39e Conférence internationale des commissaires à la protection des données et de la vie privée

Hong Kong, du 26 au 27 septembre 2017

Résolution sur la protection des données dans les véhicules automatisés et connectés

Auteur de la proposition :

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Commissaire fédéral à la protection des données et à la liberté d'information, Allemagne

Coparrains :

- **Commission Nationale de l'Informatique et des Libertés (CNIL)**
  Autorité de protection des données, France
- **Le Commissaire à la protection de la vie privée pour les données personnelles, Hong Kong, Chine**
- **Garante per la protezione dei dati personali**
  Autorité de protection des données, Italie
- **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)**
  Institut national pour la transparence, l'accès à l'information et la protection des données personnelles, Mexique
- **Commissariat à la protection de la vie privée, Nouvelle-Zélande**
- **Informacijski pooblaščenec Republike Slovenije**
  Commissaire à l'information de la République de Slovénie
- **Commissariat à l'information, Royaume-Uni**

Reconnaissant que les véhicules automatisés et connectés peuvent procurer d'importants avantages aux utilisateurs en raison de leur grande facilité d'utilisation ou commodité, et qu'ils peuvent aussi être avantageux pour la population en général en permettant

d'améliorer la circulation ainsi que la sécurité des conducteurs et des passagers des véhicules, des autres usagers de la route et des piétons;

Soulignant l'avancement rapide des technologies d'automatisation et de connexion de véhicules, permettant l'élaboration et le lancement de produits, de dispositifs ou de services de télématique nouveaux et innovateurs qui, dans bien des cas, incluront la collecte et le traitement de données personnelles rendus possibles par divers capteurs qui y sont installés, ce qui pourrait représenter de nouveaux défis pour les droits fondamentaux à la protection des données personnelles et de la vie privée des utilisateurs, en particulier dans les différents contextes où les véhicules peuvent être utilisés par de nombreuses personnes;

Considérant la déclaration issue de la réunion des ministres des Transports du G7 et du commissaire européen aux Transports qui a eu lieu à Cagliari, en Italie, les 21 et 22 juin 2017[1], qui reconnaît la nécessité de suivre les lignes directrices pertinentes en vigueur à propos de la cybersécurité et de la protection des données, et encourage tous les acteurs à évaluer comment les données nécessaires peuvent être utilisées p élaborer des services et des applications qui amélioreront la sécurité et les conditions de trafic tout en respectant les intérêts des consommateurs en matière de cybersécurité et de protection de la vie privée;

Considérant la déclaration issue de la réunion des ministres responsables de l'Économie numérique du G20 tenue à Düsseldorf, en Allemagne, les 6 et 7 avril 2017, sur la numérisation pour un monde interconnecté[2], qui reconnaît la nécessité de renforcer la confiance à l'égard de l'économie numérique en respectant les cadres juridiques de protection des données et de la vie privée, et en accroissant la sécurité dans l'utilisation des technologies de l'information et de la communication, ainsi que la transparence et la protection des consommateurs;

Préoccupée par le manque apparent de mécanismes d'information, de choix pour les utilisateurs, de contrôle de données et de consentement valide qui permettraient aux propriétaires, aux conducteurs et aux passagers de véhicules, aux autres usagers de la route et aux piétons de contrôler l'accès aux données des véhicules et aux données relatives à la conduite, ainsi que leur utilisation;

Observant le développement de différentes technologies de systèmes de transport intelligents coopératifs faisant en sorte que des véhicules transmettent leurs données positionnelles et cinématiques en diffusant continuellement de l'information à d'autres véhicules (v2v), à l'infrastructure de transport (v2i) ou à d'autres entités tierces (v2x) pour

[1] http://www.g7italy.it/sites/default/files/documents/Final Declaration_0.pdf

[2] https://www.bmwi.de/Redaktion/DE/Downloads/G/g20-digital-economy-ministerial-declaration-english-version.pdf?__blob=publicationFile&v=12

constituer un portrait global de la situation de trafic afin de favoriser la sécurité et la fluidité de la circulation;

Préoccupée par la possibilité que la diffusion de données par les véhicules, sans restrictions ni distinctions, dans le contexte des communications v2v, v2i et v2x, pourrait entraîner l'accès non autorisé aux données personnelles des conducteurs, des passagers ou d'autres personnes par des tiers, ou leur traitement ultérieur;

Soulignant toutefois que les technologies des systèmes de transport intelligents coopératifs doivent être conçus de manière à permettre la traçabilité et l'authentification des véhicules;

Reconnaissant que les concepteurs des différentes technologies des systèmes de transport intelligents coopératifs sont conscients des risques d'atteinte à la vie privée découlant de ces technologies et ont déployé des efforts considérables pour minimiser ces risques en recourant à la pseudonymisation et à d'autres méthodes qui réduisent la quantité de données personnelles et le risque d'identification;

Soulignant qu'une vaste collecte de données transmises dans un système de véhicules connectés incluant un système de transport intelligent coopératif peut non seulement entraîner l'accumulation des profils de déplacement de particuliers, mais aussi créer de grandes quantités de données concernant l'évaluation des comportements relatifs à la conduite, qui pourraient constituer des renseignements valables pour certaines entités, par exemple les compagnies d'assurance automobile, les constructeurs de véhicules, les publicitaires et les organismes d'application de la loi et de la sécurité routière, en particulier lorsque les données seront personnalisées, par exemple par l'utilisation d'identificateurs de véhicule de diffusion;

Mentionnant les solutions intégrant des pratiques exemplaires qui sont utilisées pour la télédiffusion et la communication radio numérique des services de police afin de restreindre l'accès à l'information diffusée aux destinataires autorisés;

Observant que les commissaires à la protection des données et de la vie privée fournissent des orientations précises quant aux règles de confidentialité applicables au traitement ou aux solutions concernant les véhicules automatisés et connectés;

Soulignant que le Forum mondial de l'harmonisation des règlements concernant les véhicules a inclus des lignes directrices sur la cybersécurité et la protection des données dans sa résolution d'ensemble sur la construction des véhicules (R.E.3)[3] en tant qu'annexe 6;

Réaffirmant la résolution sur le profilage[4] adoptée par la 35e Conférence internationale des commissaires à la protection des données et de la vie privée en 2013 à Varsovie ainsi que la

[3] https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r5f.pdf

[4] https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution-FR.pdf

résolution sur les mégadonnées adoptée à la 36e Conférence internationale à Fort Balaclava, à Maurice[5];

La 39e Conférence internationale des commissaires à la protection des données et de la vie privée invite toutes les parties concernées, notamment :

- **les organismes de normalisation;**
- **les autorités publiques,**
- **les constructeurs de véhicules et les fabricants d'équipement,**
- **les fournisseurs de services axés sur les données, par exemple les services de reconnaissance de la parole, de navigation, de télémaintenance ou de télématique pour l'assurance automobile,**

à respecter intégralement les droits fondamentaux que possèdent les utilisateurs pour la protection de leurs données personnelles et de leur vie privée, et à en tenir compte comme il se doit à toutes les étapes de la création et du développement de nouveaux dispositifs ou services.

Les parties susmentionnées sont donc exhortées à :

1. prendre en considération les attentes raisonnables des utilisateurs de véhicules relativement à la transparence et au contexte du traitement des données,
2. recourir à des mesures d'anonymisation ou de pseudonymisation pour réduire au minimum la quantité de données personnelles,
3. conserver les données personnelles uniquement pendant la période de temps qui est nécessaire pour les fins auxquelles elles sont traitées,
4. fournir des moyens techniques pour supprimer les données personnelles lorsqu'un véhicule est sur le point d'être vendu ou retourné à son propriétaire,
5. fournir des contrôles de la confidentialité précis et faciles à utiliser par les utilisateurs de véhicules, pour que ces personnes puissent accorder ou empêcher l'accès à différentes catégories de données dans les véhicules,
6. fournir des moyens techniques permettant aux utilisateurs de véhicules de restreindre la collecte de données,

[5] https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Big-Data-French.pdf

7. fournir des dispositifs sécuritaires de stockage de données qui assurent aux utilisateurs de véhicules le contrôle intégral de l'accès aux données recueillies par leurs véhicules,

8. prévoir des mesures techniques pour des composantes sécuritaires de communication en ligne qui protègent contre les cyberattaques et empêchent l'accès non autorisé aux données personnelles ainsi que leur interception,

9. élaborer et mettre en œuvre des technologies pour des systèmes de transport coopératifs intelligents de manière à :

    a. prévenir l'accès non autorisé aux données personnelles recueillies par des véhicules (v2v), l'infrastructure de transport (v2i) ou d'autres entités tierces (v2x) et l'interception de ces données,

    b. permettre aux utilisateurs de véhicules d'empêcher la diffusion de données positionnelles et cinématiques tout en continuant à recevoir des avertissements concernant des dangers de la route,

    c. protéger contre les activités illégales de repérage et de localisation de conducteurs,

    d. s'assurer que les mécanismes de sécurité pour les communications v2v, v2i et v2x pendant les processus d'authentication ne posent pas d'autres risques par rapport à la protection des données personnelles et de la vie privée,

    e. limitent le risque du repérage des véhicules et de l'identification des conducteurs.

10. concevoir des technologies et des architectures de protection de la vie privée qui traitent adéquatement les données personnelles dans les véhicules,

11. offrir aux utilisateurs de véhicules des modes de conduite protégeant la confidentialité et incluant des paramètres réglés par défaut,

12. effectuer des évaluations de l'incidence sur la protection des données pour des activités nouvelles, innovatrices ou risquées d'élaboration ou d'application de ces technologies,

13. promouvoir le respect de la confidentialité des données personnelles des utilisateurs de véhicules en assurant le traitement responsable de ces données, en tenant dûment compte des torts que le traitement et l'utilisation pourraient causer aux utilisateurs de véhicules,

14. engager un dialogue avec les commissaires à la protection des données et de la vie privée pour élaborer des outils de conformité se rapportant au traitement relatif aux véhicules connectés et assurer une certitude juridique dans ce domaine.