La saisie des voitures connectées

1. Les voitures et l'« internet des objets ». « En novembre ou en décembre cette année nous devrions être capables d'aller d'un stationnement de Californie jusqu'à un stationnement de New York sans toucher à un bouton de tout le voyage ». Cette citation d'Elon Musk, prémonitoire à l'époque, dépeignait la vision de ce dernier sur les objets connectés et plus particulièrement les véhicules. Les objets connectés peuvent être définis comme des objets ordinaires qui nous entourent et qui ont la capacité de communiquer des informations diverses à d'autres objets. Ils ont aussi la capacité de recevoir des données ou des instructions, voire même d'être commandés à distance. Parmi ce très grand nombre d'objets connectés, les véhicules connectés ont pris une très grande place ces dix dernières années. Selon le comité européen de la protection des données, le véhicule connecté est « un véhicule équipé de nombreuses unités de contrôle électronique qui sont reliées entre elles par un réseau embarqué, ainsi que de moyens de connectivité lui permettant de partager des informations avec d'autres dispositifs à l'intérieur et à l'extérieur du véhicule »[1]. En somme, il s'agit de véhicules équipés de technologies de communication qui leur permettent d'échanger des données avec d'autres appareils et systèmes tels que d'autres véhicules ou des infrastructures routières ou des appareils mobiles type smartphones, tablettes ou des serveurs et des plateformes en ligne[2]. Ces véhicules connectés interagissent avec leur écosystème et peuvent faire l'objet de commande à distance ou même de prise de décisions individuelles au lieu et place du conducteur face à une situation dangereuse en utilisant pour ceci l'intelligence artificielle.

L'histoire de la voiture connectée s'inscrit dans un processus plus vaste de l'évolution des objets connectés qui sont apparus pour les premiers, dans les années 80 avec le distributeur de boissons de « Carnegie Mellon » souvent cité comme le premier objet connecté qui pouvait signaler à distance que les boissons étaient disponibles. Mais c'est en 1999 que le terme « internet des objets » est inventé par Kevin Ashton et à partir de 2010 où il y a une véritable multiplication de tels objets dans les domaines de la maison intelligente, de la santé, du bien-être, de la ville intelligente, de l'industrie 4.0, de l'agriculture et enfin de l'automobile avec l'apparition des TESLA. Pour le reste de l'étude, les expressions de « véhicule » connecté et de « voiture » connectée – qui n'est, au fond, qu'une catégorie particulière de véhicule ; la plus courante – seront utilisées indifféremment.

2. Les voitures connectées et les procédures civiles d'exécution. À première vue, les problèmes juridiques sur la saisie des véhicules – ou des voitures – connectés ne sont pas évidents. En effet, depuis la loi n° 91-650 du 9 juillet 1991 et le décret n° 92-755 du 31 juillet 1992, des procédures spécifiques de voies d'exécution sont applicables à la saisie de véhicules terrestres à moteur. Dans sa réforme, le législateur avait souhaité adapter les voies d'exécution à l'évolution de la société et plus particulièrement à l'évolution des types de fortunes des

[1] Lignes directrices 01/2020 *sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité.*

[2] V. sur le sujet : D. Paret, H. Rebaine, *Véhicules autonomes et connectés - Techniques, technologies, architectures et réseaux : du multiplex à l'Ethernet automobile*, Dunod, 2019.

Français et des objets saisis[3]. C'est ainsi qu'avait été prévue la saisie par déclaration à la préfecture du véhicule, ce dernier n'étant pas immobilisé physiquement mais le débiteur ne pouvant le vendre car aucun nouveau certificat d'immatriculation ne peut plus être délivré. Également, une procédure spécifique de saisie par immobilisation des véhicules avait été prévue soit à l'aide d'un « sabot de Denver », soit avec une mise en gardiennage dudit véhicule ou toute autre solution. Ces procédures, qui figurent aujourd'hui aux articles L. 233-1, L. 233-2 et R. 233-1 et suivant du Code des procédures civiles d'exécution, sont bien évidemment applicables aux véhicules connectés. Seulement, les spécificités des véhicules connectées ne pouvaient, par définition, pas être prises en considérations dans les années 1990 ou même au début des années 2010. Du fait même de l'évolution technologique des voitures connectées, il est donc légitime de s'interroger sur l'éventuelle nécessité d'une procédure spécifique plus adaptée en termes d'exécution. Par ailleurs, eu égard à la particularité de tels objets et du fait que ces derniers collectent et utilisent de très nombreuses données, certaines étant personnelles à leur propriétaire, un certain nombre de problèmes juridiques peuvent se poser. Qu'en est-il, par exemple, de la saisie puis de la vente aux enchères dudit véhicule contenant des données collectées lors de son usage ? Il s'agit principalement de l'historique de sa localisation, des données de conduite et de diagnostics, des données multimédias et de différents évènements. C'est ainsi que des enjeux juridiques et éthiques se posent qui s'inscrivent dans les cadres règlementaires actuels qui sont notamment les dispositions européennes et de la loi nationale française dont la CNIL assure le respect.

L'automobile contemporaine ne se résume plus être un simple objet de mobilité mais constitue désormais un véritable nœud technologique complexe. Cette métamorphose rapide, impulsée par le rythme exponentiel du progrès technique et alimenté à la vitesse des besoins et envies consuméristes de notre société engendre une rupture paradigmatique qui dépasse de loin le cadre strictement mécanique et laisse le droit positif en peine pour s'adapter à cette cadence vertigineuse. Le véhicule pensé comme un bien physique, stable et isolé se heurte désormais à une réalité hybride, décentralisée et fluide. Une reconfiguration structurelle qui brouille les frontières entre le bien saisi et ses attributs numériques. Face à cette situation, il nous est apparu opportun de présenter dans une première partie les éléments qui ralentissent, aujourd'hui, la saisie des véhicules connectés (I). Et, dans une deuxième partie, plus prospective, de proposer quelques solutions novatrices pour accélérer et sécuriser le déroulement d'une procédure plus que trentenaire aux enjeux technologiques du XXI^{e} siècle (II).

I. La saisie des voitures connectées, une saisie ralentie

3. Annonce. Les freins qui peuvent ralentir la saisie des voitures connectées sont de deux ordres. Ils peuvent être tantôt juridiques (A), tantôt techniques (B).

A. Des freins juridiques

[3] R. Perrot, Ph. Théry, *Procédures civiles d'exécution*, 3^{e} éd., Dalloz, 2014, p. 11 et s.

4. La nécessaire protection des données personnelles. Le véhicule connecté ne saurait être considéré comme neutre sur le plan informationnel. En effet, outre son hyper connectivité structurelle, il embarque à bord une quantité colossale de données relatives tant à l'objet de la saisie qu'au propriétaire lui-même ; lesquelles sont stockées dès sa première mise en circulation, collectées quotidiennement et analysées pour observer les habitudes de conduites et optimiser les services. Il s'agit là surtout de données qui relèvent de la sphère personnelle. Un véhicule connecté garde en mémoire les données sensibles relatives aux historiques de trajet relevant d'une géolocalisation précise, les comptes utilisateurs et mots de passe, la synchronisation des applications mobiles, contacts et messages, outre les profils biométriques d'ouverture (empreinte digitale, reconnaissance faciale ou vocale). *De facto*, saisir le véhicule revient à saisir les données qui y sont inhérentes.

Les données en question peuvent être classées en trois catégories : des données permettant l'identification directe de la personne, comme l'identité du conducteur ou celle de du titulaire de la carte grise ; des données permettant une identification indirecte par le recoupement de différentes données, comme le détail des trajets effectués ; et enfin des données de géolocalisation. La collecte de ces données est source de progrès, mais elle présente également le risque de révéler des pans entiers de la vie des usagers, ce qui peut constituer une atteinte particulièrement intrusive au principe du respect de la vie privée protégé au niveau national par l'article 9 du Code civil et au niveau international par l'article 8 de la Convention européenne des droits de l'homme. Si la collecte de données est techniquement possible, tout l'enjeu est de savoir ce qu'il advient de ces données pour savoir comment et de quelle manière elles sont protégées. Dans le cadre d'une saisie de véhicule connecté que deviendront-elles ? Et le fait que le véhicule soit le support de données protégées ne pourrait-il pas le rendre *de jure* insaisissable ?

5. Les difficultés liées à la protection des données personnelles. En réalité, les données – le contenu – doivent bien être distinguées expressément du véhicule saisi – le contenant. L'enjeu juridique auquel est confronté le commissaire de justice est ici le respect scrupuleux du Règlement Général sur la Protection des Données (RGPD) mais aussi de la loi n° 78-17 du 6 janvier 1978, dite « informatique et libertés »[4]. À l'intérieur d'un véhicule, les données peuvent être collectées de trois manières différentes. Tout d'abord, les données collectées peuvent être traitées uniquement par l'usager et ne sont pas transmises à une tierce personne. On peut citer la détection du franchissement de ligne blanche ou l'alerte de risque de collision. On est alors dans un cas dit « in-in » pour lequel aucune protection juridique n'est applicable. Ensuite, les données collectées peuvent être transmises au fournisseur de service afin de fournir un service à l'usager. Par exemple, l'assistance dépannage ou l'appel d'urgence. On est alors dans un cas dit « in-out » dans lequel les données traitées bénéficient d'une protection avec le RGPD et la loi informatique et libertés. Enfin, les données collectées peuvent être transmises aux fournisseurs de service afin de déclencher une action automatique dans le véhicule. Par exemple, l'info trafic dynamique, la maintenance à distance. On est alors dans un cas dit « in-out-in », où les données traitées sont également soumises à une protection juridique avec le RGPD et la loi informatique et libertés. La mise en œuvre de la saisie d'un véhicule connecté répond au traitement des données « in-out-in » puisqu'elle va nécessiter une action extérieure non voulue par l'usager. Il faudra donc faire application tant du RGPD et de la loi informatique

[4] V. sur le sujet : Th. Douville, « La saisie des objets connectés », in R. Laher, dir., *Le 10e anniversaire du Code des procédures civiles d'exécution*, LexisNexis, 2023, p. 87 et s.

et libertés. En France, la CNIL s'est intéressée à ce sujet en publiant un pack de conformité ayant pour thème « Véhicules connectés et données personnelles », puis tout récemment au sein d'un club conformité elle a soumis ce thème à consultation publique. Un nouveau projet de recommandation sur l'utilisation des données des véhicules connectés est en cours d'élaboration. Il ressort de ces différents rapports que de nombreux obstacles existent à la collecte des données personnelles. Ces obstacles devront être pris en compte dans le cadre de la mise en place de la saisie des véhicules connectés.

L'un des principaux freins sera l'obtention du consentement de l'usage du véhicule à l'utilisation des données collectées. En effet, les articles 6 et 7 du RGPD prévoient un consentement exprès, libre et éclairé. Il faudrait donc, en principe, que le débiteur ait consenti préalablement à la possibilité d'une saisie de son véhicule connecté et que son consentement soit donné dans des conditions bien spécifiques et univoques. De plus, le consentement devra être renouvelé notamment dans le cadre des mises en jour des logiciels. L'article 4, 1°) de la loi informatique et libertés et l'article 5-1-a du RGPD prévoient une règle de loyauté de la collecte. Il s'agira donc de faire consentir, en toute loyauté et transparence, l'acquéreur d'un véhicule connecté à la possibilité de la saisie de ce dernier. Le principe de loyauté et transparence implique qu'une information complète tant sur la forme que sur les conséquences de l'engagement d'une procédure de saisie soit donnée. Mais comment faire accepter un tel principe de saisie ? Et quelle sanction pour celui qui refuserait ? On voit bien, ici, que le droit des données personnel s'oppose frontalement au droit de l'exécution. Dans le cadre de la collecte des données, un responsable du traitement doit aussi être désigné, il définit les grandes lignes du traitement et les directives qui sont le plus souvent appliquées par son sous-traitant. Il garantit également la confidentialité des données collectées, évitant ainsi leur divulgation à des tiers non autorisés. Qui sera désigné en pareille situation ? Le flou reste entier. Naturellement, le commissaire de justice en charge de la procédure devra être en lien étroit avec le responsable de traitement. Mais il est absolument nécessaire que les rôles de chacun puissent être définis et délimités afin de garantir les règles posées par le RGPD. Et, pour l'heure, aucun texte légal ou règlementaire ne le fait. Enfin, le principe de durée limitée de conservation des données pourrait être un obstacle supplémentaire. En effet, ces données ne peuvent être conservées de manière indéfinie par le responsable du traitement suivant l'article 4, 5°) de la loi informatique et libertés et l'article 5-1-e du RGPD. Le consentement de l'usager doit donc être fréquemment renouvelé et, dans le cas contraire, la saisie ne semble pas pouvoir se faire.

B. Des freins techniques

6. Annonce. L'habitacle du véhicule devient un nouveau chez soi ; le digital a envahi l'espace, le Wifi a pris place à bord et l'aide à la conduite est devenue usuelle. En somme, une connectivité qui lie un bien à un ou des autres en les rendant interdépendants. Pour autant, le cœur du problème réside dans la persistance d'un pouvoir de contrôle du propriétaire sur le bien, y compris après son appréhension physique. Cette fonctionnalité pose une menace directe à l'efficacité de la saisie, qu'elle soit pratiquée par appréhension physique ou par une éventuelle immobilisation virtuelle à créer. L'efficacité même des procédures civiles d'exécution est freinée par un ensemble d'obstacles techniques propres à la nature même de l'automobile connectée définie désormais par l'immixtion d'éléments extrapatrimoniaux (données, comptes, licences, data) dans la consistance matérielle du véhicule.

Dans cette nouvelle configuration, deux lignes de tensions majeures viennent freiner les avancées et méritent une attention particulière. La première réside dans l'hyperconnectivité du véhicule (1), laquelle tend à défier l'autorité et l'effectivité des mesures d'exécution forcée par la création d'un lien numérique intrinsèque et persistant entre le véhicule connecté, son conducteur et son fabricant, susceptible de neutraliser et contourner les effets de la saisie. La seconde concerne la complexité opérationnelle de la saisie sur le terrain (2) tant en raison des contraintes techniques liées à l'identification et à l'immobilisation du véhicule qu'à la problématique de sa conservation sécurisée sous la responsabilité d'un tiers gardien ou du commissaire de justice.

1°) L'hyperconnectivité fonctionnelle

7. L'accès et la conservation des données. Outre les règles juridiques précédemment évoquées qui imposent au commissaire de justice un principe de minimisation des traitements, l'obligation d'information de la personne concernée et la limitation des accès, celui-ci est tenu à la résolution des défis techniques de sécurisation desdites données, principalement pour prévenir et empêcher leur extraction, leur consultation par des tiers non autorisés et assurer leur restitution dans des conditions conformes au droit. Or, au regard du droit positif, il serait fort imprudent pour le commissaire de justice d'y procéder lui-même en ce que de telles opérations requièrent une expertise propre dans un domaine qui dépasse le seul domaine du droit. Et la responsabilité du commissaire de justice serait de manière quasi systématique engagée en cas de mauvaise manipulation, désactivation partielle ou scellé numérique incomplet par exemple.

Mais un problème persiste même avec l'intervention d'un expert qui serait mandaté pour protéger les données postérieurement à la saisie. En effet, une cybersécurité est également requise pour assurer la défense des données voire la sécurisation systémique du véhicule connecté dans sa globalité. Il faut bien garder à l'esprit que contrairement au véhicule thermique traditionnel dont l'inertie mécanique constitue un état de neutralité, le véhicule connecté ne connait pas de véritable état d'extinction fonctionnelle. C'est un mode veille qui se substitue à l'activité manifeste, maintenant une forme de disponibilité latente, tributaire alors de l'autonomie résiduelle de la batterie. À l'inverse d'un véhicule classique susceptible de faire uniquement l'objet de dégradations extérieures, il devient désormais la cible d'une potentielle cyberattaque postérieure à la saisie. Le véhicule, et a fortiori les données embarquées, peuvent être victimes d'une intrusion externe via tous les réseaux sans fil désormais omniprésents (Wifi, *Bluetooth*, 4G/5G), d'une attaque ciblée via une faille d'une application installée ou du compte cloud auquel il est rattaché voire un effacement à distance ou un sabotage informatique des fonctions critiques.

8. Le pilotage à distance. Un véhicule connecté est susceptible d'être géolocalisé en temps réel par son propriétaire ou son utilisateur. Il est dès lors possible pour ces derniers de le déverrouiller à distance ou, à l'inverse, de le verrouiller complètement via une application appropriée ou une clé directement dédiée à cet effet. *A fortiori*, il est possible de déplacer un véhicule de ce type de manière autonome en le commandant à distance, sans oublier qu'il est susceptible d'être activé ou désactivé entièrement (ou partiellement) par une simple commande externe via une application mobile ou via un logiciel constructeur conçu lui-même et valorisé comme une plus-value dans le choix et l'achat de ce type véhicule. La difficulté technique est

posée : la dépossession physique, qu'elle soit complète (avec enlèvement) ou partielle (par l'immobilisation), n'entraine plus nécessairement la perte de contrôle du véhicule. Un contrôle numérique peut toujours être exercé sur le bien pourtant saisi juridiquement, voire dépossédé. Les effets de la saisie se révèlent réversibles et son efficacité amoindrie ; et ce, davantage quand on sait que c'est la dépossession qui reste l'élément psychologique le plus impactant pour le débiteur.

Le commissaire de justice est responsable des opérations de saisie et, en cas de dépossession, il peut être désigné un tiers en qualité de gardien. Comment garantir l'intégrité, voire la disponibilité d'un bien saisi, qui peut finalement être technologiquement piloté à distance par le débiteur ? Si ce dernier a de mauvaises intentions, il lui serait possible de se connecter au véhicule saisi pour le piloter et le dégrader volontairement pour diminuer sa valeur (en le faisant rouler contre un obstacle, en baissant toutes les vitres et ouvrant les portes en cas d'intempérie, etc.) plutôt que de supporter une vente forcée. De plus, dans de tels cas, qui verrait sa responsabilité engagée ? L'efficacité de la saisie suppose par conséquent une neutralisation immédiate des canaux de contrôle à distance et par là même, un coût supplémentaire qui alourdit la procédure par l'intervention d'un technicien agréé (à supposer que celui-ci puisse agir sans distinction des différents modèles de véhicules, ou alors s'ajouterait encore la tâche ardue de contacter le technicien idoine selon le constructeur automobile requis). À défaut, un accès au *backend*[5] de chaque fabricant est à prévoir mais reste encore à ce que tous les groupes automobiles coopèrent pour la création d'une fonction et la mise à disposition en faveur des commissaires de justice d'une partie de leur serveur pour bloquer les canaux de contrôle d'un véhicule saisi.

9. La dépendance au constructeur. Le constructeur automobile est susceptible de jouer un rôle prépondérant dans l'efficience ou l'échec de la saisie d'un véhicule connecté. En effet, ce dernier est un acteur incontournable dans la perte de maitrise effective du bien lors de la saisie du fait du lien numérique intrinsèque existant avec l'objet de la saisie. Un véhicule peut également recevoir une commande *via* l'infrastructure du constructeur par l'intermédiaire de serveurs distants. Il y a là un cordon ombilical digital qui n'est jamais réellement coupé et, techniquement, il subsiste une possibilité que le véhicule connecté reçoive, après saisi, des instructions émises par son propriétaire ou utilisateur via le constructeur auprès duquel ce premier se serait manifesté en prenant soin de lui dissimuler l'existence de toute mesure d'exécution forcée sur sa voiture. Le constructeur pourrait alors réactiver certaines fonctionnalités, effacer des données, paralyser la bonne mise en marche du véhicule selon les consignes qui lui seraient données, en méconnaissance du cadre légal applicable. L'exemple précédent illustre une dissimulation volontaire de la mesure de saisie par le propriétaire ou l'utilisateur du véhicule à l'égard du constructeur mais rien n'exclut que ce dernier agisse sciemment contre la saisie. La relation qui lie le propriétaire ou l'utilisateur du véhicule repose sur une logique commerciale et contractuelle à l'égard d'un client à satisfaire. En l'absence de cadre normatif strict, instaurant des sanctions pour un tel agissement et sans dispositif légal de notification officielle de la saisie au constructeur préalable ou concomitante, comment établir juridiquement la preuve de la connaissance effective de la mesure, la participation active du constructeur et le faire condamner ? À cette difficulté probatoire, s'ajoute alors une autre difficulté technique très concrète : la multiplicité des constructeurs et leur localisation. En effet, même en rassemblant les différentes marques pour les centraliser auprès du siège du groupe automobile auxquelles elles appartiennent, leur nombre reste significatif, d'autant que les

[5] C'est-à-dire la couche d'accès aux données qui ne sont pas directement accessibles par l'utilisateur.

différents groupes de constructeurs sont pour la plupart situés à l'étranger, compliquant de fait toute action à l'encontre, voire même toute prise de contact. Une harmonisation des normes et une coopération légale sont indispensables en amont pour neutraliser préventivement toute nouvelle instruction sur un véhicule connecté saisi.

Cette dépendance fonctionnelle qui unit le véhicule à son constructeur rend instables les effets concrets de la saisie. Tous les véhicules connectés embarquent dans leur système des licences ou abonnements qui sont indispensables à leur bon fonctionnement. Encore une fois : il ne faut plus réduire un véhicule à un simple objet mécanique isolé mais bien à une entité hybride dynamique interagissant avec son environnement. La fonction principale de rouler peut désormais être conditionnée à l'existence d'une licence ou d'un abonnement actif auprès de son constructeur. Les fonctionnalités encadrant la navigation, l'autopilote, les mises à jour, les systèmes d'alarmes, d'entretien, de diagnostics et la maintenance à distance relèvent directement des serveurs de ce dernier et déterminent la mise en marche optimale du véhicule. Or, la saisie d'un véhicule connecté n'assure pas *de facto* la transférabilité des droits sur ces attributs extrapatrimoniaux. Pour cause, ces derniers ne sauraient être modifiés, supprimés ou transférés automatiquement et pourtant, ils sont indissociables du bien saisi. Il en résulte un risque important d'aboutir à la paralysie involontaire du bien saisi. Par ailleurs, tous les services virtuels en question reposent, pour beaucoup, sur la connexion aux serveurs distants et infrastructures informatiques externalisées et contrôlées par le fabricant. Tous les avantages qui en découlent pour le propriétaire ou l'utilisateur du véhicule sont indéniables tant au niveau du confort de sa conduite que dans la plus-value technologique. Cependant, cette dépendance inhérente au véhicule connecté affecte directement la proportionnalité et l'efficience entre la mesure de saisie et l'objectif poursuivi de la vente du bien pour le paiement d'une créance liquide et exigible. En effet, cette valeur ne repose plus là encore uniquement sur des caractéristiques mécaniques et le bon état général du véhicule mais intègre des éléments immatériels et fonctionnels indissociables de l'univers numérique du constructeur ; la qualité des services dématérialisés participant indéniablement à la valeur fonctionnelle. Cette dernière serait alors amoindrie en cas de rupture délibérée ou dysfonctionnement involontaire avec son constructeur. Il s'agit là d'un nouveau critère à prendre en compte mais qui n'est pas aisé à vérifier avant de pratiquer la saisie. Comment être sûr pour le commissaire de justice que cette liaison numérique et virtuelle est toujours bien configurée pour le véhicule connecté avant de le saisir ? Problème : il est laborieux d'avoir accès à une telle commande tant que le véhicule n'est pas immobilisé.

b) Les difficultés opérationnelles

10. Identification, présence à bord et *timing* de la saisie du véhicule. La saisie d'un véhicule motorisé en l'état positif du droit est réalisable par immobilisation avec ou sans enlèvement. Pour ce faire, le commissaire de justice doit avoir le véhicule dans son champ de perception visuel direct, d'autant que le Code des procédures civiles d'exécution lui impose également de consigner dans son procès-verbal l'état du véhicule et les objets visibles apparents au sein de l'habitacle[6]. L'avantage et l'intérêt de la saisie sur un véhicule motorisé connecté seraient alors

[6] CPCE, art. R. 223-8.

d'envisager en plus une saisie à distance, dématérialisée et potentiellement immédiate, à ne pas confondre avec la saisie par déclaration d'ores et déjà existante mais n'entrainant pas l'immobilisation du véhicule. Toutefois, cette innovation procédurale se heurte à une série d'obstacles majeurs susceptibles d'en freiner l'efficacité. Le premier écueil réside dans l'identification même du véhicule cible. En effet, alors que la saisie d'un véhicule classique s'appuie, après localisation, sur la seule reconnaissance de sa plaque d'immatriculation, ce mode d'identification s'avère inopérant en l'état pour procéder à une saisie dématérialisée. Il conviendrait donc de pouvoir avoir une individualisation par une empreinte électronique propre à chaque véhicule connecté mais ici, reste encore à ce qu'un fichier centralisé soit créé à l'instar du Système d'Immatriculation des Véhicules (SIV), ainsi qu'un outil dématérialisé unifié afin de bloquer à distance tout type de véhicule connecté sans considération de son constructeur automobile, supposant une coopération normative et opérationnelle à l'échelle internationale dans un domaine où la souveraineté des constructeurs, souvent extraterritoriaux, demeure un frein considérable à toute interopérabilité.

À supposer acquise l'identification certaine du véhicule connecté, subsiste une question déterminante : celle du moment opportun pour mettre en œuvre la mesure de saisie. Si celle-ci demeure soumise en toute hypothèse au strict respect des plages horaires légalement encadrées en matière d'exécution forcée, elle exige également une appréciation stratégique du *timing* afin d'assurer l'appréhension exclusive du véhicule ciblé, hors de toute situation mobile susceptible d'en compromettre la sécurité. Rappelons l'évidence : le véhicule, aussi connecté soit-il, a pour fonction principale d'assurer la mobilité. Dès lors, si le commissaire de justice procède à une saisie à distance sur un véhicule en stationnement, la mesure conserve une dimension maîtrisable, mais qu'en serait-il d'une activation à distance lorsqu'un véhicule circule à 130 km/h sur autoroute ? Une telle hypothèse, dans laquelle un système d'arrêt à distance provoquerait une immobilisation soudaine, soulève des interrogations d'une gravité singulière, et notamment sur le plan humain et les atteintes physiques et corporelles qui seraient portées au conducteur ou aux usagers de la route ; sans même parler d'une possible qualification pénale[7]. Dès lors, il s'agirait paradoxalement d'un véhicule juridiquement saisi, matériellement endommagé par un accident, voire irréversiblement détruit en raison même de l'exécution de la mesure à distance. Par ailleurs, qu'en serait-il lorsque le véhicule est immobilisé alors même que celui-ci est stationné sur chez un tiers, ou plus encore lorsque l'immobilisation est pratiquée sur un véhicule stationné sur la voie publique mais dont le stationnement est conditionné par l'assujettissement à des contraintes horaires et tarifaires ? Ces différentes hypothèses mettent en lumière le nombre de paramètres à prendre en considération et anticiper, de moyens techniques à mobiliser et la lourde responsabilité qui pèse sur le commissaire de justice pour *in fine* un résultat aléatoire voire contreproductif.

D'autant qu'il ne s'agit là que de conséquences matérielles, s'ajoute une dimension autrement plus essentielle : celle tenant à la présence d'être vivant dans l'habitacle au moment de la saisie. Qu'il soit à l'arrêt ou en mouvement, le véhicule saisi de façon dématérialisée est susceptible d'avoir à son bord une personne ou un animal qui modifie radicalement la portée juridique, éthique et morale de la mesure d'exécution. Déjà une mise en danger par un éventuel accident si le véhicule était en circulation, mais, même à l'arrêt, les risques demeurent élevés. En effet, l'activation d'un verrouillage automatique à distance par un arrêt brutal pourrait porter atteinte à des libertés individuelles voire entraîner un traitement dégradant dans le cas où des êtres

[7] Pouvant aller jusqu'à l'homicide involontaire. V. CP, art. 221-6 et s.

vivants seraient bloqués à l'intérieur : un enfant endormi à l'arrière, un passager inconscient, des animaux dans le coffre. Sans même parler, ici aussi, des risques de qualifications pénales en cas d'atteinte à leur intégrité physique. Autant d'éléments à prendre en considération au-delà même de la simple saisie du véhicule. Par conséquent, la possibilité d'une immobilisation automatisée, sans moyen fiable et certain de vérification préalable de la vacuité du véhicule, représente un obstacle technique majeur à la mise en œuvre sécurisée et licite de la saisie.

11. Véhicule en cours de recharge et autonomie de la batterie. Il ne saurait être fait abstraction d'une autre hypothèse pratique qui est celle du temps de chargement d'un véhicule. Force est de constater que la motorisation électrique devient la norme dans le domaine des véhicules connectés. À ce jour, 1,3 million de voitures électriques circulent en France, soit plus de 15% de l'ensemble des véhicules, un chiffre en pleine croissance exponentielle. Par conséquent, le moment idoine de la saisie est encore présent sous le prisme de ce paramètre. Lors du rechargement à une borne, le véhicule est relié par un câble à cette dernière. Ce branchement est verrouillé électroniquement. Ce dispositif de sécurisation destiné initialement à prévenir toute déconnexion malveillante ou non autorisée par un tiers, devient paradoxalement, un obstacle à l'exécution matérielle d'une saisie par immobilisation avec enlèvement. Toute tentative de retrait forcé pourrait endommager le système tant l'infrastructure de la borne, qui plus est souvent propriété d'un tiers, que le véhicule lui-même, exposant par là même l'officier public et ministériel à une mise en cause de sa responsabilité.

En outre, le débranchement d'une borne de rechargement est généralement accompagné d'une notification au propriétaire ou l'utilisateur du véhicule. Si celui-ci se trouve à proximité, il n'est jamais bon qu'il soit informé en temps réel d'un enlèvement physique de son véhicule, au risque d'être véhément à l'encontre des protagonistes. C'est d'ailleurs pour cette raison que la solution de différer la saisie le temps que le câble soit retiré par le propriétaire ou l'utilisateur lui-même n'est pas forcément envisageable. La saisie ne devrait pas être tributaire de facteurs de cette nature. Ainsi, l'assistance d'un opérateur habilité semble être la seule alternative envisageable dans cet exemple : il pourrait intervenir pour faire cesser le rechargement et désactiver le verrouillage électronique du câble en toute sécurité (en présentiel ou à distance), mais cela suppose encore une harmonisation technologique des systèmes entre les constructeurs de bornes cette fois-ci et sans doute la création d'un outil commun ou d'un protocole technique unifié en ce sens, à ce jour inexistant.

L'autonomie énergétique représente enfin un paramètre non négligeable. Dès l'instant où la saisie – physique ou dématérialisée, immobilisée avec ou sans enlèvement – est effectuée, un compte à rebours implicite s'enclenche : celui de la durée restante de la batterie avant l'épuisement complet. Comme évoqué, un véhicule électrique connecté n'est jamais véritablement à l'arrêt mais davantage dans un mode veille. Par conséquent, il doit rester alimenté et avoir une source électrique pour assurer le maintien de ses fonctions et surtout son démarrage. À l'inverse d'un véhicule thermique dont le carburant demeure stable à l'arrêt, celui qui est électrique, et *a fortiori* connecté, finit inexorablement par vider sa batterie. Certains constructeurs prévoient un démarrage de secours de la batterie basse tension mais les conditions techniques diffèrent suivant les modèles de véhicule ; or tous sont unanimes sur un point : décharger sa batterie à 0% présente le risque d'endommager les composants du véhicule. La sécurisation du stationnement du véhicule saisi pourrait passer par l'extraction de la batterie mais un tiers spécialisé devrait alors être disponible pour intervenir, alourdissant d'un cout complémentaire la procédure. Le commissaire de justice ou le gardien du véhicule est responsable de la conservation et il devra assurer une alimentation électrique du bien. Or, de

nouveau, cette exigence ne saurait être réduite à un simple branchement de câble. Le processus d'alimentation est conditionné à une validation électronique depuis l'interface du véhicule, ce qui suppose d'y avoir accès. De nouveau, l'interconnexion soulève une autre problématique : au-delà de la clé traditionnelle ou électronique, le véhicule peut ne pas être accessible sans l'empreinte digitale, une reconnaissance biométrique ou l'application mobile du propriétaire ou utilisateur. L'accès est alors techniquement impossible en l'état sans cet artefact personnel, qui n'est pas saisissable en lui-même.

12. Reconditionnement numérique. Le véhicule connecté présente une complexité intrinsèque double résultant à la fois de sa structure mécanique traditionnelle et de son architecture numérique avancée. Ces deux composantes, bien que distinctes dans leur nature, sont aujourd'hui inextricablement liées et interdépendantes, et leur bon état respectif conditionne la valeur économique globale du bien. Autrefois, l'évaluation mécanique d'un véhicule saisi pouvait s'effectuer de manière relativement aisée, notamment par une simple mise en circulation permettant d'observer le comportement routier ; en revanche, la dimension « connectée » échappe à cette forme empirique d'évaluation. Dans ce contexte, le rôle du commissaire de justice, chargé d'apprécier l'opportunité de la saisie en vue d'une éventuelle vente forcée, s'en trouve considérablement complexifié. En cas de vente amiable, le problème ne se pose pas véritablement : il suffira au commissaire de justice de laisser le débiteur saisi procéder à la réinitialisation du véhicule pour lequel il a trouvé un acheteur. Mais faire vendre un véhicule connecté saisi qui n'aurait pas été déconnecté complètement de la configuration du propriétaire ou utilisateur d'un débiteur passif (configuration personnelle, historiques de localisation, accès à distance, etc.) équivaut à faire dévaluer considérablement le prix et l'opportunité de la mesure forcée. Au-delà des seules considérations financières évoquées ci-dessus, se pose la question de la légalité même de la vente. L'absence de réinitialisation intégrale du système numérique du véhicule emporte le risque manifeste d'une transmission illicite à l'acquéreur de données inhérentes à la personne même de l'ancien utilisateur. Il ne s'agit pas d'une simple tolérance juridique d'une purge théorique d'éventuels vices par une adjudication en l'état mais bien d'un transfert d'actifs à un tiers de données personnelles protégées et soumises au RGPD.

Au regard des contraintes techniques, l'intervention d'un tiers spécialisé apparait non seulement opportune mais absolument indispensable pour permettre le reconditionnement complet du véhicule connecté en vue de sa mise en vente dans des conditions conformes. Mais qui faire intervenir ? En outre, des inconvénients tenant au cout du reconditionnement numérique viennent aussi grever la rentabilité de la vente aux enchères. Et cette nouvelle opération requiert la mise à disposition physique du véhicule pendant une période significative. Enfin, la pluralité des intervenants, conjugués à l'opacité de certains écosystèmes numériques automobiles introduit un aléa non négligeable quant à la traçabilité des opérations effectuées, ce qui peut entrainer un contentieux postérieur à la vente, notamment en cas de résurgences de données résiduelles ou de dysfonctionnements ultérieurs.

II. La saisie des voitures connectées, une saisie à accélérer

13. Annonce. Afin de faciliter et de sécuriser la saisie des voitures connectées, il serait bon que le législateur se saisisse de la question, tant s'agissant du sort des données numériques (A) que d'une possible immobilisation numérique (B).

A. Le sort des données numériques

14. Le contrôle par le juge de l'exécution. Actuellement, le commissaire de justice qui saisit un véhicule connecté doit, comme nous l'avons vu, respecter plusieurs principes fondamentaux posés par le RGPD et la loi informatique et libertés. La licéité et la finalité des données collectées doivent être réalisées pour une finalité précise et légitime, en lien direct avec la procédure d'exécution. La minimisation des données implique que seules les données strictement nécessaires à la finalité de la saisie doivent être collectées. La sécurité des données doit être protégée contre tout accès non autorisé, toute altération ou toute divulgation. La traçabilité de toutes les actions effectuées sur les données doit être documentée, y compris les accès, les extractions et les modifications. Le commissaire de justice doit également veiller à respecter les droits des tiers, tels que les passagers ou les utilisateurs secondaires du véhicule, dont les données pourraient également être collectées.

Dans ce cadre, le Juge de l'Exécution (JEX) devrait voir son importance considérablement accrue car il joue un rôle clé dans l'évaluation de la proportionnalité et de la légalité de la saisie. Cette évolution de son office est essentielle pour répondre aux défis posés par les nouvelles technologies et les données numériques embarquées dans les véhicules modernes. Le JEX doit désormais naviguer entre les impératifs de l'exécution et les exigences de protection des données personnelles, tout en garantissant le respect des droits fondamentaux des individus. En effet, la complexité des systèmes embarqués dans ces véhicules nécessite une expertise accrue pour s'assurer que les saisies sont effectuées de manière juste et équitable, sans porter atteinte aux libertés individuelles. Mais cette évolution des pratiques judiciaires ne paraît pas, à elle seule, suffisante pour corriger tous les défauts du droit positif.

15. La sécurisation par le commissaire de justice. L'inspiration du droit comparé offre des perspectives intéressantes pour comprendre comment différents systèmes juridiques abordent la saisie des biens numériques. Aux États-Unis, l'approche est plus flexible pour la saisie de biens numériques, avec une jurisprudence développée sur les données associées aux objets saisis. Par exemple, les États-Unis ont lancé un label de sécurité informatique pour les objets connectés, ce qui pourrait inspirer des pratiques similaires en France pour sécuriser et encadrer l'accès aux données des véhicules connectés lors de leur saisie. Cette approche flexible pourrait être bénéfique pour accélérer les procédures de saisie tout en garantissant une protection adéquate des données. Au Québec et au Royaume-Uni, des modèles intéressants sont également observés[8]. Le Québec, avec sa Charte des droits et libertés, admet des dérogations au droit à la vie privée pour l'exécution de décisions de justice, à condition qu'elles soient strictement

[8] V. sur le sujet : R. Laher, « La saisie des supports numériques en France, en Angleterre et au Québec », in L. Antoniolli, M. Cardillo, F. Cortese, L. de Carbonnières, F. Mynard, C. Piciocchi, dir., *Numérique & Environnement*, Università di Trento Facoltà di Giurisprudenza, 2024, p. 81 et s.

nécessaires. Au Royaume-Uni, le Data Protection Act de 2018, bien que post-Brexit, reprend les standards du RGPD et permet une exemption judiciaire sous réserve de garanties suffisantes. Ces approches montrent l'importance de trouver un équilibre entre l'efficacité judiciaire et la protection des données personnelles.

Pour garantir le respect des principes énoncés ci-dessus, plusieurs évolutions pourraient être mises en place :

- L'identification préalable des données numériques présentes dans le véhicule connecté avant toute intervention permettrait au commissaire de justice d'identifier la nature des données embarquées et d'évaluer leur sensibilité au regard du droit des données personnelles.
- L'accès sécurisé aux données devrait se faire *via* des interfaces dédiées et sécurisées, éventuellement avec l'aide d'experts informatiques assermentés.
- La journalisation de toutes les actions effectuées sur les données devrait être consignée dans un registre, garantissant ainsi la traçabilité et la transparence.
- La conservation limitée des données collectées devrait être pour une durée strictement nécessaire à la procédure judiciaire, puis détruites ou restituées.
- Une collaboration étroite avec les constructeurs automobiles semble essentielle pour faciliter l'accès aux données tout en garantissant leur sécurité. Cette collaboration pourrait prendre la forme de protocoles nationaux de coopération, incluant la mise en place de plateformes sécurisées permettant aux constructeurs de communiquer les données essentielles du véhicule sur autorisation judiciaire.
- La création de registres nationaux des véhicules connectés, référencés par un identifiant unique (VIN), avec traçabilité et API sécurisée, ainsi que le développement d'interfaces normalisées d'extraction de données, accessibles uniquement aux commissaires de justice habilités, sont également des éléments clés de cette collaboration.

Si l'on refuse de considérer sur cette question le commissaire de justice comme un « tiers de confiance » pouvant extraire et conserver les données personnelles, à qui confier cette mission ? Il pourrait s'agir d'un professionnel agréé par le constructeur, d'un opérateur habilité à intervenir sur les systèmes embarqués ou encore d'une entité unique dotée d'une compétence certifiée en matière de cybersécurité automobile. Dans tous les cas, son rôle serait central pour la réinitialisation. Cette opération, loin d'être triviale, est presque assimilable à une situation monopolistique tant elle résulte de capacités techniques et d'un savoir spécifique pour respecter les différents protocoles et interfaces sécurisées sans porter atteinte à l'intégrité logicielle du système. Cela dit, un éventuel monopole entrainerait une dépendance structurelle à l'égard de ce tiers, qui se traduit aussi par des couts additionnels non négligeables, une incertitude quant à leur disponibilité et une délégation de gouvernance et de responsabilité.

On le voit, face à ces défis techniques et juridiques, la profession de commissaire de justice est amenée à repenser ses outils, ses méthodes et ses obligations. La saisie ne peut plus se concevoir comme un acte purement matériel, car, elle devient une opération mixte, se mêlant avec les notions de réseau et données numériques. Dans ce contexte, l'exemple des véhicules connectés illustre parfaitement les enjeux pratiques de cette mutation. Ces biens, à la fois tangibles et numériques, nécessitent donc une approche renouvelée de l'immobilisation, ouvrant la voie à une immobilisation numérique.

B. L’horizon d’une immobilisation numérique

16. Le préalable à l’immobilisation à distance. L’évolution des technologies et des cadres juridiques ouvre la voie à une réflexion sur la possibilité d’une immobilisation numérique des véhicules connectés. Cette notion émergente implique non seulement la sécurisation physique des biens saisis mais également la maîtrise et le contrôle des flux de données associés. L’immobilisation numérique pourrait ainsi représenter l’avenir de la saisie des véhicules connectés, intégrant des protocoles avancés de gestion des données et des technologies de blocage à distance pour une efficacité accrue et une facilité pour le commissaire de justice qui n’aurait plus à se déplacer pour poser le fameux « sabot de Denver ». Cependant, si le débiteur conserve l’accès à l’application mobile associée à son véhicule, il peut potentiellement le redémarrer sans contact, le localiser à distance, ou encore supprimer ou manipuler des historiques de trajets ou de données, empêchant par exemple la bonne traçabilité du véhicule, ce qui peut avoir une incidence, notamment en cas de vente judiciaire future. Dans le cadre d’une saisie d’une voiture connectée, il convient donc impérativement de neutraliser les fonctions connectées, au risque de rendre la mesure de saisie incomplète ou contournable. Cette évolution exige une adaptation des professionnels et de leur pratique dans un cadre règlementaire spécifique protecteur des droits du débiteur. Plusieurs mesures opérationnelles pourraient être envisagées pour renforcer l’effectivité de l’immobilisation numérique.

Le préalable nécessaire à une telle immobilisation est celui d’une coopération qui supposerait une intervention des constructeurs de voitures connectées, soit volontairement lors de la vente, soit forcée par une disposition législative. Cela impliquerait la création d’un fichier des voitures connectées, semblable au fichier SIV existant et la création d’un mécanisme d’autorisation de communication des données nécessaires à l’immobilisation à distance du véhicule. Il conviendrait, par exemple, de systématiser, dès la saisie, l’autorisation de communiquer les données nécessaires à l’immobilisation à distance (identifiants numériques relatifs aux véhicules, désactivation immédiate des fonctions à distance) en l’intégrant dans le contrat de vente ou de *leasing*, par le biais d’une clause ; ou en prévoyant une obligation légale pour les constructeurs. Cette autorisation pourrait comprendre l’autorisation de fournir les données de géolocalisation pour l’exécution d’une décision de justice, ainsi que les données permettant une immobilisation à distance dans un cadre légal et judiciaire bien défini.

17. La mise en œuvre de l’immobilisation à distance. Toutefois, malgré l’étape de la coopération préalable prévoyant l’autorisation d’accès aux données, l’immobilisation à distance rencontre plusieurs problèmes pratiques. Dans un premier temps, la saisie des véhicules situés à l’étranger est à exclure, celui-ci ne pouvant faire l’objet d’une mesure en raison d’un problème de compétence territoriale. En outre, il existe une difficulté concernant la saisie d’un véhicule en circulation. Le véhicule ne peut être immobilisé pour des raisons d’ordre pratique et de sécurité routière. Partant, il pourrait être envisagé une saisie à effet différé du véhicule en circulation. Ainsi, la saisie serait juridiquement efficace dès sa mise en œuvre numérique mais n’entrainerait l’immobilisation du véhicule lorsqu’il serait en stationnement hors d’une voie de circulation. En tout état de cause, le blocage du véhicule pourrait se faire à distance, empêchant

tout redémarrage. Cette nouvelle procédure d'immobilisation à distance pourrait être corrélée à la faculté de dénoncer cet acte de saisie, par courriel ou SMS aux adresse et numéro fournis lors de la signature du contrat de vente du véhicule ou plus sûrement au contrat de *leasing*. La procédure devrait prévoir un système de déblocage immédiat identique à la faculté d'immobilisation à distance.

Cela permet d'entrevoir un potentiel schéma de procédure.

Étape 1. Il conviendrait de signifier un commandement de payer avant immobilisation. Ce commandement pourrait prévoir une sommation d'abord à fournir mot de passe et informer, qu'à défaut, le constructeur sera contraint de les communiquer au commissaire de justice. Il est nécessaire d'également informer le débiteur que ses données personnelles seront stockées dans un coffre-fort numérique (protection RGPD).

Étape 2. L'immobilisation numérique à distance du véhicule connecté se ferait par la notification de l'acte de saisie à un tiers saisi qui pourrait être le constructeur sur le modèle de la saisie attribution et du PV de saisie dématérialisé via l'ADEC.

Étape 3. La dénonce immédiate – ou après arrêt du véhicule – par voie dématérialisée, par courriel ou SMS aux adresse et numéro fourni lors du contrat de vente ou de leasing. Autrement, la dénonce pourrait se faire par voie dématérialisée, si le débiteur a consenti à ce mode de signification d'acte.

En tout état de cause, il convient de prévoir une récupération physique du véhicule en l'absence de contestation à l'issue du délai ouvert au débiteur.

Cette perspective représente une opportunité de repositionnement pour la profession. En effet, le commissaire de justice peut devenir un acteur central dans la sécurisation des biens considérés comme « hybrides » et dans leur appréhension au point de vue juridique. À travers la saisie d'un véhicule connecté, c'est la question de la transparence juridique et de la confiance du justiciable qui sont mises en lumière. En maîtrisant ces enjeux d'identification du bien, de sa neutralisation et de la sécurisation des données qu'il contient, le commissaire de justice renforce son image de professionnel adaptable, rigoureux et moderne, en phase avec les évolutions technologiques de la société qui se reflètent dans le contentieux. L'horizon d'une immobilisation numérique, illustré par l'exemple des voitures connectées, annonce un tournant majeur dans les pratiques d'exécution. La profession doit accompagner activement ces mutations, plutôt que de les subir, à condition de se doter d'outils adaptés, de clarifier ses prérogatives territoriales, et de faire évoluer son cadre d'action. La profession de commissaire de justice doit relever ce défi et garantir la pleine effectivité de sa mission d'exécution des titres exécutoires dans un environnement où les biens sont désormais aussi virtuels que matériels.