

L'accessibilité des données issues de l'« Event data Recorder » en procédure pénale

LEONARDO GOMEZ MARIACA*

MOTS CLEFS	Procédure pénale – Event Data Recorder – Accessibilité – Perquisition – Transparence des données
ZUSAMMENFASSUNG	Der Artikel beleuchtet die verschiedenen rechtlichen Wege des Zugriffs auf Daten, die aus einem «Event Data Recorder» (im Folgenden: EDR) in Strafverfahren stammen. Zunächst wird auf die Geschichte dieser Technologie eingegangen. Anschliessend untersucht der Artikel die Frage, ob die Polizei befugt ist, Daten aus einem EDR zu erlangen. Er kommt zum Schluss, dass die Daten als «Aufzeichnungen» zu qualifizieren sind und nur mit einem Durchsuchungsbefehl erhoben werden dürfen. Schliesslich analysiert der Artikel die Empfehlung der Freiburger kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation vom 10. Mai 2023 und kommt zum Schluss, dass die Strafrechtsbehörde im Rahmen eines Strafverfahrens möglicherweise umgangen werden kann, da die Daten aus einem EDR sofort erstellt werden.
RÉSUMÉ	L'article met en lumière les différentes voies légales pour accéder aux données résultant d'un « Event Data Recorder » (EDR) en procédure pénale. Il revient sur l'histoire de cette technologie. Ensuite, l'auteur s'interroge sur la compétence de la police pour récupérer les données issues d'un EDR, en concluant que ces dernières doivent être qualifiées d'« enregistrements » et qu'elles ne peuvent être collectées qu'avec un mandat de perquisition. Enfin, l'article analyse la recommandation du 10 mai 2023 de l'autorité cantonale fribourgeoise de la transparence, de la protection des données et de la médiation et conclut à un possible contournement de l'autorité judiciaire dans le cadre d'une procédure pénale en raison de l'instantanéité de l'établissement des données issues d'un EDR.
ABSTRACT	This article examines the various legal possibilities for accessing data from an event data recorder (hereafter EDR) in legal proceedings. It begins with a review of the history of this technology. The article then examines the scope of the police to recover EDR data, concluding that EDRs should be classified as 'recordings' and that they can only be collected with a search warrant. Finally, the article analyses the Recommendation of 10 May 2023 of the Fribourg cantonal authority for transparency, data protection and mediation, and concludes that the judicial authority can be bypassed in criminal proceedings due to the instantaneous nature of EDR data.

I. Introduction

Les technologies embarquées dans les véhicules jouent un rôle clé en matière de sécurité routière. Parmi ces dispositifs, l'Event Data Recorder (ci-après : EDR), ou « en-

registreur de données d'événement », occupe une place particulière en tant qu'outil capable d'enregistrer des informations cruciales en cas d'événement, c'est-à-dire généralement un accident impliquant un véhicule automobile. L'EDR est un système embarqué dans le véhicule qui mesure en permanence un certain nombre de données, mais ne les enregistre que lorsqu'un changement de vitesse de plus de 8 km/h intervient en l'espace de 150 milli-secondes¹ ou lors du déclenchement de systèmes non réversibles², comme le déploiement de l'airbag. Ces données sont enregistrées depuis cinq secondes avant l'événement

* LEONARDO GOMEZ MARIACA, avocat-stagiaire. Je tiens à remercier les experts du « Forensisches Institut Zürich » pour les échanges très constructifs et pour leurs différentes remarques. Je remercie également les procureurs, greffières et greffiers des différents ministères publics cantonaux qui ont répondu aux questions relatives à leur pratique respective. Je remercie enfin l'Autorité cantonale fribourgeoise de la transparence, de la protection des données et de la médiation pour ses explications ainsi que la Direction de la sécurité, de la justice et du sport du canton de Fribourg pour sa collaboration. Les opinions exprimées dans la présente publication sont celles de l'auteur. Elles ne prétendent pas refléter les opinions ou les points de vue des institutions précitées. Cette contribution est publiée sous une licence Creative Commons. DOI de cet article: 10.3256/978-3-03929-084-0_05.

¹ Art. 5.3.1.1 et 5.3.1.2 du règlement ONU N 160 – Prescriptions uniformes relatives à l'homologation des véhicules à moteur en ce qui concerne l'enregistreur de données de route [2021/1215], OJ L 265 du 26 juillet 2021, 10. Ce règlement est repris au sein du droit européen par le règlement délégué (UE) N 2022/545, lui-même repris par l'art. 102a al. 1 OETV en droit suisse.

² Art. 5.3.1.3 du règlement ONU N 160, 10.

jusqu'à 300 millisecondes après l'événement³. Elles sont généralement stockées dans le module de contrôle des airbags (« Airbag Control Module », ci-après : ACM)⁴. L'EDR n'enregistre aucune image ni aucun son⁵. Il garde en mémoire les données dynamiques du véhicule, notamment la vitesse avant l'événement, la position des freins, de la pédale d'accélérateur, l'angle de direction, les changements de vitesse dus à l'événement, le statut des ceintures, le déclenchement des airbags⁶.

En Suisse, l'art. 102a OETV, en vigueur depuis le 1^{er} avril 2024, intègre le règlement de droit européen (UE) 2019/2144 et le règlement délégué (UE) 2022/545. Il oblige les nouveaux véhicules à être équipés d'un EDR. Cette obligation est reprise selon le même calendrier que l'Union européenne (ci-après : UE)⁷ : les voitures de tourisme⁸ et les voitures de livraison⁹ importées devaient en être munies au plus tard dès une importation au 7 juillet 2024 ; pour les minibus, les autocars, les camions et les tracteurs à sellette, l'obligation s'appliquera à partir du 7 janvier 2029 au plus tard¹⁰. L'annexe II de l'OETV indique quels systèmes sont reconnus en droit suisse, bien

qu'une équivalence soit possible pour autant qu'elle soit prouvée par le constructeur¹¹. Il convient également de souligner que, bien que les véhicules importés avant ces dates et déjà en circulation ne doivent pas être équipés de tels dispositifs, de nombreux constructeurs ont déjà intégré des EDR dans leurs véhicules sur une base volontaire.

Les données enregistrées au sein d'un EDR sont souvent déterminantes dans le cadre d'une procédure judiciaire, mais elles soulèvent toutefois des questions quant à leur accessibilité. Au travers de cet article, nous explorerons les différentes voies légales permettant d'accéder aux données issues d'un EDR en procédure pénale. Nous commencerons par retracer l'évolution du cadre légal applicable depuis ses origines aux États-Unis jusqu'à sa transposition dans le droit suisse, en passant par les normes onusiennes et européennes, et analyserons les différentes définitions légales y afférentes (II.). Ensuite, nous poserons la question de la définition de ces données en droit procédural pénal suisse : doivent-elles être qualifiées de « traces numériques » ou d'« enregistrements » au sens de l'art. 246 CPP ? La réponse à cette question est déterminante pour établir si la police est compétente pour mettre en sûreté ces données de manière autonome ou si un mandat de perquisition ordonné par le Ministère public s'avère nécessaire (III.). Enfin, nous aborderons la question de l'accessibilité d'un enregistreur de données en procédure pénale en nous appuyant sur le principe de transparence. Pour ce faire, nous analyserons une recommandation émise par la préposée cantonale à la transparence et à la protection des données du canton de Fribourg (ci-après : la préposée) ainsi que la décision subséquente de la Direction de la sécurité, de la justice et du sport du canton de Fribourg (ci-après : DSJS) (IV.).

II. L'« Event Data Recorder »

A. Aspects historiques

L'EDR est apparu aux États-Unis au début des années 1990, lorsque le producteur d'automobiles General Motors l'a installé dans le système de contrôle des airbags afin de collecter des informations, lors d'une décélération rapide ou d'un impact, permettant de déterminer si le déploiement des airbags était nécessaire¹². En 1991, la National Highway Traffic Safety Administration (ci-après :

³ Annexe 4 du règlement ONU N 160, 17.

⁴ STEFAN ZUBER, Event Data Recorder – endlich auch in Europa !(?), in : Hardy Landolt / Manfred Dähler (éd.), Jahrbuch zum Strassenverkehrsrecht 2023, Zurich / Saint-Gall 2023, 355 ss, N 18.

⁵ ANDRÉ BLANC et al., Digitale Unfallspuren im Event Data Recorder, in: ZSV / RCR 2/2022, 79 ss, 83.

⁶ BLANC (n. 5), 83 ; JOËLLE VUILLE / JÖRG ARNOLD, Moyens de preuve techniques et appréciation des preuves lors de la reconstruction d'accidents de la route, ZSV / RCR 2015 II, 51 ss, 52 (cité : Moyens).

⁷ Rapport explicatif de l'OFROU du 23 décembre 2023 sur la révision partielle du 22 décembre 2023 de l'ordonnance du 19 juin 1995 sur les exigences requises pour les véhicules routiers (OETV ; RS 741.41), ASTRA-D-33B23401/1225, 13 (cité : rapport explicatif).

⁸ Art. 11 al. 2 let. a OETV : les « voitures de tourisme » sont des voitures automobiles légères affectées au transport de personnes comptant neuf places assises, conducteur compris, au maximum (catégorie M₁ jusqu'à 3,50 t).

⁹ Art. 11 al. 2 let. e OETV : les « voitures de livraison » sont des voitures automobiles légères affectées au transport de choses (catégorie N₁), y compris celles qui sont équipées, dans le compartiment de charge, de sièges supplémentaires rabattables destinés au transport occasionnel et non professionnel de personnes, pour autant que le nombre total de places assises, siège du conducteur inclus, ne soit pas supérieur à 9.

¹⁰ Annexe II du règlement (UE) N 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, JO L 325 du 16 décembre 2019, 24.

¹¹ P. ex. les modèles de véhicules actuels provenant des USA disposent souvent d'EDR, dont l'équivalence doit être prouvée par le constructeur (cf. rapport explicatif, 13).

¹² VUILLE / ARNOLD (n. 6), Moyens, 52.

NHTSA) a commencé à expérimenter les EDR dans le cadre du programme Special Crash Investigations¹³. En 1997, le National Transportation Safety Board (ci-après : NTSB) recommande à la NHTSA d'utiliser les EDRs afin de « *gather more and better real-world data*¹⁴ ». La même année, le Jet Propulsion Laboratory de la NASA recommande à son tour à la NHTSA de « *study the feasibility of installing and obtaining crash data for safety analyses from crash recorders on vehicles*¹⁵ ». Le 28 août 2006, le Department of Transportation (ci-après : DOT) dont fait partie la NHTSA publie le règlement 49 Partie 563 du Code of Federal Regulations (ci-après : CFR) avec pour titre « EVENT DATA RECORDERS ».

Ce règlement contient une première liste de quinze catégories de données qui doivent obligatoirement être enregistrées dans l'EDR (il s'agit p. ex. de la vitesse du véhicule, de l'état des freins et du déclenchement de l'airbag)¹⁶, une seconde liste de 30 catégories de données qui doivent être consignées sous certaines conditions (« *if recorded* » ou « *if equipped* »), il s'agit p. ex. du statut des ceintures de sécurité¹⁷. Une troisième liste indique la portée, la précision et la résolution (« *range, accuracy, and resolution* ») en accord avec lesquelles les données des deux premières listes doivent être reportées¹⁸. Ce règlement est entré en vigueur le 1^{er} septembre 2012 pour la plupart des véhicules automobiles équipés¹⁹.

Au sein de l'ONU, le groupe de travail de la Commission économique pour l'Europe des Nations unies (CEE-ONU), nommé le World Forum for Harmonization of Vehicle Regulations (ou aussi appelé WP.29), a adopté lors de sa 183^e session, qui s'est tenue entre le 9 et le 11 mars 2021, une proposition de nouveau règlement ONU des EDR²⁰. Suivant cette dernière, le règlement

n° 160 de l'ONU, sur les prescriptions relatives à l'homologation des véhicules à moteur en ce qui concerne l'enregistreur de données de route, est entré en vigueur le 30 septembre 2021²¹. Ce règlement s'inspire fortement du règlement américain NHTSA 49 CFR Part. 563²².

Dans la foulée, le Parlement européen et le Conseil de l'UE ont repris le règlement n° 160 de l'ONU et l'ont intégré au sein du règlement (UE) n° 2019/2144 du 27 novembre 2019 qui prévoit l'utilisation d'un EDR sur les voitures et camionnettes neuves dès le 6 juillet 2022 (sur les autres véhicules neufs à partir de 2026) selon le calendrier instauré à l'annexe II²³. Le règlement délégué (UE) n° 2022/545 de la Commission européenne du 26 janvier 2022, dont l'art. 2 prévoit l'intégration du règlement n° 160 de l'ONU²⁴, encadre les méthodes de récupération des données ainsi que les normes de contrôle technique sur les véhicules légers (M₁ et N₁). En Suisse finalement, le règlement (UE) n° 2019/2144 et le règlement délégué (UE) n° 2022/545 ont été repris au sein de l'ordonnance concernant les exigences techniques requises pour les véhicules routiers (art. 102a al. 1 OETV et son annexe II) selon la modification du Conseil fédéral du 22 décembre 2023.

En droit américain, l'EDR est défini comme suit : « *Event Data recorder (EDR) means a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event. For the purposes of this definition, the event data do not include audio and video data*²⁵. » On retrouve la même définition au sein du règlement ONU n° 160, alors que le règlement (UE) n° 2019/2144 définit l'enregistreur de données d'événements de manière plus souple en tant qu'« *un système uniquement destiné à enregistrer et mémoriser les paramètres et informations critiques en rapport avec l'accident peu avant, pendant et immédiatement après une colli-*

¹³ « Final rule » sur le Titre 49 CFR Part. 563 de la NHTSA, publié au Federal Register, Vol. 71 N 166, le lundi 28 août 2006, NHTSA-2006-25666, 5097 ss, 5099.

¹⁴ HAMPRON C. GABLER et al., Use of Event Data Recorder (EDR) – Technology for Highway Crash – Data Analysis, document N 75 (projet 17-24) de la NHTSA, décembre 2004, 122.

¹⁵ CHIDESTER AUGUSTUS B., REAL WORLD EXPERIENCE WITH EVENT DATA RECORDERS, publié en juin 2001 par la NHTSA dans le cadre de la 17^e International Technical Conference on the Enhanced Safety of Vehicles Conference, disponible sous : https://www.nhtsa.gov/sites/nhtsa.gov/files/real_world_experience_with_event_data_recorders.pdf, consulté le 16 septembre 2024.

¹⁶ NHTSA 49 CFR Part. 563 chap. 563.7 Data elements Table I.

¹⁷ NHTSA 49 CFR Part. 563 chap. 563.7 Data elements Table II.

¹⁸ NHTSA 49 CFR Part. 563 chap. 563.8 Data elements Table III.

¹⁹ NHTSA 49 CFR Part. 563 chap. 563.3 Application.

²⁰ (WP.29) World Forum for the Harmonization of Vehicle Regulations (183^e session), (GRSG) Proposal for a new UN Regula-

tion on Event Data Recorder, ECE/TRANS/WP.29/2020/123/Rev.1.

²¹ Règlement ONU N 160, 3 ss

²² ZUBER (n. 4), N 11.

²³ Règlement (UE) N 2019/2144, 1 ss.

²⁴ Règlement délégué (UE) N 2022/545 de la Commission du 26 janvier 2022 complétant le règlement (UE) 2019/2144 du Parlement européen et du Conseil en établissant des règles détaillées relatives aux procédures d'essai et aux prescriptions techniques spécifiques pour la réception par type des véhicules à moteur en ce qui concerne leur enregistreur de données d'événements et pour la réception par type de ces systèmes en tant qu'entités techniques distinctes et modifiant l'annexe II dudit règlement, JO L 107 du 6 avril 2022, 18 ss.

²⁵ NHTSA 49 CFR Part. 563 chap. 563.5 Définitions let. b.

sion²⁶ ». Toutefois, le règlement délégué (UE) n° 2022/545 vient préciser cette définition en obligeant les ERD à être conformes aux prescriptions techniques énoncées dans le règlement ONU n° 160. Finalement, le droit suisse fait directement référence au règlement (UE) n° 2019/2144 et au règlement délégué (UE) n° 2022/545 pour définir l'EDR (art. 102a al. 1 OETV).

En ce qui concerne l'avenir de la législation, il convient de souligner que l'ONU a très récemment adopté le règlement n° 169, qui est entré en vigueur le 20 juin 2024²⁷. Ce dernier traite des normes relatives aux EDR dans les véhicules des catégories M₂, M₃, N₂ et N₃, soit principalement les autobus et les poids lourds. L'UE se prépare à adopter un nouveau règlement délégué intégrant le règlement n° 169, le projet ayant déjà été adopté par la Commission européenne le 26 juillet 2024²⁸. S'il devait être définitivement adopté, ce nouveau règlement délégué serait applicable à partir du 7 janvier 2026. Une adaptation de l'OETV pour intégrer ce dernier au droit suisse sera alors sans doute nécessaire.

Enfin, il convient de souligner que les EDR ont initialement été mis en place pour des questions de sécurité des véhicules comme produits : « *The purpose of this part is to help ensure that EDRs record, in a readily usable manner, data valuable for effective crash investigations and for analysis of safety equipment performance (e.g., advanced restraint systems). These data will help provide a better understanding of the circumstances in which crashes and injuries occur and will lead to safer vehicle designs*²⁹ ». En pratique, les assurances civiles prévoient parfois contrac-

tuellement d'accéder aux données issues des EDR en cas d'accident³⁰.

Toutefois, l'introduction récente de l'art. 102a OETV semble remettre cette possibilité en question, la loi donnant l'accès aux données aux « *autorités responsables de l'étude et l'analyse d'accidents* », sans plus de précisions. L'expression « *uniquement par les autorités responsables de ces tâches* » (« *von den für diese Aufgaben zuständigen Behörden* ») semble faire référence aux entités ayant une mission d'ordre public à l'étude et l'analyse des accidents. Cette question n'ayant aucunement été abordée lors de l'introduction de cette disposition³¹, il s'agit d'une interprétation littérale de notre part.

B. Aspects technico-légaux

L'EDR est un module électronique supplémentaire dans une unité de commande électronique existante (généralement l'airbag). Il ne constitue donc pas un dispositif autonome indépendant du véhicule. Sur le plan technique, l'EDR se distingue de la fameuse « boîte noire » que l'on retrouve notamment dans les avions (et parfois dans les trains et sur les navires) par le fait qu'il n'enregistre pas les données en continu tout au long du fonctionnement du véhicule, mais uniquement sur une courte période autour de l'accident³². La précision en droit américain selon laquelle l'EDR n'enregistre pas de données audio ou vidéo,

d'un véhicule donné à partir des données mémorisées », cf. Règlement (UE) N 2019/2144, N 13.

²⁶ Art. 3 n° 13 du Règlement (UE) N 2019/2144, 9.

²⁷ Règlement ONU N 169 – prescriptions uniformes relatives à l'homologation des enregistreurs de données de route pour véhicules utilitaires lourds [2024/1218], OJ L 2024/1218 du 23 mai 2024, 1 ss.

²⁸ Projet de règlement délégué complétant le règlement (UE) 2019/2144 du Parlement européen et du Conseil en établissant des règles détaillées relatives aux procédures d'essai et aux prescriptions techniques spécifiques pour la réception par type des véhicules à moteur lourds en ce qui concerne leur enregistreur de données de route et pour la réception par type de ces systèmes en tant qu'entités techniques distinctes et modifiant l'annexe II dudit règlement, adopté par la Commission européenne le 26 juillet 2024, C(2024)5214.

²⁹ NHTSA 49 CFR Part. 563 chap. 563.2 « Purpose ». On peut également citer : « *Ces données aideront à mieux comprendre dans quelles circonstances se produisent les accidents et les blessures et, ainsi, faciliteront la conception de véhicules plus sûrs* », cf. Règlement ONU N 160, N 0.3 ou encore : « *Ces enregistreurs devraient être capables d'enregistrer et de mémoriser les données de telle manière que celles-ci puissent être utilisées par les États membres uniquement afin de mener des analyses de sécurité routière et d'évaluer l'efficacité de mesures spécifiques qu'ils ont prises, sans permettre d'identifier le propriétaire ou le détenteur*

³⁰ Le prestataire AXA, p. ex., propose une option télématique intitulée « Safe Driver Bonus » qui lui permet d'accéder aux données issues des EDR afin de reconstituer les circonstances de l'accident. Cette option propose un rabais sur la prime d'assurance pour les jeunes conducteurs jusqu'à 25 ans. : <https://www.axa.ch/fr/particuliers/offres/vehicules-voyages/assurance-auto/assurance-jeunes-conducteurs.html> (consulté le 9 février 2024). Il existe également des modèles d'assurance auto beaucoup plus intrusifs en termes de protection des données (p. ex. « Pay as you drive » ou « Pay how you drive »). Pour en savoir plus à ce sujet : cf. VOLKER LÜDEMANN / CHRISTIN SENGSTÄCKEN / KERSTIN VOGELPOHL, Pay as you drive: Datenschutz in der Telematikversicherung, in: RDV 6/2014, 302 ss.

³¹ Le rapport explicatif, p. 13, confirme sans précision supplémentaire : « seules les autorités responsables de l'analyse des accidents ou de la réception par type sont autorisées à traiter les données ». De plus, le questionnaire envoyé lors de la procédure de consultation fédérale de cette révision partielle n'aborde pas la question (il s'agit du retour du canton de Vaud) : https://www.vd.ch/fileadmin/user_upload/organisation/dire/sg-dire/oe/OAE/Consultations/2022/65._Réponse_CE.pdf (consulté le 9 février 2025).

³² ZUBER (n. 4), N 17 ; EDR Q&As de la NHTSA du 11 août 2006, disponible sous : https://www.nhtsa.gov/sites/nhtsa.gov/files/edr_qas_11aug2006.pdf (consulté le 10 février 2024).

reprise depuis en droit européen et national, est capitale, les boîtes noires enregistrant parfois des communications radio ou des bruits environnants³³.

L'EDR doit être distingué de l'enregistreur de données au sens de l'art. 102 OETV. On peut distinguer à cet égard l'enregistreur de fin de parcours (« *Restwegaufzeichnungsggerät* » ; RAG) et l'enregistreur de données d'accident (« *Unfalldatenspeicher* » ; UDS), qui répondent aux exigences du législateur. Ces enregistreurs de données doivent enregistrer les paramètres définis à l'art. 102 al. 2 let. a-d OETV pendant au moins les 30 secondes ou les 250 mètres précédant un événement. Des paramètres supplémentaires peuvent être enregistrés, en fonction des besoins. L'enregistrement de ces paramètres à partir de la mémoire circulaire enregistrant en permanence – les anciennes données sont écrasées en continu – se fait manuellement. Contrairement au RAG, l'UDS dispose en outre de capteurs internes d'accélération et de vitesse de rotation. Ces capteurs permettent une analyse plus détaillée d'un accident, d'une part, et un enregistrement automatique des données à l'aide de valeurs seuils définies, d'autre part.

Pour récupérer les données enregistrées dans l'EDR, un Crash Data Retrieval a été développé par Vetronix Corporation, puis racheté par l'entreprise allemande Robert Bosch GmbH dans les années 2000. Cet appareil a été commercialisé par la suite sous le nom de « Bosch Crash Data Retrieval » (ci-après : Bosch CDR), il est aujourd'hui compatible avec la plupart des véhicules des constructeurs³⁴. Il est d'ailleurs possible de trouver actuellement en ligne un kit d'outils Bosch CDR contenant tout le matériel nécessaire (à l'exception du câble pour la lecture *direct to module*) pour effectuer une récupération des données issues d'un EDR pour une valeur de USD 5'900.00³⁵. Par conséquent, il est théoriquement possible pour un justiciable d'extraire lui-même les données d'un EDR en cas d'absence d'intervention de la police, pour les produire en procédure pénale ou auprès de son assurance civile pour prouver une éventuelle absence de faute.

III. « Traces numériques » ou « enregistrements » ?

A. Les différentes solutions

En cas d'accident, les traces de freinages, de peintures, d'impacts, etc. sont recueillies et mises en sécurité par la police sur la base de l'art. 306 al. 2 let. a CPP³⁶. L'intervention de la police dans ce cadre est indépendante et ne nécessite pas l'autorisation du Ministère public³⁷. En effet, la police doit pouvoir entreprendre les premières investigations même sans ordre du Ministère public³⁸. Dans ce contexte, les données issues de l'EDR pourraient ainsi être considérées comme des « traces » au sens de l'art. 306 al. 2 let. a CPP³⁹. Néanmoins, la question de l'applicabilité de l'art. 246 CPP se pose, car si les données provenant d'un EDR devaient être considérées comme des « enregistrements », alors une perquisition d'enregistrement devrait être prononcée.

Il convient de constater que les deux solutions aboutissent à un chemin procédural très différent. Dans le cadre de cet article, les Ministères publics des cantons ont été contactés afin de leur demander quelle était leur pratique à ce sujet. Si tous n'ont pas répondu, nous avons reçu de nombreux retours. Le « Forensisches Institut Zürich » (ci-après : le FOR) a également été contacté. Nous avons sélectionné les réponses qui, selon nous, méritaient une analyse plus approfondie.

1. La solution dite des « traces numériques »

La première solution analysée consiste à considérer les données extraites d'un EDR comme des « traces » qui doivent être mises en sûreté par la police au sens de l'art. 306 al. 2 let. a CPP. Cette solution doit selon nous être qualifiée de pragmatique, puisqu'elle considère à juste titre qu'il n'est pas possible de s'opposer à un éventuel mandat de perquisition des données issues de l'EDR par la mise sous scellés, aucun secret ne pouvant raisonnablement être invoqué au sens de l'art. 248 CPP.

En effet, la modification du 17 juin 2022 du CPP, entrée en vigueur le 1^{er} janvier 2024, définit de manière encore plus restrictive les motifs de mise sous scellés⁴⁰. À titre

³³ VUILLE / ARNOLD (n. 6), Moyens, 53.

³⁴ BLANC et al. (n. 5), 81 ; ANDREAS LEU / JÖRG ARNOLD, Le Kit Bosch (CDR) (Crash Data Retrieval Kit) – Lecture des données d'accidents à partir de véhicules modernes, Feuille spécialisée du « Forensisches Institut Zürich », 12^e éd., juin 2014 (version 2017).

³⁵ <https://crashdatagroup.com/collections/kits-bundles/products/bosch-cdr-900-dlc-tool-kit> (consulté le 9.02.2025).

³⁶ CR CPP-PAREIN, ART. 306 N 4.

³⁷ BSK StPO-GALELLA / RHYNER, art. 306 N 11.

³⁸ Message du Conseil fédéral du 21 décembre 2005 relatif à l'unification du droit de la procédure pénale, FF 2006 1057, 1244 (cité : Message CPP).

³⁹ BLANC et al. (n. 5), 88.

⁴⁰ Message du Conseil fédéral du 28 août 2019 concernant la modification du code de procédure pénale (mise en œuvre de

d'exemple de ce durcissement, le Tribunal fédéral a récemment indiqué qu'il ne considérerait plus les secrets dits « mous » (secret commercial, secret d'affaires, secret de fabrication, secret bancaire) comme des motifs de mise sous scellés, et ce que quel que soit le statut procédural de la personne qui les fait valoir⁴¹. En ce qui concerne les données issues d'un EDR, il convient de rappeler que ce dernier n'enregistre en principe les informations que cinq secondes avant l'événement⁴². Il est donc difficile d'imaginer quel secret pourrait être invoqué pour justifier la mise sous scellés au sens de l'art. 248 al. 1 CPP, surtout que le texte de ce dernier a été modifié pour que l'intéressé ne puisse plus invoquer « d'autres motifs » pour faire valoir son droit de refuser de déposer ou de témoigner. Cette modification a été effectuée parce qu'en pratique, le texte de loi à lui seul n'indiquait pas clairement dans quelles situations le justiciable pouvait demander la mise sous scellés⁴³. De même, quand bien même les données issues d'un EDR seraient qualifiées de « documents personnels » au sens de l'art. 264 al. 1 let. b CPP, l'intérêt public lié à la poursuite pénale primerait vraisemblablement sur l'intérêt de la personne concernée à la protection de sa sphère privée, en raison de la nature de ces données.

Le Tribunal fédéral est d'ailleurs d'avis que les objets qui ne sont manifestement pas protégés par un secret et qui ne se prêtent pas à une perquisition et à une levée de scellés peuvent être dispensés de scellés et le Ministère public peut les affecter à un autre usage⁴⁴. JOSITSCH et SCHMID estiment en effet que les objets qui ne sont ni des documents, ni des enregistrements, ni des supports de données et qui ne portent pas atteinte à des droits de confidentialité dignes de protection ne sont pas soumis à la perquisition au sens des art. 246 ss CPP, mais confisqués ou saisis⁴⁵. DELLAGANA-SABRY pense enfin que les documents et enregistrements incriminants et non couverts par un secret protégé ou par un autre motif peuvent faire l'objet

d'une perquisition contre laquelle l'opposition au sens de l'art. 248 CPP n'est pas possible⁴⁶. Par conséquent, il peut être argumenté que la police devrait librement pouvoir mettre en sûreté les données issues de l'EDR au sens de l'art. 306 al. 2 let. a CPP, puisque même dans l'hypothèse où une ordonnance de perquisition devrait être exigée, le justiciable ne pourrait pas justifier une mise sous scellés qui empêcherait l'autorité judiciaire d'obtenir finalement les données en question.

2. La solution dite des « enregistrements »

La seconde solution analysée consiste à considérer les données extraites d'un EDR comme des « enregistrements » devant être perquisitionnés au sens de l'art. 246 CPP. Selon nous, cette solution doit être qualifiée de prudente, car elle a le mérite de préserver l'intégrité de la procédure pénale dans l'éventualité où les données extraites ne peuvent être qualifiées de « traces numériques ». En effet, si les données de l'EDR devaient bien être qualifiées d'« enregistrement », alors une perquisition effectuée par la police sans mandat préalable et en l'absence de péril en la demeure contreviendrait à l'art. 241 al. 1 CPP.

À ce propos, l'art. 241 al. 3 CPP n'entre en ligne de compte que lorsqu'à défaut d'une perquisition immédiate, la perte du moyen de preuve est à craindre⁴⁷. Aussi, même si les données d'un EDR peuvent être abimées, nous nous rallions à l'opinion de KELLER qui considère qu'il est pratiquement exclu de retenir une urgence en cas de perquisition d'enregistrements, car il n'est guère probable que le Ministère public soit injoignable, au moins pour ordonner la perquisition des documents par oral⁴⁸. À titre d'exemple, il convient de relever que le Tribunal fédéral considère que la fouille d'un téléphone portable par des agents de police sans mandat constitue « *eine Durchsuchung von Aufzeichnungen im Sinne von Art. 246 StPO*⁴⁹ », peu importe la manière dont la perquisition a eu lieu⁵⁰. Enfin, il y a lieu de remarquer que l'exigence de mandat posée par l'art. 241 al. 1 CPP ne constitue pas toujours une prescription d'ordre dont la violation serait sans effet sur le caracté-

la motion 14.3383 de la Commission des affaires juridiques du Conseil des États « Adaptation du code de procédure pénale », FF 2019 6351, 6402 (cité : Message CPP Adaptation).

⁴¹ TF 7B_950/2024, 7B_976/2024 (15 novembre 2024), c. 2.4.2. Pour une analyse de cette jurisprudence : KATIA VILLARD, Secret d'affaires et secret bancaire ne suffisent plus (du tout), publié le 11 décembre 2024 par le Centre de droit bancaire et financier, disponible sous : <https://cdf.ch/1389/>, consulté le 28 décembre 2024.

⁴² JOËLLE VUILLE / JÖRG ARNOLD, L'appréciation des preuves techniques en matière de circulation routière – les traces numériques, in: ZSV / RCR 3/2019, 60 ss, 63 (cité : Appréciation).

⁴³ Message CPP Adaptation (n. 40), FF 2019 6402.

⁴⁴ ATF 144 IV 74, 79 s., c. 2.6.

⁴⁵ PK StPO-JOSITSCH / SCHMID, art. 246 N 1 ; du même avis : CR CPP-HOHL / CHIRAZI, art. 248 n°p 1.

⁴⁶ YASMINE DELLAGANA-SABRY, Perquisitions en procédure pénale, thèse Genève 2021, Genève / Zurich / Bâle 2021, 141.

⁴⁷ BSK StPO-GFELLER, art. 241 N 33 et 33a.

⁴⁸ ANDREAS J. KELLER, Kommentar zur Schweizerischen Strafprozessordnung StPO, art. 246 N 4.

⁴⁹ ATF 139 IV 128, c. 1.3.

⁵⁰ Soit en particulier que le téléphone mobile ait été déverrouillé à ce moment-là et que l'intéressé n'ait donc pas eu besoin de divulguer le code d'accès de son téléphone : cf. TF 7B_102/2024 (11 mars 2024), c. 2.4.4.

tère exploitable des preuves récoltées⁵¹. Il faut en effet se fonder sur les circonstances concrètes du cas d'espèce⁵². Par conséquent, il peut être argumenté que la police ne peut pas librement recueillir les données issues de l'EDR, et qu'elle doit disposer d'un mandat de perquisition écrit, ou au moins d'une confirmation orale de la part du Ministère public (éventuellement le tribunal du fond) au sens de l'art. 241 al. 1 CPP. En effet, il convient de souligner que, bien que la police ait un devoir de mettre en sûreté les traces et les preuves (art. 306 al. 2 let. a CPP), la perquisition est une mesure de contrainte au sens de l'art. 196 CPP, qui a également pour objectif de mettre les preuves en sûreté (art. 196 let. a CPP).

3. La solution dite « hybride »

Nous attribuons à cette dernière solution le qualificatif d'« hybride » car elle combine des éléments des deux solutions précédemment analysées. La solution hybride se compose de deux étapes. Dans un premier temps, les données issues de l'EDR sont considérées comme des « traces numériques » et doivent être mises en sûreté par la police au sens de l'art. 306 al. 2 let. a CPP. Dans un second temps, l'analyse des données récoltées est considérée comme une « *Durchsuchung der Aufzeichnungen* » : les données sont ainsi considérées comme un enregistrement et nécessitent un mandat de perquisition au sens de l'art. 246 CPP⁵³.

Cette solution doit selon nous être qualifiée de pratique, car elle a le mérite de se concentrer à la fois sur la conservation des données et sur le respect de l'intégrité de la procédure. Le raisonnement derrière ces deux étapes est le suivant : les données stockées dans l'EDR ne contiennent aucune indication sur le conducteur du véhicule, ni aucune information sur la localisation spatiale ou temporelle d'un événement⁵⁴. Aussi, la possibilité de mettre en relation des données de collision issues d'un EDR avec un conducteur n'est pas différente, au fond, de celle de mettre en relation des traces analogues (p. ex. des traces de freinage) avec un conducteur⁵⁵. Ces deux types de traces n'ont aucun rapport avec des pensées ou des idées humaines⁵⁶,

c'est pourquoi il ne s'agit pas d'« enregistrements » au sens du CPP.

En effet, bien que l'art. 306 al. 2 let. a CPP ne fasse pas la distinction entre « trace analogue » et « trace numérique », ce critère est important du point de vue de l'art. 246 CPP. La lettre de l'art. 246 CPP exprime de manière large la notion « d'enregistrements ». Le législateur a en effet voulu une formulation étendue afin que les progrès technologiques à venir en matière de stockage ou de traitement de données puissent encore être perquisitionnés⁵⁷. C'est pourquoi la majorité de la doctrine retient que les enregistrements englobent tous les supports de données, c'est-à-dire les supports d'expression de la pensée humaine, indépendamment de la manière dont ils sont stockés, en particulier ceux qui se trouvent sous forme électronique dans des supports de stockage⁵⁸. Il est donc judicieux que la direction de la procédure donne un mandat analogue à celui d'une perquisition d'enregistrements pour l'analyse des traces numériques par les experts⁵⁹.

B. Analyse critique

1. Prudence est mère de sûreté

Alors, quelle solution suivre ? La solution des traces numériques – pragmatique –, la solution des enregistrements – prudente –, ou la solution hybride – pratique – ? Pour répondre à cette question, il convient premièrement de rappeler que l'art. 246 CPP est une mesure de contrainte visant à mettre les preuves en sûreté au sens de l'art. 196 al. 1 let. a CPP. La perquisition de documents et enregistrements (art. 246 CPP) est un acte de procédure qui porte atteinte aux droits fondamentaux, en particulier à la sphère privée des personnes intéressées (art. 196 al. 1 CPP et 13 al. 1 Cst.)⁶⁰. Par conséquent, la perquisition doit être fondée sur une base légale, être justifiée par un intérêt public, être proportionnée au but visé et ne pas violer l'essence des droits fondamentaux (art. 36 Cst.)⁶¹. Il s'agit en effet d'une perquisition d'enregistrements au sens de l'art. 246 CPP lorsque les documents ou les sup-

⁵¹ TF 7B_102/2024 (11 mars 2024), c. 2.5.1.

⁵² BSK StPO-THORMANN / BRECHBÜHL, art. 246 N 6.

⁵³ Il s'agit notamment de la solution promue par le « Forensisches Institut Zürich ».

⁵⁴ VUILLE / ARNOLD (n. 42), Appréciation, 65.

⁵⁵ JÖRG ARNOLD, Digitale Spuren in Fahrzeugen die Zukunft ist bereits Realität Verkehrsunfalluntersuchung – neue Technologien und der Event Data Recorder, Kriminologie 12/2015, 742 ss, 745.

⁵⁶ ARNOLD (n. 55), 754 ; VUILLE / ARNOLD (n. 6), Moyens, nbp 17.

⁵⁷ HOHL / CHIRAZI (n. 45), N 17.

⁵⁸ DAMIAN K. GRAF, Praxishandbuch zur Siegelung: StPO inkl. revidierter Bestimmungen VStrR - IRSG - MStP, Berne 2022, N 35; DANIEL JOSITSCH, Grundriss des schweizerischen Strafprozessrechts, 4^e éd., Zurich / Saint-Gall, N 402; JO PITTELOU, Code de procédure pénale – Commentaire à l'usage des praticiens, art. 246-art. 248 N 559; KELLER (n. 48), art. 246 N 6.

⁵⁹ ARNOLD (n. 55), 745.

⁶⁰ TF 7B_102/2024 (11 mars 2024), c. 2.3.3.

⁶¹ Message CPP (n. 38), FF 2006 1197.

ports de données doivent être lus ou vus, compte tenu de leur contenu ou de leur nature, pour établir leur aptitude à prouver, pour les séquestrer ou pour les verser au dossier⁶². En vertu de l'art. 198 en relation avec l'art. 241 al. 1 CPP, de telles perquisitions de documents et de supports de données doivent être en principe ordonnées par le ministère public (éventuellement le tribunal du fond)⁶³.

Deuxièmement, il convient de préciser qu'en cas de perquisition, l'ayant droit doit pouvoir invoquer, en plus des éventuels secrets, des objections accessoires, telles que l'insuffisance des soupçons laissant présumer une infraction⁶⁴, l'absence de pertinence des objets et/ou documents séquestrés pour la procédure pénale, la violation du principe de proportionnalité et/ou l'illicéité de l'ordre de perquisition, puisqu'il n'est en principe pas admissible de pouvoir présenter au cours d'une procédure pénale des preuves obtenues de manière illicite⁶⁵ ou encore des privilèges et immunités internationaux et nationaux, qui jouissent en principe d'une protection complète, sous réserve notamment d'une levée de ceux-ci⁶⁶. Aussi, la voie du recours prévue à l'art. 393 CPP entre en ligne de compte si les griefs soulevés ne concernent aucun intérêt juridiquement protégé par le maintien du secret protégé par les scellés⁶⁷. Ce moyen de droit doit ainsi être ouvert, puisque l'intéressé ne peut défendre ses droits au cours d'une procédure de levée de scellés. Par conséquent, selon nous, la simple absence de motif de scellés ne suffit pas à écarter d'emblée la nécessité d'un mandat de perquisition, puisque d'autres motifs d'inexploitabilité doivent pouvoir être invoqués par le justiciable.

Troisièmement, il convient de répondre la question suivante : les données issues d'un EDR peuvent-elles être mises en relation avec une idée humaine ? À notre avis, la réponse est positive. En effet, bien que ces données ne caractérisent pas directement le conducteur, elles reflètent, selon nous, l'expression d'une pensée humaine : une soudaine accélération avant un accident révèle quelque chose sur l'intention du conducteur (p. ex. la volonté de commettre un suicide ou un attentat) tout comme un freinage peut traduire l'intention d'éviter un accident ou, pour reprendre l'hypothèse d'un suicide, un changement d'avis

au dernier moment. La difficulté réside en réalité dans l'interprétation des données selon la probable volonté du justiciable⁶⁸.

On peut objecter que des traces analogues, p. ex. de freinage, présentent les mêmes caractéristiques que leur contrepartie numérique enregistrée dans l'EDR, sans qu'elles ne puissent pour autant être qualifiées d'« enregistrements ». Toutefois, selon nous, la différence réside dans le support électronique. En effet, le législateur a voulu faire preuve de prudence face aux enjeux liés à la protection de la sphère privée dans le cadre de l'évolution des technologies⁶⁹. Par conséquent, les documents et enregistrements visés à l'art. 246 CPP correspondent à l'ensemble des supports d'information envisageable susceptible d'être utilisé comme moyen de preuve⁷⁰. En somme, cela concerne n'importe quelle information figurant sur n'importe quel support⁷¹. Le terme de « traces numériques » au sens de « trace » pour l'art. 306 al. 2 let. a CPP, doit être compris en opposition avec l'art. 246 CPP, et doit donc, selon nous, être réservé à des données n'ayant aucun rapport avec l'action humaine (p. ex. les données issues d'une machine mesurant la température).

C'est pourquoi, selon nous, il n'est pas possible de considérer dans un premier temps que des données issues d'un EDR ne reflètent pas l'expression des pensées du justiciable afin de pouvoir les mettre en sûreté, puis de considérer ces dernières comme un enregistrement au moment de l'exploitation des données. Le contraire reviendrait à admettre que les données en question acquièrent soudainement, une fois mises en sûreté, un rapport avec une idée humaine nécessitant la mise en place d'une mesure de contrainte portant atteinte à la sphère privée des personnes intéressées, en l'occurrence la perquisition. De plus, il convient de souligner qu'en tant que mesure de contrainte, l'art. 246 CPP a pour objectif de mettre les preuves en sûreté (art. 196 let. a CPP) et non d'autoriser leur analyse.

Finalement, la solution de l'enregistrement doit selon nous s'imposer, car elle respecte la lettre et l'esprit de la loi, spécialement de l'art. 246 CPP. Ce dernier a été conçu par le législateur comme étant le plus inclusif possible en prévision des futures avancées technologiques. Par conséquent, il convient selon nous d'opter pour la solution la plus prudente, en accord avec la volonté du législateur.

⁶² ATF 109 IV 154, c. 1.

⁶³ Message CPP (n. 38), FF 2006 1220.

⁶⁴ L'emploi d'un véhicule comporte des risques inhérent (art. 62 al. 1 LCR), il peut donc être argumenté qu'en cas d'accident, la présomption qu'une infraction ait été commise est grande. Néanmoins, cette présomption ne doit pas prendre le dessus sur la présomption d'innocence (art. 10 CPP).

⁶⁵ ATF 143 IV 270, c. 6 et 7.

⁶⁶ DELLAGANA-SABRY (n. 46), 142.

⁶⁷ TF 1B_550/2021 (13 janvier 2022), c. 3.1.2.

⁶⁸ Sur les difficultés d'interprétation des données issues d'un EDR: cf. VUILLE / ARNOLD (n. 42), *Appréciation*, 64 s.

⁶⁹ HOHL-CHIRAZI (n. 45), N 17.

⁷⁰ ATF 108 IV 76, c. 1

⁷¹ PITTELOU (n. 58), N 559; DANIEL JOSITSCH / NIKLAUS SCHMID, *Handbuch des schweizerischen Strafprozessrechts*, 4^e éd., Zurich / Saint-Gall 2023, N 1073; Message CPP (n. 38), 1220.

C. Quid de l'art. 102a al. 1 OETV ?

1. Une *lex specialis* ?

L'art. 102a al. 1 OETV prévoit expressément que les autorités responsables de l'étude et de l'analyse des accidents sont les seules à pouvoir traiter les données issues des EDR. Il est alors légitime de qualifier cet article de *lex specialis* par rapport au CPP, puisqu'il serait inutile d'introduire une disposition qui prévoit l'accès à ces données aux autorités si, d'un autre côté, le CPP prévoyait des limites à cet accès en imposant la nécessité d'un mandat de perquisition. Toutefois, cette conclusion se heurte à un obstacle pratique important.

L'obligation d'équiper les voitures d'une EDR introduite par l'art. 102a al. 1 OETV suit le même calendrier que l'UE. Ainsi, les voitures de tourisme et les voitures de livraison importées en Suisse doivent en être munies au plus tard dès la date d'importation du 7 juillet 2024. Pour les minibus, les autocars, les camions et les tracteurs à sellette, l'obligation s'appliquera à partir du 7 janvier 2029 au plus tard⁷². Néanmoins, la plupart des voitures de tourisme et de livraison actuellement en circulation et équipées d'un EDR ont été importées en Suisse avant le 7 juillet 2024. Par conséquent, l'obligation de l'art. 102a al. 1 OETV n'est, à l'heure actuelle, pas applicable à la très grande majorité des véhicules circulant en Suisse. Cette transition progressive implique donc une cohabitation temporaire entre les deux cadres juridiques jusqu'à ce que l'art. 102a OETV devienne pleinement applicable. Le même problème se présentera pour les véhicules des catégories M₂, M₃, N₂ et N₃, qui devront sans doute bientôt également être équipés d'un EDR en Suisse (*supra* II / A).

2. Des « données personnelles » au sens de la LPD ?

Il convient d'ajouter à ce stade que les données issues d'un EDR (102a OETV) ou d'un enregistreur de données (art. 102 OETV) peuvent selon nous être considérées comme des « données personnelles » au sens de l'art. 5 let. a LPD. Ces dernières sont définies comme « toutes les informations concernant une personne physique identifiée ou identifiable ». Il s'agit d'une large notion qui doit être interprétée de manière extensive⁷³. Bien que les informations contenues dans un EDR ne se rapportent pas directement au conducteur en tant qu'individu identifié⁷⁴, elles

sont néanmoins exploitées pour analyser et évaluer indirectement⁷⁵ son comportement au moment de l'accident. En l'espèce, les données EDR doivent être mises en relation avec le conducteur du véhicule concerné, puisqu'elles sont utilisées pour reconstituer ses actions (freinage, accélération, direction) et, par conséquent, évaluer sa responsabilité dans un accident⁷⁶. De plus, ces données ne sont pas analysées isolément, mais sont corrélées avec d'autres sources d'information, telles que les traces de freinage relevées sur la chaussée, les témoignages des personnes impliquées, les relevés de temps et de lieu permettant d'établir la chronologie des faits⁷⁷. Cette mise en relation avec des données analogues permet donc, à l'aide de moyens raisonnables⁷⁸, d'identifier le conducteur, confirmant ainsi leur caractère personnel⁷⁹. La personne concernée est identifiable lorsqu'il est possible de déduire à qui les données se rapportent, par corrélation d'informations ou en raison du contexte⁸⁰. L'art. 102a al. 1 OETV renforce par ailleurs cet argument, en prévoyant expressément que les données issues d'un EDR doivent être traitées conformément à la législation fédérale sur la protection des données par les « autorités responsables de ces tâches », sans que ces dernières ne soient identifiées plus clairement (cf. *supra* II/A). Ce renvoi législatif tend à démontrer que le législateur lui-même reconnaît la nature sensible de ces données.

À ce propos, il est important de rappeler que l'art. 2 al. 3 LPD dispose que les traitements de données personnelles effectués dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par des dispositions fédérales de procédure, ainsi que les droits des personnes concernées, obéissent au droit de procédure applicable. Une procédure est régie par les dispositions de

l'établissement de profils de personnalité. La réglementation est conforme au droit suisse de la protection des données et ne recèle aucun risque d'atteinte à un droit fondamental en la matière ».

⁷⁵ BSK DSG-BLECHTA / DAL MOLIN / WESIACK-SCHMIDT, art. 5 N 22.

⁷⁶ D'un avis similaire dans le contexte plus large du traitement de données télématiques par l'assurance véhicule : LARA BLUMER, *Telematik und Motorfahrzeugversicherung : Rahmenbedingungen und Vertragsgestaltung in der Schweiz*, Zurich / Genève 2024, N 221.

⁷⁷ Pour un exemple de mise en relation de données issues d'un EDR avec des données analogues : cf. ZUBER (n. 4), N 42 ss.

⁷⁸ Sachant néanmoins que le matériel nécessaire à l'extraction des données coûte, *pour l'instant*, plusieurs milliers de francs, le caractère « raisonnable » des moyens nécessaires peut être remis en question. Cette évaluation devra être réalisée selon l'ensemble des circonstances du cas d'espèces (cf. MEIER / TSCHUMY [n. 73], N 25).

⁷⁹ OFK DSG-GLASS, art. 5 N 14.

⁸⁰ PC LPD-JACOT-GUILLARMOD, art. 5 N 11.

⁷² Annexe II du règlement (UE) N 2019/2144, 24.

⁷³ CR LPD-MEIER / TSCHUMY, art. 5 N 19.

⁷⁴ Cf. rapport explicatif, p. 13 : « Seulement enregistrés en cas d'accident, ces éléments ne comportent pas d'informations sur les personnes impliquées et ne peuvent pas être utilisés pour

la procédure fédérale dès lors qu'un état de fait particulier est traité par une autorité conformément aux prescriptions de l'une de ces lois⁸¹. Par conséquent, la LPD ne s'applique en principe pas à la procédure pénale, qui est régie par le CPP⁸². Une application concurrente de la LPD aux droits procéduraux contreviendrait en effet au principe de la sécurité du droit, aurait pour conséquence un conflit de lois et retarderait inutilement les procédures⁸³. Après la clôture de la procédure pénale, l'art. 99 al. 1 CPP indique que le traitement des données, la procédure et les voies de droit sont régis par les dispositions fédérales et cantonales sur la protection des données. Les données issues des EDR deviennent donc des données personnelles au moment de leur extraction, qui dans la pratique survient, en règle générale, dans le cadre d'une procédure pénale, où la LPD ne s'applique pas.⁸⁴

IV. LTrans et accessibilité des données issues d'un EDR en procédure pénale : un exemple fribourgeois

A. Préambule

Nous trouvons pertinent de nous arrêter sur un cas fribourgeois où la LTrans a été invoquée afin d'accéder à l'enregistreur de données d'un véhicule de la police cantonale fribourgeoise pour servir de preuve dans le cadre d'une procédure judiciaire. Il convient de préciser à ce stade que les véhicules munis de feux bleus et d'un avertisseur à deux sons alternés (au sens des art. 78 al. 3 et 82 al. 2 OETV) doivent être équipés d'un enregistreur de données (art. 102 al. 1 OETV). Les exigences sont plus grandes que celles en vigueur dans le cadre de l'art. 102a al. 1 OETV, puisque l'enregistreur de données doit enregistrer la vitesse, le statut du feu stop et des clignoteurs de direction, le statut du feu bleu et de l'avertisseur à deux sons alternés ainsi que le statut du feu de croisement durant les trente secondes précédant un événement ou sur les 250 derniers mètres parcourus (art. 102 al. 2 OETV).

⁸¹ Message du Conseil fédéral du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6634.

⁸² Certaines preuves recueillies par des particuliers peuvent en revanche tomber sous le coup de la LPD (cf. ATF 146 IV 226 et arrêt 6B_768/2022 du 13 avril 2023). Pour en savoir plus à ce sujet : ALEXANDRE GUISAN / CÉLIAN HIRSCH, La surveillance secrète de l'employé – De la protection des données à la procédure pénale, SJZ/RSJ 115 (2019) Nr. 23, 707 ss.

⁸³ ATF 138 III 425, c. 4.3.

⁸⁴ CR LPD-MÉTILLE / DI TRIA, art. 2 N 62 ss.

Dans l'affaire qui nous occupe, la préposée à la transparence a rendu une recommandation le 10 mai 2023 conformément à l'art. 33 al. 2 LInf-FR, qu'elle a ensuite rendue publique en vertu de l'art. 41 al. 2 let. 2 LInf-FR. La police cantonale fribourgeoise a été contactée dans le cadre de cet article et a fourni des renseignements concernant la décision prise à la suite de cette recommandation, suivant l'art. 8 al. 1 let. b LInf-FR. Le 12 juin 2023, la police cantonale fribourgeoise a rendu une décision, contre laquelle un recours a été déposé auprès de la DSJS. La DSJS a ensuite rejeté ce recours. Elle nous a transmis une version anonymisée de sa décision du 22 novembre 2023. L'analyse portera donc sur la recommandation du 10 mai 2023, ainsi que sur cette dernière décision.

B. Recommandation du 10 mai 2023

1. Résumé des faits

La personne concernée (ci-après : la requérante) est entrée en collision début 2023 avec un véhicule de la police cantonale fribourgeoise lors d'une manœuvre dans un rond-point, endommageant son véhicule de manière importante. Le constat d'accident indique qu'elle s'est engagée alors que la police circulait déjà. Par courrier, elle a demandé les données du véhicule (vitesse, feux, sirène, vidéo) pour contester l'évaluation de son assurance, estimant que la police roulait trop vite. La police a refusé, indiquant que la sirène n'était pas activée, que le gyrophare l'était et que la vitesse (corrigée de 14 km/h, cf. art. 8 al. 2 let. c OCCR-OFROU) était de 16,27 km/h. Le véhicule n'était pas équipé d'une caméra. La requérante a ensuite réitéré sa demande, qui a de nouveau été refusée. Face à ce second refus, la requérante a saisi la préposée à la transparence. La médiation ayant échoué, une recommandation a été émise, articulée principalement autour de trois points.

2. Raisonement juridique

Premièrement, la préposée a estimé que les données issues du RAG du véhicule de police constituent un document officiel au sens de la LInf-FR⁸⁵. En effet, l'art. 22 al. 1 LInf-FR précise que constituent des documents of-

⁸⁵ Recommandation de la préposée du 10 mai 2023 – accès aux données enregistrées d'une voiture de police (art. 21 al. 1 let. a LInf – procédure de juridiction en cours), disponible (uniquement en allemand) sous : https://www.fr.ch/sites/default/files/2024-04/recommandation-du-10-mai-2023--acces-aux-donnees-enregistrees-dune-voiture-de-police-art-21-al-1-let-a-linf---procedure-de-juridiction-en-cours_0.pdf (consultée le 5 janvier 2025), N 17 à 20 (citée : Recommandation).

ficiels les informations enregistrées sur un support quelconque et qui concernent l'accomplissement d'une tâche publique. L'al. 2 ajoute que sont également réputés documents officiels les documents qui peuvent être établis par un traitement informatique en extrayant les informations concernées d'une base de données. Ainsi, les données en question ont été produites par la police dans l'exercice de ses fonctions, achevées et non destinées à un usage personnel (art. 22 al. 3 Llnf-FR) ou auxiliaire (art. 2 al. 2 de l'ordonnance fribourgeoise sur l'accès aux documents)⁸⁶.

Deuxièmement, la préposée a constaté que la requérante avait déposé une plainte pénale durant le mois de mai 2023 contre la police cantonale fribourgeoise. Il était donc possible que le document officiel demandé présente un lien étroit avec la procédure engagée. Si tel devait être le cas, la consultation du document serait régie par la législation spéciale (art. 21 al. 1 let. a Llnf-FR). Se fondant sur l'ATF 147 I 47, sur lequel nous reviendrons (cf. *infra* IV/D), la préposée était plutôt d'avis que la Llnf-FR s'appliquait au document demandé (« *Aus diesen Gründen neigt die Beauftragte eher der Ansicht zu, dass das InfoG auf den Zugang zum angeforderten Dokument anwendbar ist* »), le Tribunal fédéral semblant exclure qu'un document établi avant la procédure puisse « *se rapporter* » (« *beziehen* ») à celle-ci⁸⁷.

Troisièmement, la préposée a relevé que la police n'a pas invoqué d'intérêts publics prépondérants pour refuser l'accès au document. Cette dernière s'est contentée d'indiquer que le document contenait « *des éléments tactiques* » (« *taktische Elemente* ») qui sont « *de nature interne* » (« *interner Natur* »). La préposée reconnaît que cela est concevable en soi, mais elle précise qu'il incombait à la police de préciser quels sont ces « *éléments tactiques* ». Sur la base des informations dont elle dispose, elle déclare ne pas être en mesure d'apprécier si des intérêts publics s'opposent à l'accès au document officiel demandé⁸⁸.

C. Décision du 22 novembre 2023

1. Résumé des faits

En juin 2023, la police a ordonné la transmission à la requérante d'une synthèse de l'analyse visuelle des données du RAG du véhicule impliqué dans la collision, estimant qu'aucun intérêt public prépondérant ne justifiait le maintien du secret, malgré la procédure pénale en cours. La requérante a ensuite contesté l'utilisabilité de la synthèse

reçue en raison de l'échelle choisie et a demandé un fichier Excel. Puis, elle a déposé un recours contre la décision du mois de juin 2023, précisant qu'elle attendait la réponse de la police avant d'en exposer les motifs.

La requérante a par la suite complété son recours, invoquant une absence de motivation et une violation de son droit d'être entendue. Elle contestait l'existence d'un intérêt privé ou public prépondérant au maintien du secret et argue que le document fourni est insuffisant pour un spécialiste. Elle souligne aussi l'absence d'informations sur les feux de stop, clignotants, feux bleus et feux de croisement, et estime qu'aucun motif juridique ne justifie le refus d'accès complet au RAG.

Dans ses observations ultérieures, la police a suspendu le traitement de la demande jusqu'à la décision sur recours. Elle a précisé que les données UDS sont inaltérables et stockées dans douze unités de mémoire, chacune associée à un seul événement. Leur transmission partielle ou anonymisée est impossible, ce qui pourrait nuire à la réputation de la police et entraver son travail. Elle soutient que l'intérêt public prévaut sur celui de la requérante, les données UDS ne permettant pas, seules, de reconstituer précisément l'accident. Enfin, elle indique ne pas disposer d'un document Excel ni de personnel formé pour en établir un à partir de ce type de données.

2. Raisonnement juridique

La DSJS clarifie en préambule, d'une part, que le document officiel demandé par la requérante concerne les données issues d'un UDS, et non d'un RAG⁸⁹ et, d'autre part, que la police n'a pas refusé de transmettre lesdites données, mais en a limité l'accès.

La DSJS a tout d'abord examiné si la limitation de l'accès aux données UDS repose sur un intérêt public prépondérant au sens des art. 26 à 28 de la Llnf-FR (qui prévoient que l'accès à un document officiel peut être restreint si nécessaire pour protéger un intérêt public ou privé). Elle relève tout d'abord que la police ne conteste pas la trans-

⁸⁶ RSF 17.54.

⁸⁷ Recommandation (n. 85), N 21 à 24.

⁸⁸ Recommandation (n. 85), N 25 à 27.

⁸⁹ La DSJS explique que les véhicules équipés de feux bleus et d'un avertisseur à deux tons alternés ne peuvent plus être équipés d'un RAG depuis le 1^{er} janvier 2009 selon l'art. 222j al. 5 OETV. Cette dernière affirmation est pourtant fautive. L'art. 222j al. 5 OETV (disposition transitoire relative à la modification de l'OETV du 28 mars 2007) concerne l'enregistreur de fin de parcours (« *Restwegschreiber* ») et non les appareils d'enregistrement de données (« *Datenaufzeichnungsgerät* »). Depuis le 1^{er} juillet 2007, l'OETV fait donc la distinction entre l'enregistreur de fin de parcours (p. ex. un tachygraphe) et les appareils d'enregistrement de données (p. ex. le RAG ou l'UDS). Par conséquent, le RAG est bien un appareil conforme à l'art. 102 OETV.

mission des données relatives à l'accident. Cependant, elle invoque le fait que les données UDS ne peuvent être séparées, modifiées ou anonymisées, car l'art. 102 al. 3 OETV interdit toute altération ou suppression des enregistrements : « *Il doit être impossible d'effacer l'enregistrement et d'en falsifier le contenu.* » Selon la police, la transmission intégrale révélerait des événements non pertinents enregistrés dans l'UDS, ce qui pourrait nuire à la réputation de la police et compromettre la confidentialité des interventions policières. La DSJS conclut que la police cantonale a correctement appliqué le principe de proportionnalité (art. 20 al. 1 Llnf-FR) en fournissant un document PDF contenant uniquement les données UDS de l'accident, plutôt que de refuser totalement l'accès.

La DSJS a ensuite examiné la demande de la requérante visant à obtenir un fichier Excel. Elle relève en premier lieu que la police ne dispose pas d'un tel document et n'a pas l'obligation légale d'en créer un (art. 20 al. 1 Llnf-FR). La production d'un tel document nécessiterait des compétences spécifiques que le personnel ne possède pas, représentant une charge de travail disproportionnée (art. 26 al. 2 let. b Llnf-FR). Elle confirme donc le refus de transmettre les données UDS au format Excel.

Enfin, la DSJS a examiné si la police avait violé le droit d'être entendu de la requérante. Cette dernière soutient en effet que la police n'a pas suffisamment motivé sa décision. Cependant, la DSJS relève que la requérante a eu l'occasion de s'exprimer lors d'un entretien de conciliation et a pu compléter son recours. En conséquence, elle estime que, même si une violation avait eu lieu, elle aurait été réparée par la procédure.

En conclusion, la DSJS a intégralement rejeté le recours.

D. Analyse critique : instantanéité v. accessibilité

Pour établir sa recommandation, la préposée s'est inspirée de l'ATF 147 I 47, qui clarifie l'application du principe de transparence aux documents se rapportant à une procédure en cours. Dans cet arrêt, le Tribunal fédéral a interprété l'art. 69 al. 2 de la Convention intercantonale sur la protection des données et le principe de transparence des cantons du Jura et de Neuchâtel (CPDT-JUNE)⁹⁰, qui soumet l'accès aux documents liés à des procédures en cours aux règles procédurales spécifiques. En l'occurrence, il s'agissait d'un rapport d'audit sur deux entreprises subventionnées, dont un journaliste demandait la publication, bien qu'il ait été versé à une procédure pénale et

civile⁹¹. Le Tribunal fédéral s'est d'abord référé au message du Conseil fédéral relatif l'art. 7 al. 1 let. a LTrans⁹² et aux recommandations du préposé fédéral à la protection des données et à la transparence du 2 décembre 2019, qui soulignent que la LTrans ne doit pas contourner les règles spécifiques d'accès aux documents judiciaires. Notre Haute Cour a ainsi établi une distinction entre (i) les documents créés en dehors d'une procédure et (ii) ceux expressément ordonnés dans le cadre d'une procédure⁹³. Seuls ces derniers échappent donc au principe de transparence⁹⁴. Le Tribunal fédéral a également précisé que des documents servant uniquement de moyens de preuve et qui ne sont ni directement en relation avec la décision attaquée ni étroitement liés à l'objet du litige ne suffisent pas à exclure la LTrans, sauf s'ils présentent un lien direct avec la décision attaquée ou l'objet du litige⁹⁵.

L'interprétation de l'ATF 147 I 47 selon laquelle un document établi avant la procédure pénale ne peut pas présenter un lien étroit avec celle-ci soulève une incohérence entre l'accès aux données issues d'un enregistreur de données au sens de l'art. 102 OETV via le principe de transparence et leur obtention par l'autorité pénale. Selon nous en effet, un mandat de perquisition au sens de l'art. 246 CPP est nécessaire pour obtenir ces données dans le cadre d'une procédure pénale. Pourtant, grâce au principe de transparence, une personne impliquée dans un accident avec un véhicule disposant d'un enregistreur de données (art. 102 OETV) ou un véhicule de fonction disposant d'un EDR (art. 102a OETV) pourrait toujours y accéder en raison du moment de leur établissement. Ces données « naissent » en effet lors de l'accident, donc avant toute procédure pénale. En conséquence, ces données ne peuvent jamais présenter un lien étroit avec la procédure pénale. Toutefois, cela crée une inégalité de traitement : les fonctionnaires conduisant un véhicule équipé selon l'art. 102 ou l'art. 102a OETV devraient *de facto* toujours supporter cette atteinte à leur sphère privée, alors que les autres justiciables peuvent se prévaloir d'un mandat de

⁹¹ ATF 147 I 47, c. A à G.

⁹² Message du 12 février 2003 relatif à la loi fédérale sur la transparence de l'administration (Loi sur la transparence, LTrans), FF 2003 1807, 1850.

⁹³ MARKUS KERN / TOBIAS EGLI, Aktuelle Rechtsprechung im Datenschutzrecht, in: Astrid Epiney / Sophie Moser / Sophia Rovelli (éd.), Die Revision des Datenschutzgesetzes des Bundes, Forum Europarecht n° 43, 2022, 107 ss, 108.

⁹⁴ CÉLIAN HIRSCH, L'accès à un document officiel lors d'une procédure pendante, disponible sous : <https://lawinside.ch/1014/> (consulté le 6 janvier 2025).

⁹⁵ Recommandation du préposé fédéral à la protection des données et à la transparence du 2 décembre 2019, ch. 15 ; ATF 147 I 47, c. 3.4.

⁹⁰ RS/NE 150.30.

perquisition pour faire valoir des motifs d'inexploitabilité. Le seul devoir d'exemplarité de l'Etat nous semble insuffisant pour justifier une telle différence de traitement. Aussi, bien que la décision de la DSJS apporte une nuance à cette dernière analyse, puisque celle-ci a jugé que la transmission complète des données pouvait porter atteinte à des intérêts publics prépondérants, il convient de souligner qu'une synthèse des données a tout de même dû être transmise, en respect du principe de proportionnalité. Il convient pourtant de reconnaître que les données en question sont, en règle générale⁹⁶, produites explicitement en vue d'une procédure judiciaire⁹⁷. C'est pourquoi nous proposons d'interpréter l'ATF 147 I 47 de manière qu'un document officiel qui (1) nécessite habituellement une mesure de contrainte (art. 196 ss CPP) pour être obtenu dans le cadre d'une procédure pénale et (2) dont la production est clairement destinée à l'autorité de poursuite pénale soit considéré comme présentant un lien étroit avec celle-ci. Cette approche assurerait une articulation plus équilibrée entre le principe de transparence et les exigences de la procédure pénale, afin d'éviter de contourner cette dernière. En effet, dans le cadre de l'affaire en cause, il ne faisait aucun doute que la production de ce document officiel visait à servir de moyen de preuve au sein de la procédure pénale.

V. Conclusion

À l'issue de cette analyse, nous estimons que les données provenant des EDR doivent être considérées comme des « enregistrements » au sens du CPP, par précaution. En effet, la technologie évolue à un rythme tel que ce qui aujourd'hui semble anodin, voire insignifiant pour la sphère privée, pourrait un jour devenir bien plus intrusif, par exemple si des sons ou des images étaient captés. Qu'en sera-t-il lorsque les secondes précédant un événement passeront de 10 à 60, puis à plusieurs heures ? Quid du jour où la localisation sera également nécessaire ? Pour clore cette réflexion, nous citerons un extrait d'une revue américaine datant de 15 ans, qui aborde la question de l'accessibilité des données issues des EDR en procédure pénale avec les mêmes termes, montrant ainsi que les technologies progressent plus rapidement que la législation censée les encadrer :

« Notwithstanding the lack of legislation protecting the right of an owner to control EDR data, the practice in many crash investigations is for law enforcement officers to request authorization from the vehicle owner to download the data, presumably to avoid Fourth Amendment challenges in criminal proceeding⁹⁸. »

⁹⁶ Comme nous l'avons vu, certaines assurances responsabilité civile prévoient parfois l'accès à ces données.

⁹⁷ ATF 147 I 47, c. 3.4.

⁹⁸ MARK A FREDRICKSON / PETER L. GREGORY / ROGER J. BURGMIEIER, *Event Data Recorder in auto-accident litigation*, in: *Minnesota Defense Spring 2010*, 3 ss, 5.