Nations Unies ECE/TRANS/WP.29/2017/46

Conseil économique et social

Distr. générale
23 décembre 2016
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Forum mondial de l'harmonisation des Règlements concernant les véhicules

171e session
Genève, 14-17 mars 2017
Point 4.14 de l'ordre du jour provisoire
Accord de 1958 :
Propositions d'amendements à la Résolution d'ensemble sur la construction des véhicules (R.E.3) soumises par les groupes de travail au Forum mondial pour examen

Proposition de projet de directive sur la cybersécurité et la protection des données

Communication du groupe de travail informel des systèmes de transport intelligents et de la conduite automatisée*

Le texte ci-après a été établi par l'expert du groupe de travail informel des systèmes de transport intelligents et de la conduite automatisée (ITS/AD). Il est fondé sur le document de travail ITS/AD-10-11-Rev.1, distribué lors de la dixième session du groupe de travail informel ITS/AD. Le groupe de travail propose au Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29) d'adopter à sa session de mars 2017 cette directive sur la cybersécurité et la protection des données.

* Conformément au programme de travail du Comité des transports intérieurs pour la période 2016-2017 (ECE/TRANS/254, par. 159, et ECE/TRANS/2016/28/Add.1, module 3.1), le Forum mondial a pour mission d'élaborer, d'harmoniser et de mettre à jour les Règlements en vue d'améliorer les caractéristiques fonctionnelles des véhicules. Le présent document est soumis dans le cadre de ce mandat.

GE.16-22882 (F) 180117 180117
1622882

I. Proposition

« Directive sur la cybersécurité et la protection des données

Directive relative aux mesures visant à garantir la cybersécurité et la protection des données des véhicules connectés et des véhicules à conduite automatisée

1. Préambule

1.1 La numérisation de la mobilité et l'augmentation du volume de données qui en résulte s'accompagnent de nouvelles exigences applicables à la sécurité des véhicules et aux infrastructures ainsi qu'à la protection des droits et des libertés des personnes auxquelles se rapportent ces données.

1.2 Les questions de cybersécurité et de cryptage des données prendront une importance croissante à mesure que l'automatisation et l'interconnectivité des fonctions de conduite se développeront.

1.3 Les véhicules connectés et les véhicules à conduite automatisée doivent donc être régis par des réglementations claires en matière de cybersécurité et de protection des données. L'objectif est de veiller à ce que les véhicules soient protégés contre les interférences et les manipulations extérieures.

1.4 La directive dont il est question ici vise à présenter les prescriptions dans ce domaine aux constructeurs automobiles, aux fournisseurs de composants et de systèmes installés sur des véhicules ainsi qu'aux prestataires de services pour ces systèmes, afin de garantir un degré élevé de cybersécurité et de protection des données. D'autres méthodes peuvent toutefois être utilisées, à condition de démontrer qu'elles garantissent un niveau de sécurité au moins équivalent.

1.5 La présente directive constitue un document d'orientation provisoire en attendant l'aboutissement des activités menées en collaboration et des travaux de recherche en cours, ainsi que l'élaboration de prescriptions plus détaillées harmonisées au niveau mondial sur la cybersécurité et la protection des données.

1.6 La présente directive doit servir de base à l'élaboration de prescriptions, dans le cadre des Règlements de l'ONU, visant à garantir la cybersécurité et la protection des données.

1.7 La présente directive n'a pas d'incidences sur les lois existantes relatives à la protection des données. Elle ne vise pas à amoindrir ou à renforcer les dispositions juridiques relatives à la protection des données.

2. Champ d'application

2.1 La présente directive porte sur les mesures applicables aux véhicules connectés et aux véhicules à conduite automatisée en ce qui concerne la cybersécurité et la protection des données.

3. Définitions

3.1 (Réservé)

3.2 On entend par "*véhicule connecté*" un véhicule équipé d'un dispositif destiné à permettre une connexion ou une communication sans fil (éventuellement à l'usage de la conduite automatisée) avec des dispositifs externes, des véhicules, des réseaux ou des services.

3.3 On entend par "*cybersécurité*" la préservation du caractère confidentiel, de l'intégrité et de la disponibilité des informations dans le "cyberespace", c'est-à-dire dans l'environnement complexe résultant de l'interaction des personnes, des logiciels et des services (par exemple sur Internet) au moyen de dispositifs technologiques et de réseaux associés à ceux-ci, cet environnement n'existant pas sous une forme physique.

3.4 On entend par "*protection des données*" la protection du droit d'une personne physique au respect de sa vie privée et familiale, de son domicile et de ses communications pour ce qui concerne le traitement des données à caractère personnel.

3.5 On entend par "*personne concernée*" la personne à laquelle se rapportent des données à caractère personnel (par exemple, les propriétaires ou les conducteurs de véhicules).

3.6 On entend par "*protection des données par défaut*" l'obligation pour un contrôleur d'appliquer des mesures techniques et organisationnelles garantissant que, par défaut, seules les données à caractère personnel nécessaires à la réalisation d'un objectif spécifique du traitement puissent être traitées.

3.7 On entend par "*protection des données dès la conception*" l'obligation pour un contrôleur d'appliquer des mesures techniques et organisationnelles appropriées à son activité de traitement afin d'appliquer les principes de protection des données pour protéger les droits des personnes concernées en réduisant la probabilité et la gravité du risque pour leur vie privée et familiale ainsi que pour le caractère privé de leur domicile et de leurs communications.

4. Prescriptions énoncées par la directive

Les véhicules connectés et les véhicules à conduite automatisée doivent faire l'objet de mesures visant à garantir la cybersécurité et la protection des données et doivent satisfaire aux prescriptions énoncées ci-après.

4.1 Généralités :

a) Le droit de toute personne au respect de sa vie privée et du caractère privé de ses communications doit être respecté ;

b) Les données à caractère personnel doivent être traitées en toute légalité, dans la transparence et de manière équitable à l'égard des personnes concernées ;

c) Les constructeurs automobiles, les fournisseurs de composants et de systèmes ainsi que les prestataires de services doivent respecter les principes de la protection des données par défaut et de la protection des données dès la conception (voir les définitions 3.6 et 3.7) ;

d) Les constructeurs automobiles, les fournisseurs de composants et de systèmes ainsi que les prestataires de services doivent veiller à ce qu'une protection adéquate soit assurée contre la manipulation et l'utilisation abusive de la structure technique ainsi que des données et des processus ;

e) Afin de prévenir tout accès non autorisé aux véhicules par le "cyberespace", les constructeurs automobiles, les fournisseurs de composants et de systèmes ainsi que les prestataires de services doivent garantir la sécurité du chiffrement des données et des communications ;

f) Le système doit être accessible à la vérification, au moyen d'un audit indépendant autorisé, des mesures appliquées par les constructeurs automobiles, les fournisseurs de composants et de systèmes ainsi que par les prestataires de services pour garantir la cybersécurité et la protection des données.

4.2 Protection des données

4.2.1 Le principe de légalité, d'équité et de transparence du traitement des données à caractère personnel implique en particulier :

a) Le respect de l'identité et de la vie privée de la personne concernée ;

b) L'interdiction d'exercer une discrimination à l'égard d'une personne sur la base de données à caractère personnel ;

c) La prise en considération des attentes raisonnables des personnes concernées s'agissant de la transparence et des conditions de traitement des données ;

d) Le maintien de l'intégrité et de la fiabilité des systèmes informatiques et, en particulier, l'interdiction de manipuler secrètement le traitement des données ;

e) La reconnaissance des avantages d'un traitement des données reposant sur la liberté en matière de circulation des données, de communication et d'innovation, pour autant que les personnes concernées soient tenues de respecter le principe du traitement des données à caractère personnel à des fins relatives à l'intérêt public supérieur ;

f) La préservation des données sur la mobilité des personnes, compte tenu des besoins et des finalités.

4.2.2 Les moyens offerts par les techniques permettant l'anonymat ou le recours aux pseudonymes doivent être utilisés.

Les personnes concernées doivent recevoir des informations complètes précisant quelles données sont collectées et traitées dans le cadre de la mise sur le marché de véhicules connectés et de véhicules à conduite automatisée, à quelles fins et par qui. Les personnes concernées doivent donner leur consentement à la collecte et au traitement de leurs données en toute connaissance de cause et sur une base volontaire.

4.2.3 La collecte et le traitement de données à caractère personnel doivent être limités aux données qui sont utiles dans le contexte de ladite collecte. Le cas échéant, la personne concernée doit avoir le droit de retirer son consentement si les fonctions visées ne sont pas nécessaires pour le fonctionnement de son véhicule ou pour la sécurité routière.

4.2.4 En outre, des mesures et des procédures techniques et organisationnelles appropriées visant à garantir le respect de la vie privée de la personne concernée doivent être mises en œuvre tant au moment de la détermination des moyens de traitement que lors du traitement lui-même. La conception des systèmes de traitement des données installés dans les véhicules doit être respectueuse de la protection des données, c'est-à-dire qu'elle doit prendre en compte les aspects liés à la cybersécurité et à la protection des données lors de l'étude des composants ("respect de la vie privée dès la conception") et qu'elle doit définir les paramètres de base de la configuration d'usine en conséquence ("respect de la vie privée par défaut").

4.3 Sûreté

4.3.1 Les normes relatives à la sûreté fonctionnelle des principaux composants ou systèmes électriques et électroniques équipant les véhicules, telles que l'ISO 26262, doivent être appliquées en tenant compte des exigences relatives à la sécurité des véhicules connectés et des véhicules à conduite automatisée.

4.3.2 La connexion et la communication à bord des véhicules connectés et des véhicules à conduite automatisée :

a) Ne doivent pas avoir d'incidences sur les dispositifs et les systèmes internes produisant les informations internes nécessaires à la commande du véhicule, sauf si des mesures appropriées ont été prises à cet effet ;

b) Doivent être conçues de manière à éviter la manipulation frauduleuse des logiciels des véhicules connectés et des véhicules à conduite automatisée ainsi que l'accès frauduleux aux informations de bord, résultant d'attaques informatiques effectuées par les moyens suivants :

i) Connexion sans fil ;

ii) Connexion câblée via le port de diagnostic, etc. ;

c) Doivent être assorties de mesures visant à garantir le passage en "mode sûr" en cas de dysfonctionnement, par exemple au moyen de la redondance.

4.3.3 Lorsque des véhicules connectés et des véhicules à conduite automatisée détectent une manipulation frauduleuse résultant d'une attaque informatique, leur système doit avertir le conducteur et, le cas échéant, prendre les commandes du véhicule pour en assurer la sécurité conformément aux prescriptions énoncées ci-dessus.

4.4 Sécurité

4.4.1 La protection des véhicules connectés et des véhicules à conduite automatisée exige des mesures de sécurité vérifiables et conformes aux normes de sécurité (par exemple la série de normes ISO 27000 ou la norme ISO/CEI 15408).

4.4.2 Les véhicules connectés et les véhicules à conduite automatisée doivent être protégés par les mesures suivantes :

a) Des mesures de protection de l'intégrité, par exemple lors des mises à jour de logiciels ;

b) Des mesures appropriées de gestion des clefs cryptographiques.

4.4.3 L'intégrité des communications internes entre les contrôleurs dans les véhicules connectés et les véhicules à conduite automatisée doit être protégée, par exemple au moyen de l'authentification.

4.4.4 Les services en ligne d'accès à distance aux véhicules connectés et aux véhicules à conduite automatisée doivent comporter une fonction fiable d'authentification mutuelle et garantir la sécurité des communications (protection de la confidentialité et de l'intégrité) entre les entités concernées. ».

II. Informations générales et proposition administrative

A. Informations générales

1. La présente directive porte sur les véhicules connectés et les véhicules à conduite automatisée.

2. La numérisation de la mobilité et l'augmentation du volume de données qui en résulte s'accompagnent de nouvelles exigences applicables à la sécurité des véhicules et aux infrastructures ainsi qu'à la protection des droits des personnes. Les véhicules connectés et les véhicules à conduite automatisée doivent donc être régis par des réglementations claires en matière de cybersécurité et de protection des données.

3. Les véhicules connectés et les véhicules à conduite automatisée doivent fonctionner de manière sûre et fiable au-delà des frontières nationales. Les droits relatifs aux données sur la mobilité des personnes doivent faire l'objet de réglementations claires.

4. L'objectif est de veiller à ce que les véhicules soient protégés contre les interférences et les manipulations extérieures. Les principes du droit international relatif à la confidentialité des données s'appliquent à la protection des données.

5. Les mesures nécessaires pour garantir la cybersécurité et la protection des données doivent faire l'objet de vérifications, par exemple de contrôles du système par des organisations extérieures.

B. Proposition administrative

6. La présente directive porte sur la construction des véhicules et fournit des informations sur les textes juridiques applicables à la conception des véhicules qui visent à l'amélioration de la sécurité et à la protection de l'environnement. Elle a les mêmes objectifs que la Résolution d'ensemble sur la construction des véhicules (R.E.3). Il est proposé d'en publier le texte (sect. I) dans une nouvelle annexe 6 à la R.E.3.