39va Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

Hong Kong, 25-29 septiembre 2017

Resolución sobre Protección de Datos en Vehículos Automatizados y Conectados

La 39° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad:

Reconociendo que los vehículos automatizados y conectados pueden ofrecer beneficios significativos a los usuarios al proporcionar mayores niveles de usabilidad o conveniencia, así como al público en general mejorando la eficiencia del tráfico y la seguridad de los conductores de vehículos y sus pasajeros, otros usuarios y peatones;

Destacando el rápido avance de los vehículos automatizados y de las tecnologías de los vehículos conectados que permite el desarrollo e introducción de nuevos e innovadores productos, dispositivos o servicios telemáticos, que, en muchos casos, incluye la recolección y el tratamiento de datos personales debido a la amplia variedad de sensores instalados en los mismos, por lo tanto, evocando nuevos desafíos a los derechos a la protección de datos personales y a la privacidad de los usuarios, especialmente cuando se trata de los múltiples escenarios en los que los vehículos pueden ser utilizados por muchas personas;

Observando la declaración de Ministros de Transporte y el Comisionado Europeo de Transporte del G7 en su reunión celebrada en Cagliari, Italia, el 21 y 22 de junio de 2017[1], la cual reconoce la necesidad de seguir las directrices existentes relevantes en materia de ciberseguridad y protección de datos, y alienta a todos los actores a evaluar cómo pueden utilizarse los datos necesarios para el desarrollo de servicios y aplicaciones que mejoren las condiciones de seguridad y tráfico y que a su vez respeten los intereses de ciberseguridad y privacidad de los consumidores;

Observando la Declaración de Ministros del G20 responsables de la Economía Digital en su reunión celebrada en Düsseldorf, Alemania, los días 6 y 7 de abril de 2017, sobre la Conformación de la Digitalización para un Mundo Interconectado[2], la cual reconoce la necesidad de fortalecer la confianza en la economía digital mediante el respeto de los marcos legales para la privacidad y la protección de los datos y el fortalecimiento de la seguridad en el uso de tecnologías de la información y la comunicación, así como la transparencia y la protección a los consumidores;

Preocupada por la posible falta de información disponible, opciones para el usuario, el control de datos y los mecanismos válidos de consentimiento para que los propietarios de los vehículos, conductores y sus pasajeros, así como otros usuarios de los caminos y

[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

carreteras y los peatones, controlen el acceso y el uso de los datos relativos al vehículo y a su conducción.

Observando el desarrollo de diferentes tecnologías para sistemas cooperativos de transporte inteligente donde los vehículos comparten sus datos posicionales y cinemáticos mediante la transmisión continua de información a otros vehículos (v2v), la infraestructura de transporte (v2i) u otras entidades que actúan como terceros(v2x) para obtener un panorama general de la situación actual del tráfico para poder fomentar la seguridad y la eficiencia del mismo;

Preocupada porque la difusión sin restricciones e indiscriminada de datos por parte de los vehículos en el contexto de la comunicación v2v, v2i y v2x podría dar lugar a un uso ilegítimo, acceso no autorizado a terceros o a un tratamiento posterior de los datos personales de los conductores, pasajeros o de otros individuos por parte de terceros;

Observando, por otra parte, que las tecnologías para los sistemas cooperativos de transporte inteligente deben diseñarse de manera que permita la rastreabilidad y la autenticación de los vehículos, considerando debidamente los principios de privacidad por diseño y privacidad por defecto;

Reconociendo que los desarrolladores de las diferentes tecnologías para los sistemas cooperativos de transporte inteligente están conscientes de los riesgos de privacidad que emergen de estas tecnologías y han realizado esfuerzos considerables para minimizar dichos riesgos reduciendo la cantidad de datos personales y dificultando la identificación de los titulares de los datos;

Observando que una recolección amplia de datos dentro de un sistema de vehículos conectados incluyendo el sistema cooperativo de transporte inteligente, podría no sólo llevar a la acumulación de perfiles de movimiento de individuos, sino también generar una gran cantidad de datos sobre la evaluación de conductas de manejo, que pueden resultar valiosas para ciertas entidades, como las compañías de seguros automotrices, los fabricantes de vehículos, los anunciantes, así como las autoridades encargadas de hacer cumplir la ley y vigilar el tránsito, particularmente cuando los datos van a ser personalizados, por ejemplo, al utilizar cualquier dato identificador transmitido por un vehículo;

Mencionando las mejores soluciones prácticas en la difusión televisiva de pago y la radio digital de la policía para restringir el acceso a la información transmitida a los destinatarios autorizados;

Observando que los comisionados de protección de datos y privacidad proporcionan orientación específica sobre las normas de privacidad aplicables al tratamiento o a soluciones relacionadas con los vehículos automatizados y conectados;

Observando que el Foro Mundial para la Armonización de la Reglamentación sobre Vehículos ha incluido las Directrices sobre Ciberseguridad y Protección de Datos en su resolución consolidada sobre la construcción de vehículos (R.E.3) [3] como anexo 6;

[3] https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r5e.pdf

Afirmando los requisitos establecidos en la parte I de la sección 4 de las Directrices sobre Ciberseguridad y Protección de datos previamente mencionadas, que incluyen la consideración de los conceptos de privacidad por diseño y privacidad por defecto;

Reafirmando la Resolución sobre Privacidad por Diseño[4] adoptada por la 32 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en 2010 en Jerusalén, la Resolución sobre Perfiles[5] adoptada por la 35ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 2013 en Varsovia, así como la Resolución sobre Big Data adoptada por la 36ª Conferencia Internacional de 2014 en Fort Balaclava (Mauricio) [6];

La 39va Conferencia Internacional de Autoridades de Protección de Datos y Privacidad hace un llamado a todas las partes involucradas, particularmente a:

- **organismos de normalización,**
- **autoridades públicas,**
- **fabricantes de vehículos y de accesorios,**
- **servicios de transporte personal y proveedores de renta de vehículos,**
- **proveedores de servicios basados en datos, tales como reconocimiento de voz, navegación, mantenimiento remoto o servicios telemáticos de seguros automotrices,**

a respetar plenamente el derecho de los usuarios a la protección de sus datos personales y su privacidad y a tomarlos suficientemente en cuenta durante cada etapa de la creación y el desarrollo de nuevos dispositivos o servicios.

Por lo tanto, se insta a las partes previamente mencionadas a:

1. Proporcionar a los titulares de los datos información exhaustiva sobre qué datos son recolectados y tratados en el uso de los vehículos conectados, con qué fines y por quiénes,
2. Utilizar medidas de anonimización para minimizar la cantidad de datos personales, o cuando esto no sea factible, utilizar la seudonimización.
3. Mantener los datos personales sólo el tiempo necesario en relación con el propósito legítimo para el que son tratados, para otros fines compatibles, o de conformidad con la ley o con el consentimiento, y suprimirlos después de este período,
4. Disponer de medios técnicos para borrar los datos personales cuando un vehículo sea vendido o devuelto a su propietario,

[4] https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf
[5] https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf
[6] https://icdppc.org/wp-content/uploads/2015/2/Resolution-Big-Data.pdf

5. Proporcionar controles de privacidad granulares y fáciles de usar para los usuarios de vehículos, que les permita, cuando sea apropiado, conceder o denegar el acceso a diferentes categorías de datos en los vehículos,

6. Proporcionar medios técnicos a los usuarios de los vehículos para restringir la recolección de datos,

7. Proporcionar dispositivos seguros de almacenamiento de datos que faciliten a los usuarios de los vehículos un control total sobre el acceso a los datos recolectados por éstos,

8. Proporcionar medidas técnicas para los componentes seguros de comunicación en línea que protejan contra los ciberataques e impidan el acceso no autorizado y la interceptación de datos personales.

9. Desarrollar e implementar tecnologías para sistemas cooperativos de transporte inteligente que:

    a. Impidan el acceso no autorizado y la interceptación de datos personales recolectados por vehículos (v2v), infraestructura de transporte (v2i) u otras entidades que actúan como terceros (v2x),

    b. Permitan a los usuarios de los vehículos inhibir el intercambio de datos posicionales y cinemáticos mientras siguen recibiendo advertencias de peligro en los caminos y carreteras,

    c. Proporcionen salvaguardas contra el seguimiento y rastreo ilícitos de los conductores,

    d. Garanticen que los mecanismos de seguridad de la comunicación v2v, v2i y v2x durante los procesos de autenticación no presenten riesgos adicionales para la privacidad y los datos personales, y

    e. Limiten la posibilidad el riesgo del seguimiento ilegítimo del vehículo y la identificación del conductor.

10. Respetar los principios de la privacidad por defecto y la privacidad por diseño, proporcionando medidas y procedimientos técnicos y organizativos para asegurar que se respete la privacidad del titular de los datos, al determinar los medios del tratamiento y cuando se traten los datos,

11. Desarrollar tecnologías y esquemas de preservación de la privacidad que favorezcan el tratamiento de los datos personales abordo,

12. Garantizar que los algoritmos de autoaprendizaje necesarios para los vehículos automatizados y conectados sean transparentes en su funcionalidad y estén sujetos a

una evaluación previa por un organismo independiente con el fin de reducir el riesgo de decisiones automatizadas discriminatorias,

13. Proporcionar a los usuarios de los vehículos modalidades de conducción amigables en materia de privacidad con configuraciones predeterminadas,

14. Llevar a cabo evaluaciones del impacto de la protección de datos para desarrollos o implementaciones de estas tecnologías que sean nuevos, innovadores o arriesgados,

15. Promover el respeto de la privacidad de los datos personales de los usuarios de vehículos mediante el tratamiento responsable de sus datos personales y tomando en consideración los posibles daños que podrían ser causados a los usuarios de los vehículos como resultado del tratamiento y uso, y

16. Entablar un diálogo con los comisionados de protección de datos y privacidad para desarrollar herramientas de cumplimiento que acompañen y proporcionen seguridad jurídica al tratamiento relacionado con los vehículos conectados.

La Comisión Federal de Comercio de Estados Unidos se abstiene de esta Resolución.