

Voitures connectées : les données aux commandes

Sarah Furrer, Tanguy Vaucher, Thomas Delacrétaz

Etudiant-e-s en ingénierie des médias, 1^{ère} année, HEIG-VD

L'industrie automobile a connu une transformation majeure au cours des dernières années. Longtemps considérée comme un simple moyen de transport, la voiture s'impose désormais comme un concentré de technologie, bardée de caméras, de détecteurs et de micros. Autant de dispositifs capables de collecter une quantité fulgurante d'informations privées. Pourtant, la manière dont ces informations sont exploitées reste floue. Surveillance permanente, risques de piratage, et fonctions verrouillées derrière des abonnements, une question s'impose : à qui appartiennent vraiment nos voitures... et nos données ?

UN NOUVEL ELDORADO

100 à 150 millions. C'est le nombre de lignes de codes embarquées dans une Tesla model 3 récente [1].

Les véhicules modernes ne sont plus de simples moyens de transport : ce sont de véritables data centers mobiles. Selon une étude du cabinet KPMG [2-3], les véhicules connectés, majoritaires sur nos routes depuis 2015 [4], génèrent en moyenne 25 giga-octets de données par heure de conduite, soit l'équivalent de 500 heures de musique en streaming. Par ailleurs, de plus en plus d'automobilistes connectent leur téléphone à leur véhicule, ouvrant ainsi aux constructeurs l'accès à bien plus d'informations qu'ils ne le devraient. Selon la fondation Mozilla, 84% des marques automobiles vendent les informations récoltées à des fournisseurs de services, comme des courtiers. De plus, près d'un constructeur sur deux accepterait de collaborer avec les autorités, même sans mandat ou décision de justice [5].

Les informations recueillies concernent d'abord les paramètres techniques du véhicule, comme la vitesse, la position GPS, les habitudes de conduite ou l'utilisation des aides. Mais elles portent aussi sur des aspects plus personnels, tels que les préférences musicales, et parfois même l'état de santé du conducteur [5]. Ces données sont précieuses, car elles peuvent facilement être revendues ou exploitées à des fins commerciales. Pourtant, faire valoir ses droits reste compliqué : seule une minorité de constructeurs permet aux conducteurs d'en refuser l'exploitation. De plus, 68% des marques présentent un mauvais historique en matière de sécurité, avec des fuites, des piratages et des violations de données, causant parfois de véritables préjudices aux automobilistes [5].

LES DÉRIVES DE LA COLLECTE DE DONNÉES

Bien qu'un cadre législatif tel que le Data Act [24] ait été adopté par l'Union européenne en mars 2023, le Parlement européen estime qu'il reste insuffisant pour garantir la protection des utilisateurs. Dans la pratique, les constructeurs automobiles ne

sont aujourd'hui soumis à aucune obligation d'informer les conducteurs sur l'usage réel des informations collectées [25].

À ce manque de transparence s'ajoutent des failles de sécurité préoccupantes. Selon une enquête du média britannique Reuters, Tesla a été impliqué dans une fuite massive : deux anciens employés ont extrait des fichiers concernant plus de 75 000 utilisateurs, en exploitant des réseaux internes mal sécurisés [16]. Entre 2019 et 2022, plusieurs employés de Tesla ont également partagé entre eux des images captées par les caméras embarquées des véhicules, y compris des scènes à caractère intime. Parmi les exemples cités : un homme entièrement nu filmé dans son garage, ou encore la vidéo d'un enfant renversé par une voiture alors qu'il circulait à vélo [16].

Quant à Volkswagen, en janvier 2025, une fuite a rendu accessibles en ligne les données de localisation d'environ 800 000 de leurs véhicules [18].

QU'EN EST-IL EN SUISSE ?

En Suisse, la collecte de données embarquées est déjà une réalité. Depuis juillet 2022, tous les véhicules neufs commercialisés en Suisse et dans l'Union européenne doivent obligatoirement être équipés d'une boîte noire [7]. Ce dispositif enregistre les quelques secondes précédant un accident : vitesse, freinage, accélérations, changements de direction, activation des clignotants, des airbags ou encore des phares [7].

Ces informations ne sont en principe utilisées qu'en cas d'accident, mais d'autres types de systèmes de surveillance commencent à se répandre. En effet, certaines compagnies d'assurance proposent des réductions de primes aux automobilistes qui permettent l'installation de traqueurs plus intrusifs [8-10]. Deux modèles dominent actuellement le marché : *Pay as you drive* (facturation selon la distance parcourue) et *Pay how you drive*, reposant sur une analyse plus poussée du comportement au volant. Ce second modèle pourrait s'imposer à plus grande échelle, d'autant que de nombreux assurés se montrent favorables à ces primes réduites [11].

À terme, cette évolution soulève une question majeure : si les boîtes noires sont désormais obligatoires, les dispositifs de surveillance avancée pourraient eux aussi le devenir. Ce glissement progressif réduirait encore davantage le contrôle des conducteurs sur les informations issues de leur propre véhicule.

UNE SURVEILLANCE ACCEPTÉE ?

Si certains dispositifs de surveillance sont imposés par la réglementation ou les constructeurs, d'autres sont désormais adoptés de manière volontaire par les conducteurs eux-mêmes.

C'est notamment le cas des dashcams, un système de caméra permettant d'enregistrer la route, et qui est en forte progression en Europe [12]. Ce phénomène s'inspire largement de pays comme la Chine ou la Russie, où ces dispositifs sont déjà très répandus comme moyen de preuve face à une justice jugée peu fiable et à une corruption policière fréquente [22-23].

En suivant une trajectoire similaire, l'Europe risque de s'exposer à des dérives comparables : surveillance permanente, restrictions de circulation, sanctions automatisées. Les images enregistrées par ces caméras, tout comme les données issues des systèmes *Pay how you drive*, peuvent certes être utilisées pour défendre un conducteur en cas d'accident, mais elles peuvent tout aussi bien se retourner contre lui.

En échange d'un sentiment de sécurité ou d'un avantage économique, les conducteurs renoncent peu à peu à une part de leur autonomie et de leur vie privée. Ce qui est présenté comme un progrès en matière de sécurité pourrait bien marquer, en réalité, un recul de nos libertés.

VERS UN GLISSEMENT DU BUSINESS MODEL

La notion même de propriété automobile est en train de basculer. Des fonctionnalités autrefois intégrées, comme les sièges chauffants chez BMW [19] ou l'aide au stationnement chez Tesla, sont désormais verrouillées derrière des abonnements. BMW a bien reculé sur ce modèle en Europe, mais la pratique reste courante en Asie, où elle suscite moins de controverse [21]. Certaines marques, comme Kia et Nissan, vont même jusqu'à intégrer des capteurs permettant de détecter l'activité sexuelle des occupants [11]. Échapper à cet écosystème ultra-connecté est théoriquement possible, mais cela exige des compétences techniques poussées et compromet la garantie du véhicule [9], ne laissant à la majorité pas d'autre option que de s'y conformer.

La digitalisation et les enjeux liés à la collecte de données poussent les constructeurs automobiles à repenser leur modèle économique. En misant sur la valorisation des informations générées par leurs véhicules, certains fabricants réussissent à baisser les prix de vente tout en maximisant les revenus issus de l'exploitation de ces données. C'est notamment le cas de plusieurs marques chinoises qui proposent des véhicules à des tarifs inférieurs à ceux de leurs concurrents occidentaux, comme Xpeng, BYD ou Geely, qui possède de nombreuses marques comme Volovo, Polestar ou encore Smart [20].

Année après année, les données deviennent plus rentables que les moteurs. Et dans un cadre juridique encore flou, cette nouvelle rente s'installe sans grand débat. D'ici à 2030, 95 % des voitures neuves devraient embarquer un système de surveillance connecté à Internet [17]. La question n'est plus de savoir si cette transformation aura lieu, mais si nous en garderons le contrôle.

RÉFÉRENCES

- [1] IEEE Spectrum. "How Software Is Eating the Car." spectrum.ieee.org, 2019, <https://spectrum.ieee.org/software-eating-car>
- [2] KPMG. "Monétisation des données automobiles : une nouvelle source de revenus ?" KPMG France, 2023, <https://kpmg.com/fr/fr/insights/data/monetisation-donnees-automobiles.html>
- [3] Stevenson, Tim. "Is Your Car Spying on You? How It May Be Selling Your Secrets and Costing You Money." *Investopedia*, Oct. 2023, <https://www.investopedia.com/is-your-car-spying-on-you-how-it-may-be-selling-your-secrets-and-costing-you-money-11728610>
- [4] KPMG. "The Future of the Car." KPMG Report, Dec. 2015, <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/12/the-future-of-the-car-report.pdf>
- [5] Mozilla Foundation. "It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy." *Privacy Not Included*, Sept. 2023, <https://www.mozilla.org/en/privacy-not-included/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy>
- [6] Hoody, Ruby M. "Mozilla Release Privacy Report on Connected Cars: Are You Driving a Privacy Nightmare?" hoody.com, Sept. 2023, <https://heig.ch/0K6kJ>
- [7] Chavaillaz, Théo, and Myriam Semaani. "Les 'boîtes noires' obligatoires dans toutes les nouvelles automobiles d'ici 2024." *RTS*, Feb. 2022, <https://heig.ch/N8XGw>
- [8] "Assurance jeunes conducteurs - Axa." *Axa*, <https://heig.ch/wa1W8>
- [9] "BonusDrive-Simpego." *Simpego*, <https://heig.ch/P53dN>
- [10] "CleverDrive - la Mobilière." *la Mobilière*, <https://heig.ch/vDBlo>
- [11] "Assurances auto Pay how you drive: guide complet pour économiser en conduisant", guide-auto.com, Jan. 2024, <https://heig.ch/vBQzI>
- [12] "Dash Cam Usage: A Quick Country-Wise Breakdown." *Vava*, <https://heig.ch/ag3bN>
- [13] Red Hat. « Logiciels Open Source et propriétaires dans le secteur automobile. » *Red Hat*, <https://heig.ch/NwNdQ>
- [14] Mozilla Foundation « Constructeurs automobiles : arrêtez de recueillir massivement nos données ! », <https://heig.ch/N2GA1>
- [15] Ariel Zibler. « Nissan, Kia can collect data on drivers' 'sexual activity' and 'sex lives': privacy watchdog » *New York Post*, <https://heig.ch/K3xaX>
- [16] Steve Stecklow, Waylon Cunningham, Hyunjoo Jin. "Tesla workers shared sensitive images recorded by customer cars". *Reuters* [Tesla workers shared sensitive images recorded by customer cars | Reuters](https://www.reuters.com/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-07-26/)
- [17] Catalina Sanchez, « Car Makers Shouldn't Be Selling Our Driving History to Data Brokers and Insurance Companies » *EFF* <https://www.eff.org/deeplinks/2024/06/car-makers-shouldnt-be-selling-our-driving-history-data-brokers-and-insurance>
- [18] Parlement européen. "Question for written answer E-000182/2025 by Niels Fuglsang (S&D) to the Commission – On the selling of vehicle data to brokers." europarl.europa.eu, Jan. 2025, https://www.europarl.europa.eu/doceo/document/E-10-2025-000182_EN.html

- [19] RTS. “Sièges chauffants à 29 francs par mois: des marques testent les options sur abonnement.” RTS, vers 2022, <https://www.rts.ch/info/sciences-tech/13243840-sieges-chauffants-a-29-francs-par-mois-des-marques-testent-les-options-sur-abonnement.html>
- [20] *The Guardian*. “Sing when you’re winning: how karaoke in cars heralds the triumph of Chinese firms.” *The Guardian*, May 20 2025, <https://www.theguardian.com/world/2025/may/20/sing-when-youre-winning-how-karaoke-heralds-the-triumph-of-chinese-carmakers>
- [21] Fortune. “BMW is now selling subscriptions for heated seats in cars – in South Korea.” *Fortune*, July 12, 2022, <https://fortune.com/2022/07/12/bmw-heated-seats-subscription-microtransactions-south-korea/>
- [22] *Wired*. “Why Almost Everyone in Russia Has a Dash Cam.” *Wired*, February 15 2013, <https://www.wired.com/2013/02/russian-dash-cams>
- [23] *Vava*. “Dash Cam Usage: A Quick Country-Wise Breakdown.” *Vava Blog*, 2023, <https://www.vava.com/blogs/dash-cam/dash-cam-usage-a-quick-country-wise-breakdown>
- [24] Parlement européen. *Question écrite : Surveillance des données personnelles par les constructeurs automobiles*. Question E-003142/2023, 25 octobre 2023. https://www.europarl.europa.eu/doceo/document/E-9-2023-003142_EN.html
- [25] Vie publique. *Les véhicules communicants nécessitent-ils de nouvelles réglementations ?* Rapport n° 009939-01, 2015, <https://www.vie-publique.fr/files/rapport/pdf/154000746.pdf>