ONU, à l'origine de cette prescription à laquelle l'Europe s'est conformée. Selon la version officielle, ces EDR ne seraient donc consultés que par les constructeurs et autres chercheurs en sécurité routière. Il apparaitrait qu'à ce jour, la police suisse, par exemple, n'hésite pourtant pas à saisir les EDR et à les faire parler, lorsqu'un grave accident de la route survient.

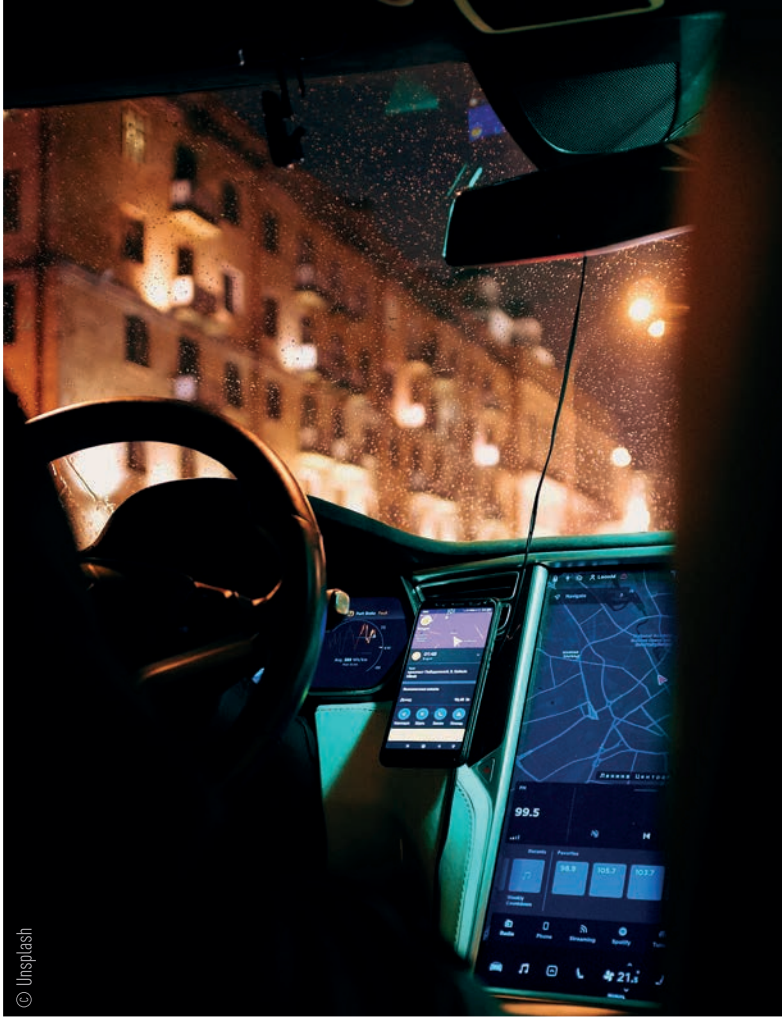
Une telle pratique n'est sans doute qu'une question de temps en France : « *La collecte [ndlr, des données] n'a qu'un objectif de statistiques, même si nous pensons qu'il s'agit en réalité d'une simple étape* », considère l'avocat Michel Benezra. Même la Commission nationale de l'information et des libertés (CNIL) n'est pas dupe, promettant de rester « *attentive au déploiement de ces dispositifs, notamment au regard des impacts qu'ils sont susceptibles d'avoir sur les droits*



TOUTES CES DONNÉES SONT RECUEILLIES PAR LE BIAIS DE CAPTEURS, DE MICROS, DE CAMÉRAS MAIS AUSSI PAR LES TÉLÉPHONES ET LES APPAREILS CONNECTÉS AUX VÉHICULES

et libertés des personnes ». L'avocat Laurent Benaiteau considère, lui, qu'il est « *parfaitement loisible d'imaginer que les officiers ou agents judiciaires, mais aussi les experts judiciaires ou la justice, pourraient rechercher les informations contenues dans l'EDR avec l'autorisation expresse du propriétaire du véhicule à des fins d'enquête judiciaire* ».

N'oublions pas enfin que même en cas d'absence de carte Sim ou d'EDR, il est toujours possible de tracer la voiture dès lors qu'un smartphone est embarqué : « *Google Maps suit l'emplacement des smartphones des usagers de la route afin de déterminer où le trafic se densifie* », rappelle un article publié par le journal quotidien belge *L'Écho*, en septembre 2021. Les chercheurs de la fondation Mozilla, qui se sont penchés sur la manière dont les voitures modernes espionnent leurs occupants dans le cadre d'une étude de septembre 2023 (*voir page 13*), s'en étaient aperçus ; selon l'une de leurs conclusions, « *toutes ces données sont recueillies par le biais de capteurs, de micros, de caméras mais aussi par les téléphones et les appareils connectés aux véhicules.* »


© Unsplash

II. DU FLICAGE POUR GÉNÉRER DE NOUVEAUX REVENUS

A. Maintenance « *over-the-air* » et options à la demande pour les constructeurs

L'Association nationale pour la formation automobile (Anfa) s'en enthousiasmait déjà en 2019 : « *Dans quelque temps, quand le véhicule arrivera sur le parking, on connaîtra grâce aux boitiers télématiques le kilométrage, les codes défaut. C'est demain.* » La maintenance à distance, appelée « *over-the-air* » ou encore « OTA », est une pratique qui tend de plus en plus à se démocratiser dans l'automobile. Le fer de lance en est une nouvelle fois Tesla, qui réalise bien des modifications sur les véhicules sans que leurs propriétaires ne soient contraints de passer par l'atelier. D'après un recensement effectué par la NHTSA (l'agence fédérale américaine chargée de la Sécurité routière) entre janvier 2020 et février 2022, ce sont sept campagnes de rappel sur 19 que Tesla a intégralement réalisées par une maintenance OTA aux États-Unis. Le cabinet spécialisé en études de marché Jato a pour sa part évalué le nombre de véhicules en capacité d'être maintenus à distance en Allemagne en 2022 : 34 % d'entre eux le sont. Des BMW d'abord (55 modèles adaptés au moment de la rédaction de cette étude), mais aussi des Mercedes (34 modèles), des Renault (24 modèles) et des Jaguar (21 modèles) : « *Seuls 55 % des modèles électriques proposent des accès OTA. Mais cela évoluera sans doute prochainement. On peut s'attendre à ce que les fabricants gagnent beaucoup d'argent avec les services supplémentaires qu'ils envoient par OTA. L'industrie de la téléphonie mobile a ouvert la voie dans ce domaine* », explique Jato. L'affaire n'a en effet pas traîné : « *Chez Volkswagen, à partir des millésimes 2020, les systèmes de GPS et d'info-trafic se remettent en temps réel à jour en OTA* », indique un article de *L'Automobile Magazine* de fin 2022. Volvo ne serait pas en reste, à l'instar de bien d'autres marques.

Assurer la maintenance d'un véhicule à distance est en soi une avancée pour l'automobiliste. Cela lui permet d'économiser du temps, pas forcément de l'argent puisque les changements de pièces ou de fluides ne peuvent être réalisés de cette manière. Mais le souci de cette pratique est qu'elle repose d'abord et avant tout sur une identification du véhicule et de son utilisateur : l'auto doit être dans une zone couverte par Internet, le propriétaire doit valider manuellement, depuis sa planche de bord, l'acceptation de la mise à jour : identité du conducteur, paramètres de conduite du véhicule et autres données censées ne pas être accessibles librement peuvent être « aspirés » par le constructeur à chaque opération « OTA ». Ce qui ouvre aussi la voie au hacking, c'est-à-dire au vol de données tant redouté aujourd'hui : « *À partir du moment où les données vont circuler, les*

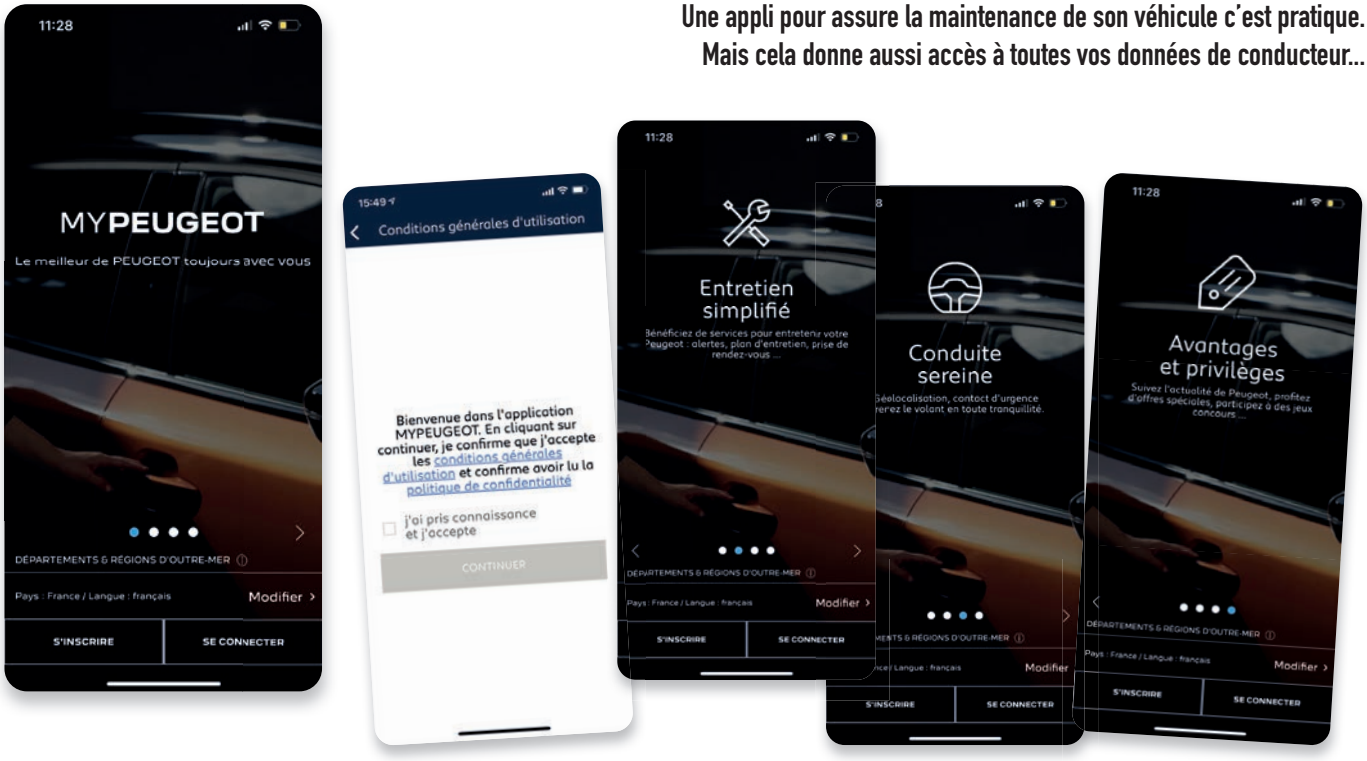
risques de piratage vont se multiplier : risques d'intrusion électronique dans le système du véhicule, risque de prise de contrôle à distance du véhicule connecté [...], r*isque de récupération illégale des données de l'utilisateur du véhicule et dans un second temps, usurpation d'identité pour réclamer l'accès aux données générées par le véhicule* », observe à ce sujet le cabinet DS Avocats, spécialiste du droit des affaires. Il serait possible de considérer que ces aléas constituent « un mal pour un bien », puisque l'OTA est un progrès indiscutable. Hélas, rien n'est gratuit avec les constructeurs d'automobiles. Si les mises à jour OTA ont été inventées, c'est d'abord pour pouvoir proposer de nouvelles fonctionnalités payantes à bord des voitures : celles-ci deviennent progressivement un nouveau lieu de consommation de services. L'article de *L'Automobile Magazine* cité plus haut le suggérait : d'après l'un des ingénieurs de BMW France, « *on peut rajouter des petites fonctions* » à l'occasion d'une mise à jour à distance.

Ces « *petites fonctions* » s'appellent en réalité des options à la demande. Un volant chauffant sur votre BMW ? Ce sera 15 € par mois. Une direction de l'essieu arrière avec grand angle de braquage sur votre Mercedes ? 489 € par an. Un mode « *sentinelle* » pour espionner le voisinage grâce à votre Tesla ? Payant aussi ! La liste est quasiment infinie, tant la diversité des services proposés dépasse quelquefois l'entendement. L'objectif final des constructeurs : plutôt que proposer un catalogue d'options lors de l'achat d'une voiture neuve, pourquoi ne pas plutôt fabriquer cette dernière avec toutes les options déjà intégrées... mais en ne les activant qu'à la condition de s'abonner, pour un montant et une durée bien définis ? Ainsi, si le premier propriétaire du véhicule ne débloque aucune option, peut-être le second en activera-t-il trois ou quatre, assurant un revenu additionnel pour le constructeur, bien après la vente du modèle neuf.

Le groupe Stellantis (ex-PSA), avec ses nombreuses marques (Peugeot, Citroën, DS, Fiat, Opel, Alfa Romeo, Jeep...), ne s'en cache pas : « *Les offres produits et abonnements basés sur les softwares devraient générer des revenus d'environ 4 milliards d'euros d'ici 2026 et d'environ 20 milliards d'euros d'ici 2030* », explique son communiqué de presse de décembre 2021, précisant que « *34 millions de voitures connectées monétisables sont attendues d'ici 2030* ». Mais pour que les voitures soient « monétisables », pour que l'automobiliste accepte docilement de remettre la main au portefeuille alors qu'avant, il réglait sa facture une bonne fois pour toutes, il faut connaître ses habitudes, ses goûts et ses envies. Bref, le surveiller et interagir avec lui le plus souvent possible. Il se trouve que d'après KPMG, « *les clients français font partie des plus importants consommateurs de services connectés en Europe.* » Le cabinet de conseil, qui estime notre parc national de véhicules connectés à 10,7 millions d'unités, souligne notre forte appétence pour ces petits « à-côtés » : « *82 % des Français bénéficiant d'un véhicule connecté consomment des services associés, dépassant Allemands, Britanniques et Américains* ». Une aubaine !

Payer pour un service ou accepter de voir son véhicule être maintenu à distance ne donne toutefois pas un blanc-seing à la pratique de l'espionnage. L'Association nationale pour la formation automobile (Anfa) avait interrogé 3 350 automobilistes européens en 2020, à l'occasion de la réalisation de son étude « *Après-vente connectée des véhicules légers* ». Il en ressortait que 79 % des personnes sondées étaient tout à fait prêtes à partager les informations liées à leur véhicule. Elles n'étaient plus que 16 % à accepter de mettre à disposition leurs données personnelles, tandis que 18 % des automobilistes interrogés ne souhaitaient partager aucune information de quelque nature que ce soit avec un tiers.

Une appli pour assure la maintenance de son véhicule c'est pratique. Mais cela donne aussi accès à toutes vos données de conducteur...



B. Quand la transgression des règles règne en maître

Impossible de ne pas parler d'espionnage pur et simple à la lecture du rapport de la fondation Mozilla, sorti en septembre 2023. Décortiquant les pratiques de 25 marques automobiles, cet organisme à but non lucratif américain dénonce alors « *la pire catégorie de produits en matière de respect de la vie privée que nous ayons étudiée* ». Pourquoi ? « *Toutes les marques collectent plus de données que nécessaire* », ce qui n'est guère une surprise. « *Elles peuvent collecter des informations super intimes vous concernant : informations d'ordre médical, préférences sexuelles, à quel point vous roulez vite, où vous roulez, quelles sont les musiques que vous aimez écouter* », détaille Mozilla, pour qui Tesla est évidemment un modèle en matière de non-respect de la vie privée. Nissan ne serait pas en reste, la fondation expliquant que cette marque se renseigne consciencieusement... sur les activités sexuelles de ses clients. Idem pour Kia, tandis que Hyundai, de son côté, assume le fait de livrer les données personnelles de ses utilisateurs aux forces de l'ordre comme aux gouvernants. Enfin, une enquête du journal américain *The Washington Post* (« *California privacy regulator's first case: probing internet-connected cars* », 30 juillet 2023) révèle que lorsqu'un téléphone portable est en mode « mains libres » à bord d'une auto, divers constructeurs se permettraient d'aspirer son contenu : carnet d'adresses, coups de fils passés, photos personnelles... Nos smartphones s'avèrent donc de précieux compléments aux capteurs et micros qui pullulent déjà dans nos voitures modernes.

Officiellement, le respect de la vie privée des clients est une priorité absolue pour les constructeurs. Une assertion vite mise à mal lorsque l'on s'y intéresse de près. Dans un document intitulé « *Information sur la protection de vos données personnelles* », Renault, par exemple, fait savoir qu'il recueille déjà les données de géolocalisation de ses clients, tout en précisant : « *Votre consentement est recueilli lorsque la règlementation nous l'impose* ». D'après le constructeur, « *nous pouvons, dans certains cas, partager vos données personnelles avec des partenaires qui les utiliseront pour leurs propres finalités [...]. Nous nous assurons de vous demander votre consentement à ce partage lorsque la règlementation l'exige, ou à tout le moins de vous permettre de vous y opposer* ». La marque au Losange précise un peu plus loin qu'elle s'arroge aussi le droit de livrer vos données personnelles à des entreprises situées en dehors de l'Union européenne. Faisant fi à ce moment-là de toute la réglementation de l'UE et de votre opposition potentielle !

Comme le veut la réglementation française, il est possible de demander à un constructeur son propre relevé de données personnelles ; ce qui a été fait auprès de Renault pour les besoins de cette présente étude. Le client peut ainsi y apprendre plein de choses. Par exemple, que l'auteur de ces lignes a donné son consentement pour recevoir les offres de Mobilize Financial Services (ex-Diac, filiale de Renault), ce qui est faux ; que les données livrées à un concessionnaire ou à un agent Renault pour réaliser une carte grise peuvent être gardées pendant 5 ans ; que chacun est soumis à un « *profilage marketing* » afin de réaliser une « *segmentation personne* ». Plus fort encore, les « *scores d'appétence* ». L'auteur de cette étude apprend donc qu'il a un goût très prononcé pour l'hybride (8/10), mais quasi-nul pour le véhicule électrique (1/10), alors que son appétence au renouvellement de son auto est plutôt élevée (7/10). Ce tissu d'inepties pourrait prêter à sourire si le rapport envoyé par Renault ne comportait toutefois pas une donnée qui pose question : en effet, le constructeur a pris connaissance de la marque, du modèle et du numéro de châssis d'une voiture possédée et revendue par l'auteur voilà près de dix ans. L'auto avait effectivement effectué un passage dans un garage qui n'arborait pas encore le panneau Renault à l'époque. Ce qui signifie donc que lorsqu'un garage indépendant intègre le réseau du constructeur, ce dernier s'approprie l'intégralité de la base de données clients, quand bien même ces données seraient anciennes ou n'auraient rien à voir avec Renault de près ou de loin. Le but recherché est d'établir des bases de données de personnes « contactables » : elles sont 21,6 millions à la fin 2023 pour Renault, dont 13,5 millions de prospects...

LORSQU'UN GARAGE INDÉPENDANT INTÈGRE LE RÉSEAU DU CONSTRUCTEUR, CE DERNIER S'APPROPRIE L'INTÉGRALITÉ DE LA BASE DE DONNÉES CLIENTS

C. La juteuse revente de la donnée déjà intégrée dans le business plan des constructeurs

Quoi de plus simple que de se faire de l'argent en revendant des informations qui ne vous appartiennent pas ? Les constructeurs automobiles n'ont absolument aucune pudeur ni retenue sur le sujet. Renault, comme vu plus haut, sollicitera les intéressés « *lorsque la réglementation l'exige* », ce qui signifie donc le moins souvent possible, voire sans doute pas du tout. Stellantis, lui, explique à qui veut l'entendre qu'il gagnera bientôt des milliards grâce aux données, sa filiale Mobilisights créée début 2023 ayant pour mission de s'assurer de « *distribuer sous licence ces data à un large éventail de clients, y compris à d'autres constructeurs automobiles* ». Pour ce faire, le groupe franco-italo-américain « *exploitera pleinement les data des 34 millions de véhicules connectés dont l'entreprise disposera à la fin de la décennie* ». Mais que l'on se « rassure ». Stellantis « *utilisera notamment des data anonymisées et agrégées* », tandis que « *le partage des données personnelles des clients se fera uniquement avec leur consentement.* »

Si les constructeurs sont aussi pressés de récupérer les fichiers clients

VOS DONNÉES, UNE MINE D'OR QUE TOUT LE MONDE VEUT EXPLOITER

Le Data Act européen (en français, « Règlement sur les données »), entré en vigueur fin janvier 2024, entérine la possibilité pour les utilisateurs d'appareils connectés « *d'accéder aux données qu'ils ont contribué à créer* » (*Contexte, 10 novembre 2023*). En clair, cela veut dire que les constructeurs, les seuls à disposer d'un accès direct à vos informations, sont désormais tenus d'ouvrir leurs serveurs à d'autres entreprises, contre « *compensation raisonnable* ». Un premier pas pour les milliers de sociétés qui attendent vos données de pied ferme, alléchées par les perspectives de business… Mais dans un article publié le 8 mai 2024, intitulé « *Bras de fer pour l'accès aux données automobiles* », le média incyber.org (spécialisé dans la confiance numérique) relève que si les constructeurs s'avèrent satisfaits, les centres de réparation et d'entretien, notamment, s'estiment toujours lésés. « *Les constructeurs ont toujours selon eux la possibilité de verrouiller l'accès aux données de leurs modèles connectés, en « imposant » la signature d'un contrat faisant d'eux les seuls destinataires des données du véhicule pour accéder à son interface, et plus généralement d'imposer leurs conditions dans ce marché* », est-il précisé dans l'article. Les assureurs, évidemment, sont solidaires de cette démarche (*voir ci-après*). Les pouvoirs publics, eux, ont obtenu de pouvoir accéder à ces informations « *en cas de circonstances exceptionnelles* », notamment pour répondre à une urgence publique… qui reste à définir. La bataille pour exploiter vos données, malgré le Data Act, fait donc toujours rage.

© Illustration LDC

de leurs réseaux de distribution, c'est pour les revendre à des sociétés comme l'allemand Caruso, par exemple, spécialiste de l'exploitation des données. Le 30 août 2023, Renault et Caruso ont fait connaître l'accord qu'ils venaient de signer. Caruso va ainsi pouvoir bénéficier des données de kilométrage et de géolocalisation de toutes les Renault ou presque, mises en circulation depuis 2021. Le site Internet de Caruso précise même qu'à partir d'un abonnement à 1 500 € par an, il est possible d'avoir accès « *à des données internes de véhicules multimarque pour un usage productif* ».

Mais alors que Caruso est une société de droit allemand, son concurrent Otonomo est pour sa part une entreprise israélienne : elle échappe donc à la législation de l'Union européenne dans tous les domaines : « *Avec Otonomo, plus de 100 fournisseurs des secteurs du transport, de la mobilité, de l'assurance et de l'automobile sont enfin en mesure d'exploiter les données et les informations relatives à la mobilité et de les transformer en atouts stratégiques et en avantages commerciaux* », annonce la société. Et qui sont ces 100 fournisseurs ? Avis, BMW, Stellantis, Daimler (Mercedes-Benz), Mitsubishi, Renault, etc.

Les différents constructeurs automobiles pourraient aussi aisément revendre les données de géolocalisation à une société comme The Ulysses Group. Cette entreprise américaine, visiblement montée par d'anciens membres de l'armée, se dit aujourd'hui capable de géolocaliser les véhicules « *dans presque tous les pays sauf en Corée du Nord et à Cuba* ». The Ulysses Group pourrait suivre 15 milliards de points de géolocalisation par mois, et se félicite aussi de la connectivité galopante des voitures modernes. Selon son propos, celles-ci ne cesseraient de livrer leur position, ce qui est un bienfait pour tous les militaires.

Les préoccupations des constructeurs devraient cependant demeurer nettement plus terre à terre. Les données des clients servent en premier lieu à proposer des offres d'assurance. Renault, via sa filiale Mobilize, a déjà lancé sa propre couverture « *Pay as you drive* » (« Payez pour ce que vous conduisez », autrement dit, le montant de votre prime est modulé selon la distance parcourue) avec l'assureur espagnol Mapfre, dans la péninsule ibérique. Il est évidemment demandé aux clients souscripteurs de bien laisser leur téléphone branché en Bluetooth lorsqu'ils roulent, afin que le constructeur (ou l'assureur) puisse consciencieusement en siphonner le contenu.

D. Les assureurs en embuscade

Alors que les assureurs maison des constructeurs ont déjà accès aux data, les « indépendants » tannent l'Europe pour qu'elle « lâche le frein à main » sur la libéralisation des données. Il en irait même de l'intérêt public, à en croire la missive du 14 décembre 2023 : « *Une action urgente est nécessaire pour une législation en faveur des consommateurs et de la concurrence sur l'accès aux données embarquées des véhicules* », ont fait savoir Insurance Europe (l'entité qui porte la voix des assureurs) et d'autres à la Commission européenne. Pourquoi une telle urgence ? « *Une étude de la fédération internationale de l'automobile Région 1 Europe a révélé qu'en l'absence de cadre réglementaire en Union européenne offrant l'égalité d'accès aux données du véhicule, les pertes pour le marché indépendant de l'après-vente automobile […] s'élèveraient à 26 milliards d'euros d'ici à 2030 et à 95 milliards d'euros d'ici à 2050* », écrivent les signataires, toute honte bue. Il serait

donc intolérable que Bruxelles tente, par sa lenteur, de protéger les consommateurs, alors qu'il sera demain possible de leur faire payer davantage ! Et qu'on se le dise : « *Plus de retard ne porterait pas seulement préjudice aux services basés sur la prise OBD, mais aussi au développement des nouvelles mises à jour over-the-air* », annoncent encore les signataires de la lettre (*voir page 11*).

Afin de créer des systèmes de tarification au plus près des habitudes du client – le fameux « *Pay as you drive* », voir plus haut –, les assureurs ont en effet besoin de connaître tous les paramètres de sa conduite. Comme le système « Youdrive », de Direct Assurance, par exemple : un rapport d'analyse est envoyé à l'utilisateur après chaque trajet. Celui-ci porte sur cinq indicateurs : accélération, freinage, virages, allure et distance parcourue. « *Votre vitesse moyenne est comparée à celle du trafic en temps réel* », prévient Direct Assurance. Un assureur concurrent propose les mêmes paramètres d'évaluation pour tarifier son offre, mais y ajoute les « *horaires de conduite* », ainsi que « *le nombre de pauses pendant de longs trajets* ». Aux États-Unis, l'incontournable Tesla a décidé de créer sa propre offre d'assurance. Celle-ci n'est d'ailleurs pas accessible en Californie, en raison de la protectrice loi sur la récupération des données clients. Mais dans les autres États, l'offre Tesla se base sur tous les paramètres déjà annoncés, en y ajoutant le « *suivi de trop près* », ainsi que la « *conduite tard dans la nuit* », c'est-à-dire entre 22 heures et 4 heures du matin. Pourquoi pas, puisqu'ici les clients sont parfaitement au courant de ce pour quoi ils signent.

L'ennui, c'est que les règles du jeu sont rarement respectées. Tesla devrait subir une nouvelle « *class action* » (recours collectif) de l'autre côté de l'Atlantique, à cause de son offre d'assurance (la marque d'Elon Musk venait d'obtenir un délai pour organiser sa défense au moment où nous rédigions cette enquête). Laquelle considère manifestement un peu trop vite que bien des conducteurs mettent de brusques coups de frein, ce qui nuit évidemment à leur score et *in fine*, à leur prime mensuelle. Faut-il donc ne pas éviter les obstacles afin de ne pas payer trop cher son assurance ?

Mais surtout, selon le troisième compte-rendu du « *Club conformité véhicules connectés* » initié par la CNIL, il apparait que « *les acteurs de l'assurance [...] font part de leur préoccupation quant à la rédaction de l'article 8, qui semble signifier que toute utilisation secondaire de la donnée ne peut être qu'anonymisée* ». Car selon un précédent compte-rendu de la CNIL, « *l'anonymisation des données tend à dégrader la qualité et l'intérêt des données* ». La préservation de la vie privée n'est-elle pourtant pas officiellement au cœur des préoccupations des assureurs comme des constructeurs ?

Alors qu'une partie de son *business model* repose sur l'interrogation de boitiers télématiques présents à bord de voitures, le système d'autopartage Ubeeqo a été vertement sanctionné par la CNIL en juillet 2022 : 175 000 euros d'amende lui ont été infligés. Pourquoi ? « *La CNIL a notamment constaté que, au cours de la location d'un véhicule par un particulier, la société collectait des données relatives à la géolocalisation du véhicule loué tous les 500 mètres, lorsque le véhicule était en mouvement, lorsque le moteur s'allumait et se coupait ou encore lorsque les portes s'ouvraient et se fermaient* », précise la Commission, pour qui « *aucune des finalités ne justifie une collecte des données de géolocalisation aussi fine que celle effectuée par la société* ».

LES ASSUREURS NE SERONT-ILS PAS TENTÉS DE COLLECTER DISCRÈTEMENT BIEN PLUS D'INFOS QUE CE DONT ILS ONT BESOIN ?

A l'instar d'Ubeeqo, à l'image des constructeurs pris la main dans le sac par la fondation Mozilla, les assureurs ne seront-ils pas tentés de collecter discrètement bien plus d'infos que ce dont ils ont besoin ? Compte tenu de l'inflation galopante des tarifs d'assurance au cours des derniers mois, il y a fort à parier que ces solutions de tarification basées sur le comportement prendront bientôt leur envol en France. Au détriment du droit à la vie privée de chacun.

Car comme il fallait s'y attendre, les assureurs sont déjà allés trop loin aux États-Unis. Le *New York Times* a publié une enquête à ce sujet en mars 2024. Selon les données que le quotidien a recueillies, General Motors (Chevrolet, Buick, Cadillac...), premier constructeur américain, vend déjà à des tiers les données de ses clients, que ces derniers soient consentants ou non. L'alerte est venue d'un citoyen américain qui ne comprenait pas pourquoi sa prime d'assurance avait brusquement augmenté de 21 %. À force de recherches, un courtier finit par annoncer à cet automobiliste que le montant de sa prime était calculé en fonction du rapport fourni par la société Lexis Nexis, qui agrège des données venues de l'automobile pour les revendre ensuite aux assureurs. Le citoyen malheureux a donc exigé de lire le rapport établi sur son comportement au volant établi par Lexis Nexis. En retour, lui ont été envoyées 258 pages édifiantes, détaillant absolument tout : heures de démarrage et d'extinction de la voiture, trajets effectués, accélérations, freinages... Selon la plainte déposée par l'intéressé en Floride, aucun consentement n'aurait été donné à qui que ce soit pour transmettre les données personnelles. Qu'importe, le système Onstar, imaginé par General Motors, espionne les conducteurs de bonne foi et permet aux constructeurs de s'enrichir en vendant ce qui ne leur appartient pas !

L'affaire ne s'arrête pas là puisqu'au Texas cette fois, en août 2024, le procureur général a lui aussi accusé General Motors d'avoir collecté les données de ses clients depuis 2015, sans vraiment les informer des implications sous-jacentes (revente et exploitation des informations générant des « *scores de conduite* » et permettant aux assureurs d'ajuster leurs primes). L'action touche 14 millions de modèles. Certes, les Chevrolet et Cadillac ne pullulent pas sur nos routes européennes. Mais Opel est concerné, puisqu'avant d'appartenir à Stellantis (ex-PSA), la marque allemande appartenait à ce groupe automobile américain... Parallèlement, Hyundai et Kia font l'objet des mêmes accusations en Californie.

III. LES NOUVELLES TECHNOLOGIES, PRÉCIEUSES ALLIÉES DES FORCES DE L'ORDRE

A. Un budget et des radars qui ne mollissent pas

Les radars automatiques installés en grande pompe par Nicolas Sarkozy en 2003 font plus que jamais partie intégrante du système répressif français. Pour cette année 2024, ce sont 339,64 millions d'euros qui ont été affectés aux « *structures et dispositifs de sécurité routière* », un montant stable par rapport à 2023. Ils sont environ 4 600 à flasher au bord des routes, ce qui constitue un record. En plus des 487 voitures radars banalisées totalement indétectables (dont 223 sont conduites par des opérateurs privés, sachant qu'ils seront une grosse centaine de plus en 2025), auxquelles notre association a d'ailleurs consacré en octobre 2023 un véritable pamphlet intitulé « *Voitures-radars privatisées : le scandaleux détournement de la sécurité routière* » (téléchargeable sur notre site www.ligue-desconducteurs.org), l'État compte cette année sur le déploiement des nouveaux radars urbains. Capables de flasher dans les deux sens de circulation, imaginés pour sanctionner aussi bien le passage à un feu rouge qu'une vitesse excessive, ceux-ci relèvent d'une sophistication toujours grandissante. Laquelle permettra très bientôt aux forces de l'ordre de réaliser un véritable « diagnostic » du conducteur, afin de déceler et de sanctionner la moindre faille de comportement : non-respect du sas vélo, vitesse excessive, etc. Avec, à la clé, l'alléchante perspective de récolter toujours plus de recettes en provenance des amendes routières.

B. Des drones pour surveiller la sécurité routière

Aujourd'hui tristement célèbres pour leur utilité dans les guerres modernes, les drones sont heureusement multitâche. Ils peuvent aussi servir à surveiller ! En région Aquitaine, les CRS qui œuvrent sur la rocade de Bordeaux (Gironde) usent déjà de drones pour visualiser le trafic en temps réel et sanctionner les contrevenants. Dans l'Essonne, ce sont les gendarmes qui n'hésitent pas à sortir leur drone pour dresser des contraventions : « *Ce dispositif efficace sera généralisé partout en France* », promettait la police sur un réseau social en 2019. Cinq ans après il n'en est rien, mais une cellule drone a tout de même été créée au sein de la Gendarmerie nationale.

En Espagne et en Suisse, les forces de l'ordre ont déjà recours aux drones pour surveiller les conducteurs. La France débute...

Une nouvelle fois, ce n'est pas tant le matériel utilisé qui pose problème. Ce sont les dérives qu'il engendre. En septembre 2023, le personnel de l'entreprise municipale de transport de Palma de Majorque (Espagne) s'est en effet ému de l'utilisation des drones effectuée par la DGT, la direction générale du trafic locale : « *La DGT inflige des amendes aux conducteurs pour non-port de la ceinture de sécurité, alors que les bus n'en sont pas équipés* », se sont plaints les chauffeurs, qui se disent « *choqués et indignés* ». Et pour cause ! « *Les chauffeurs concernés ont été photographiés par un drone de la DGT, c'est pourquoi aucun agent n'a pu vérifier sur place l'absence de ceintures de sécurité sur les véhicules* », continuent les malheureux employés. Très fière de ces drones qui sanctionnent en dépit du bon sens, la DGT espagnole a même fait savoir qu'elle envisageait d'acquérir 39 appareils prochainement, car ils remplaceraient opportunément les hélicoptères dans les actions de sécurité routière.

L'usage du drone répressif n'est pas que le seul apanage espagnol ou français. En Suisse aussi, la police cantonale de Thurgovie (au nord du pays) use de son modèle réduit volant pour relever des excès de vitesse. Bientôt la généralisation des drones qui permettent de sévir d'abord, pour éventuellement réfléchir ensuite ?

C. Une vidéoverbalisation devenue aussi banale qu'injuste

Si les drones sont plutôt récents, les caméras de surveillance permettant de vidéoverbaliser ne le sont plus vraiment : « *Depuis la première expérimentation en 2008, plus d'une centaine de municipalités ont eu recours à ce mode de verbalisation qui ne nécessite pas l'interception du conducteur* », se félicite la Sécurité routière. Naturellement en pointe sur un tel dispositif, la mairie de Paris. En décembre 2022, au micro de France Bleu, l'adjoint au maire en charge de la sécurité a fait savoir à quel point il tenait en haute estime ces caméras parfaitement indétectables pour les automobilistes : « *Nous avons la volonté, dès le début de l'année 2023, de doubler notre capacité de vidéoverbalisation. C'est un moyen extrêmement important pour nous de réguler la circulation* », a ainsi fait savoir Nicolas Nordman, ravi d'annoncer un peu plus tard l'installation de 320 caméras sur 64 sites différents. Personne n'a visiblement rien eu à y redire, à l'exception du vice-président des Verts au Conseil de Paris. Celui-ci a juste fait remarquer que « s*ur le plan sécuritaire, cela signifie que c'est autant de gens qui ne sont pas sur le terrain mais affectés derrière des caméras* ». Dans son édition du 18 octobre 2022, *Le Parisien* révélait qu'un tiers des verbalisations routières dans la capitale serait le fait de la vidéoverbalisation, soit environ 280 000 actes en 2021. Gageons que le nombre croissant de caméras va faire exploser ces chiffres !

Or, une nouvelle fois, le problème de la répression par caméra réside dans son côté aveugle et bien souvent injuste, un écueil généralement évité lorsqu'un contrevenant a l'occasion de s'expliquer auprès d'un agent des forces de l'ordre. Le Lecteur automatique des plaques d'immatriculation (Lapi), embarqué dans des Renault Zoé et Peugeot 208 à Paris, sert ainsi à sanctionner le stationnement non-payé. Il agit comme une caméra de vidéosurveillance. En juin 2023, le groupe communiste à la mairie de Paris a fait adopter un vœu tout à fait intéressant : « *Les recettes de stationnement atteignent 342 millions d'euros en 2022. Elles ont quintuplé depuis 2013 [...]. Les recours formulés par les Parisiens explosent à une vitesse encore plus rapide que le nombre d'amendes, ils ont quasiment triplé en 2021. Notons que 64 % des recours donnent lieu à une réponse favorable* », ont écrit les élus. Traduisez : 64 % des amendes – désormais appelées forfaits post-stationnement – dressées par la machine puis contestées, n'étaient pas fondées. Soit quasiment les deux tiers. Belle efficacité ! Sans oublier bien entendu les milliers de citoyens tracassés afin de prouver leur bonne foi, évidemment. Mais il y a pire... En confiant les Zoé/208 à des opérateurs privés, à l'instar de ce qui se déroule aujourd'hui avec les voitures-radars privatisées, la mairie de Paris a mis toutes les chances de son côté pour que cette affaire dérape. Le vœu du groupe communiste ne se prive pas de le rappeler : « *[...] sur les contrôles de stationnement fictifs, la justice a récemment relevé que l'entreprise Streeteo avait eu massivement recours à des contrôles effectués par des agents non-assermentés [...]. Voilà pour la fraude et la logique de rentabilité financière. Cette situation a obligé la ville à rembourser plus de 5 000 contraventions illégales qu'avait infligées Streeteo* ».

Les voitures chargées de sanctionner le stationnement non-payés battent des records d'amendes injustifiées.

D. La vidéoverbalisation pour sanctionner bientôt dans les Zones à faibles émissions

Annoncée depuis plusieurs années désormais, la répression systématique des contrevenants dans les Zones à faibles émissions (ZFE) n'a toujours pas été mise en place. Davantage qu'un souci technique, le problème serait plutôt d'ordre social pour l'exécutif, qui craint un mouvement de rébellion massif des automobilistes dès que les amendes commenceront à pleuvoir. En Grande-Bretagne par exemple, il ne s'est pas passé 48 heures avant que les premières caméras destinées à surveiller les « *low emission zones* » soient dégradées...

Installer des caméras pour surveiller les vignettes Crit'Air reviendrait ainsi à en disposer 200 de plus dans la capitale. Mais c'est à Toulouse, début 2023, qu'a été annoncée la nouvelle : 60 caméras ont été déployées pour surveiller la ZFE et sanctionner les automobilistes propriétaires d'autos jugées trop polluantes : « *L'écologie est le nouveau prétexte pour déployer des caméras de vidéosurveillance et légitimer des politiques répressives* », a fait remarquer l'association La quadrature du net, qui défend les droits et les libertés sur Internet, dans un article de janvier 2023 de *La Dépêche du Midi*.

Sans compter qu'à la Ligue de Défense des Conducteurs, en juin 2023, nous avions mis la main sur un document officiel de la Direction générale des infrastructures, des transports et des mobilités (DGITM), détaillant les six étapes du contrôle automatisé qu'on nous promet... Six étapes où nous avons systématiquement décelé des failles potentielles d'exploitation des données, comme le montre l'illustration page suivante !

E. Les lettres et SMS envoyés aux « mauvais conducteurs » de l'État de Washington

La technologie ne permet pas seulement de surprendre les conducteurs en infraction. Elle permet aussi de les garder en mémoire indéfiniment ! Dans l'État de Washington, au nord-ouest des États-Unis, un « *programme de messagerie personnalisé envoie des courriers et SMS aux automobilistes de la région ayant eu des antécédents d'accidents ou d'infractions au code de la route* », a fait savoir un article du *Washington Post* de juin 2023. Ainsi, bien qu'ils n'aient commis aucune infraction à l'instant T, ce sont 100 000 conducteurs environ qui ont reçu un texte tel que le suivant : « *Quelqu'un dans votre foyer conduit dangereusement* », ou encore « *Votre véhicule a des antécédents d'excès de vitesse* ». Selon l'article du *Washington Post*, l'efficacité de ce genre de pratique serait avérée, à défaut de se révéler courtoise ou sensée aux yeux des citoyens.

Cette volonté de moraliser et de responsabiliser coûte que coûte les automobilistes intéresse aussi quelques assureurs français (*voir par ailleurs page 14*). Grâce aux données télématiques précédemment détaillées, un assureur pourrait tout à fait envoyer des SMS à ses sociétaires, leur expliquant par exemple que tel virage a été pris trop vite, ou qu'il ne s'agit pas d'entrer à vive allure dans les ronds-points. Une mutuelle qui a pignon sur rue ne fait pas mystère qu'elle serait largement prête à franchir le pas !

F. Le système ougandais, une inspiration pour nos pouvoirs publics ?

D'une superficie deux fois inférieure à celle de la France, l'Ouganda, pays anglophone d'Afrique de l'Est, témoigne d'une population conséquente de 47 millions d'habitants. Sur le thème du flicage des conducteurs à haute dose, Human Rights Watch a tiré le signal d'alarme en novembre 2023 : « *En Ouganda, un nouveau système de surveillance utilisant des plaques d'immatriculation de haute technologie permettra au gouvernement de suivre tous les véhicules dans le pays à chaque instant de la journée* », indique l'ONG de défense des droits de l'homme. Selon elle, « *toutes les nouvelles plaques comprennent un gadget équipé d'une carte Sim* », tandis que même les touristes de passage seront tenus d'acquérir ces plaques d'immatriculation de dernière génération. Selon *The Africa Report*, ce système est mis en place pour lutter contre les assassinats et « *les assaillants qui s'échappent souvent à moto* ».

Il n'en reste pas moins que les automobilistes ougandais ont vu le coût moyen de l'immatriculation multiplié par cinq du jour au len-

demain (soit l'équivalent de 175 euros pour une nouvelle plaque, sachant que le revenu mensuel moyen dans le pays s'élève à 76 €, selon le site Donnéesmondiales.com). Et lors de l'immatriculation, il leur est détaillé le prix de l'amende pour un feu rouge grillé, un excès de vitesse, etc.

Certes, l'Ouganda ne se distingue pas par son modèle démocratique, mais nous ne sommes pas dupes. La méthode africaine, au paroxysme de la surveillance des citoyens, pourrait bien inspirer les dirigeants de notre propre pays, où l'on suit déjà les livreurs et les routiers « à la culotte ». N'en doutons pas, nous, conducteurs lambda, sommes les prochains sur la liste.

L'ONG Human Rights Watch alerte sur les dérives du flicage du gouvernement ougandais qui, depuis février 2024, impose des traceurs sur tous les véhicules du pays.
Sa campagne vidéo, sur Youtube, que nous vous traduisons ci-dessous, fait froid dans le dos :

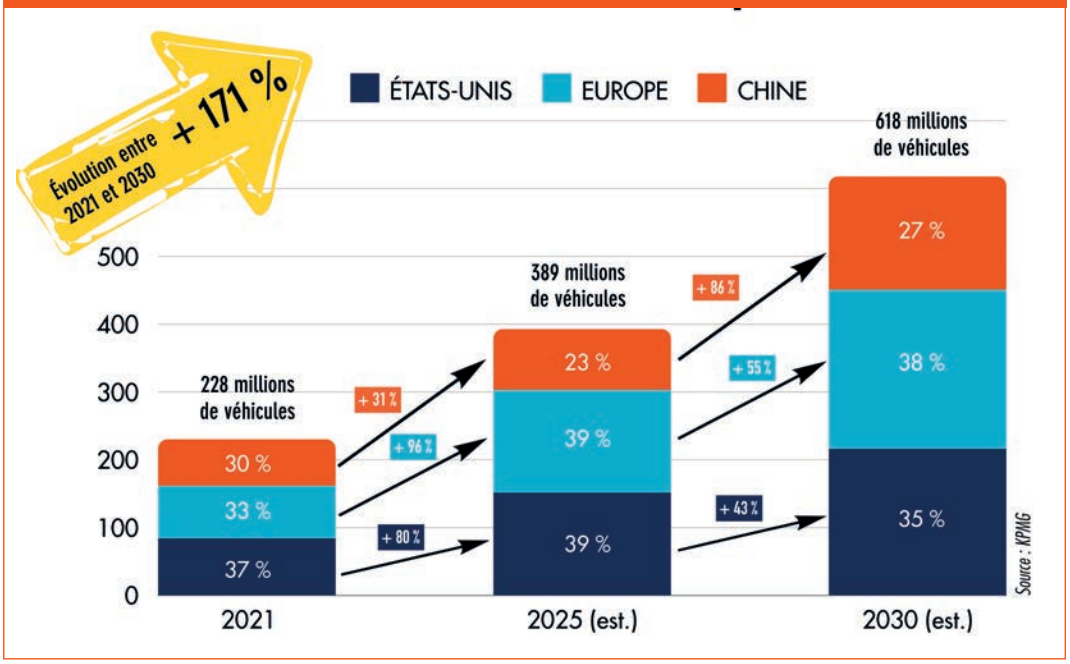
1. « *Et si votre gouvernement traquait systématiquement, en temps réel, la position de votre véhicule ?*
2. *C'est exactement ce que le gouvernement ougandais s'apprête à faire grâce à son nouveau système de surveillance, soi-disant pour lutter contre la criminalité.*
3. *Les traceurs de plaques d'immatriculations peuvent surveiller les usagers dès que l'appareil émet un signal.*
4. *Dès le 1er février 2024, tous les propriétaires de véhicules en Ouganda devront enregistrer de nouvelles plaques d'immatriculation dotées de dispositifs de localisation* »

CONCLUSION

À l'image de ce qui a pu se dérouler à l'occasion du scandale du diesel chez Volkswagen en 2015 – c'est-à-dire un constructeur qui ment à dessein aussi bien aux autorités qu'à ses clients – il ne faut en aucun cas faire confiance aux marques qui promettent de préserver l'intimité de chacun. À mesure que le parc de voitures connectées grossit (à vue d'œil, comme le montre l'infographie ci-dessous), la guerre économique est devenue une réalité et son intensité, particulièrement entre la Chine et le monde occidental d'aujourd'hui, fait que tous les coups sont permis. Nous l'avons vu page 13, la fondation Mozilla a prouvé que tous les constructeurs pillaient les données personnelles des conducteurs sans leur demander leur consentement. L'enquête du *New York Times*, plus récente, n'a fait que corroborer ce qui avait été soulevé par Mozilla. Ces histoires américaines ne doivent surtout pas être regardées de loin par les Français. Ainsi, lorsqu'il précise que « *votre consentement est recueilli lorsque la réglementation nous l'impose* », Renault avoue et prévient qu'il entend faire fi de ce fameux consentement par tous les moyens. À l'image d'une société européenne qui ne paie pas d'impôts en établissant son siège sur une île paradis fiscal, Renault et les autres sont largement capables de traiter les données de leurs clients hors d'Europe, afin de les revendre en toute quiétude au plus offrant.

Outre la « monétisation » de chaque conducteur voulue par les acteurs du monde économique, les forces de l'ordre se réjouissent aussi de l'innovation galopante en matière de caméras *(voir les radars-tourelles, page suivante)*. Grâce à la vidéoverbalisation, un agent seul derrière son écran peut surveiller plusieurs rues en même temps et distribuer amendes à foison : tant pis si le contrevenant avait une bonne excuse pour chevaucher la ligne blanche : le code de la route l'interdit ! Une aubaine pour les finances publiques, qui se porteront mieux avec davantage de recettes issues des amendes routières. Une aubaine aussi pour la police ou la gendarmerie, qui ne parviennent plus à recruter qui que ce soit, tant leurs effectifs sont soumis à une détestable « logique du chiffre » par tous les moyens. Il ne serait donc pas étonnant que demain, l'État choisisse de mettre en place un système proche de ce qui est vu en Ouganda (*voir page 18*) : une puce sur chaque véhicule permettant de le tracer en permanence, tout simplement. Impensable ? Les chauffeurs routiers sont déjà soumis à un traçage permanent de leur comportement via le chronotachygraphe. Les chauffeurs livreurs sont pour la plupart espionnés et tracés par leur employeur en permanence. Il y a donc lieu de penser que l'automobiliste lambda, sous couvert d'amélioration de la sécurité routière ou de sa propre sécurité, sera prochainement soumis au même type de flicage, qu'il soit consentant ou pas. C'est d'ailleurs ce qui ressort de l'interview que Maître

LES VOITURES CONNECTÉES À LA CONQUÊTE DU MONDE

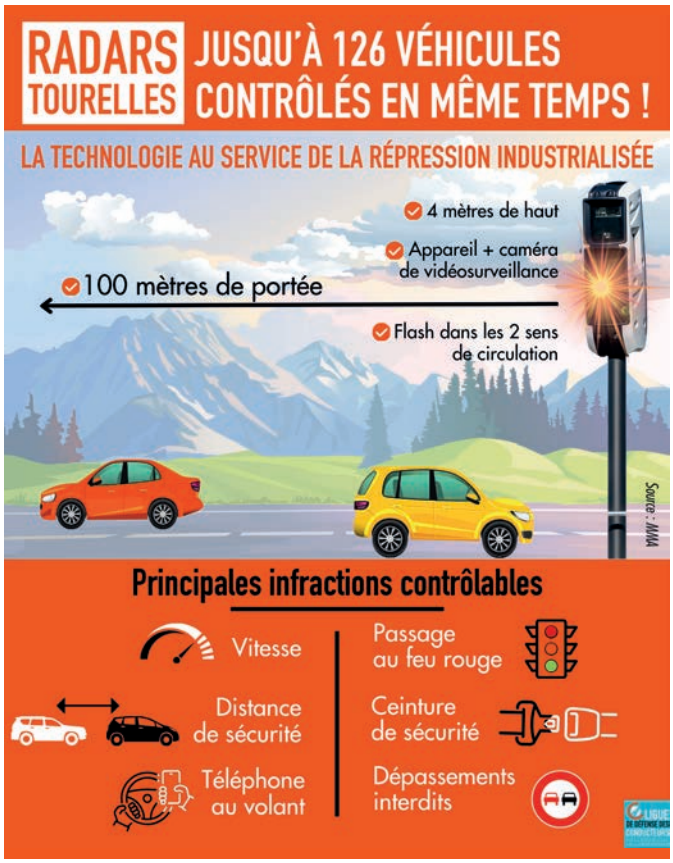


Entre 2021 et 2030, le nombre de voitures connectées dans le monde va bondir de plus de 170 %... et 212 % rien qu'en Europe !

CONCLUSION

Jean-Baptiste Le Dall nous a accordée sur ces vastes sujets, que nous joignons ci-contre à cette conclusion.

Ce que demande la Ligue de Défense des Conducteurs ? Que soient circonscrits tous les risques de dérives que nous avons énumérées dans cette étude. Que l'État se porte garant de la protection de nos données. « *Les sujets liés à la mobilité individuelle se multiplient, notamment concernant la protection des données générées à bord des véhicules connectés. La généralisation de la vidéoverbalisation représente également un véritable sujet de préoccupation pour les automobilistes et les motards qui nous suivent* », écrivions-nous en janvier 2023 à Jean-Noël Barrot, alors ministre délégué chargé de la Transition numérique. Un sujet dont nous lui avions alors proposé de débattre lors d'un entretien… qu'il n'a pas pris le temps de nous accorder. Espérons que les futurs ministres qui lui succéderont se sentiront davantage concernés.



Dans le cadre des élections européennes de juin 2024, nous avions également interpelé les candidats avec la question suivante : « *Selon une étude automobile Lifesearch, les consommateurs français (mais aussi allemands) souhaitent principalement limiter la collecte de données personnelles à la maintenance du véhicule, la possession*

« L'AUTOMOBILE N'EST PLUS L'ESPACE DE LIBERTÉ QUE NOUS AVIONS AUPARAVANT »

Entretien avec Jean-Baptiste Le Dall, avocat spécialiste du droit routier

Ligue de Défense des Conducteurs : Est-il légal, pour un constructeur ou un tiers, de collecter des informations sur l'utilisateur d'une voiture ?

Jean-Baptiste Le Dall : Oui, tout à fait. Chacun peut mettre en place un système de traitement des données personnelles, mais il y a un certain nombre de paramètres à respecter : les personnes dont on traite les données doivent avoir un droit d'accès, savoir comment ces données sont traitées, etc. Les informations traitées ou conservées doivent avoir une légitimité et il doit y avoir quelqu'un au sein de l'entreprise, qui s'occupe de cela. En cas de contrôle de la CNIL, il faut pouvoir justifier de l'intérêt de la collecte de tel et tel paramètre.

LDC : Les automobilistes n'ont donc pas le choix…

JBLD : Beaucoup de consommateurs et d'assurés sont aussi tout à fait d'accord pour payer moins cher avec des systèmes comme le « *pay as you drive* » par exemple, et donc de livrer leurs données liées à la conduite. Le problème c'est qu'au bout d'un moment tout le monde paiera le même prix, sauf celui qui refusera de livrer ses données et qui paiera plus cher. Le consommateur a de moins en moins la possibilité de dire non.

LDC : Depuis juillet 2024, tous les véhicules neufs sont nécessairement pourvus d'un enregistreur de données, soi-disant à des seules fins d'étude. Ne croyez-vous pas que les tribunaux vont bien vite réclamer leur lecture dès qu'il y aura litige ?

JBLD : Avant que techniquement, une juridiction soit capable de mettre le nez dans ce genre d'appareils, il se passera du temps ! Il faudrait que nous soyons calibrés pour le faire en France. Nous ne sommes pas comme aux Etats-Unis où les dommages et intérêts vont servir d'amende, ici, en France, nous sommes sur l'indemnisation d'un préjudice.

LDC : ***Les recours semblent exploser avec la vidéoverbalisation. N'est-ce pas la preuve que le système a été d'abord inventé pour faire de l'argent plutôt que pour rendre service à la collectivité ?***

JBLD : Au départ, Marseille a mis en place la « sulfateuse à PV »

CONCLUSION

avec la Renault Zoé qui contrôle les voitures en stationnement. La CNIL a un peu hurlé, mais il ne s'est rien passé de plus. De là, la mairie de Paris s'est dit « *bon, ok, la CNIL a dit que ce n'était pas bien, mais je vais faire pareil* ». On a donc eu le droit aux Zoé qui circulent 24 heures sur 24 pour sanctionner le moindre dépassement de temps, mais aussi les personnes qui avaient la carte mobilité inclusion par exemple, et qui se faisaient verbaliser dans tous les sens...

LDC : 64 % des recours sur le stationnement sont valables à Paris !
JBLD : C'est délirant. Pendant des années, sur le stationnement payant, nous avons eu un faux semblant qui consistait à dire que l'on faisait payer pour favoriser la rotation en surface. La première fois où l'on a fait tomber les masques, c'est lors de la réforme de la dépénalisation du stationnement, qui a été annoncée dans le cadre du financement des projets du Grand Paris. À cette occasion a été admis que le stationnement payant est une source de revenus pour tout le monde, pour les collectivités, l'État, etc. C'est manipulé pour rapporter le plus d'argent possible et conçu pour que la contestation soit compliquée à mettre en œuvre.

LDC : Nous commençons à avoir des voies réservées sur les routes, avec des caméras qui filment le nombre de passagers à bord. Sans compter les drones, les radars intelligents... L'automobile et la liberté qu'elle incarnait au départ n'ont-elles pas été perverties ?
JBLD : Il faut savoir qu'aujourd'hui, les textes de loi permettent déjà de constater quasiment toutes les infractions avec des radars automatiques. Mais ce n'est pas encore déployé ! Demain, quand cela arrivera vraiment, tout le monde va crier. L'exploitation de clichés ou d'images photographiques avec de l'intelligence artificielle permettra d'aller plus loin dans l'intimité et le flicage du conducteur. Il est clair que l'automobile n'est plus l'espace de liberté que nous avions auparavant.

ENSEMBLE, NOUS DEVONS VEILLER À CE QUE LA TECHNOLOGIE CONTRIBUE EN PRIORITÉ À LA SÉCURITÉ ET AU CONFORT DES CONDUCTEURS, AVANT D'ÊTRE UN OUTIL DE FLICAGE ET DE RÉPRESSION

du véhicule et le comportement de conduire. Or, les voitures connectées, dotées de plus de 200 capteurs et caméras, sont capables de récupérer bien davantage d'informations : vitesse, style de conduite, observation des autres usagers... Comment comptez-vous encadrer l'exploitation de ces données ? Pensez-vous initier des projets de mesures permettant de garantir aux usagers plus de transparence sur l'utilisation de leurs données ? Envisagez-vous d'offrir la possibilité aux conducteurs de refuser de transmettre les données qu'ils ont générées et dont ils sont propriétaires ? Considérez-vous qu'il soit prioritaire de s'assurer à l'échelle européenne que la collecte de données ne se retournera pas contre les conducteurs (système de contrôle des infractions routières, augmentation des primes d'assurance) ? »
Ceux qui ont répondu, quel que soit le bord politique, ont été unanimes : la transparence sur l'utilisation des données, leur protection renforcée, la mise en place d'un consentement explicite avant leur récolte, sont autant de « dossiers » sur lesquels nos nouveaux députés au Parlement de Strasbourg promettent de se pencher.
Reste à voir si leur implication, de même que celle de nos représentants élus à l'échelle nationale, sera suivie d'actions, de règlements, de lois qui sauront mieux nous protéger. À la Ligue de Défense des Conducteurs, nous serons extrêmement vigilants. Tout comme nos sympathisants, toujours prompts à signaler les abus. Sur le sujet des données, comme sur celui de la répression automatisée, nous savons que nous pouvons compter sur eux.

Ligue de Défense des Conducteurs – Novembre 2024
Réalisation : Alexandra Legendre (textes et illustrations), avec Alexandre Lenoir (texte) et l'équipe de la LDC – Delphine Mandeville (direction artistique)

LIGUE DE DÉFENSE DES CONDUCTEURS

STOP À LA RÉPRESSION ABSURDE, OUI À LA CONDUITE RESPONSABLE

Pour rester en contact

Site internet : www.liguedesconducteurs.org

E-mail : contact@liguedesconducteurs.org
Téléphone : 01 43 95 40 20
Adresse : 23 avenue Jean Moulin - 75014 Paris

Retrouvez-nous aussi sur les réseaux sociaux
Facebook - X (ex-Twitter) - LinkedIn - Instagram

NOTRE CHARTE DU CONDUCTEUR RESPONSABLE

Article 1 J'ADAPTE MA CONDUITE à la densité du trafic, à l'état de la route, aux conditions météorologiques et à ma forme du moment.

Article 2 JE NE SUIS PAS SEUL SUR LA ROUTE. Je garde mes distances et vérifie très régulièrement dans mes rétroviseurs que je ne gêne personne ; je me décale largement pour laisser passer ou doubler les deux-roues.

Article 3 JE NE CONDUIS PAS sous l'emprise de substances altérant sensiblement ma vigilance et mes réflexes.

Article 4 J'ENTRETIENS régulièrement mon véhicule pour garantir une sécurité maximale.