BOSCH

Seguridad y responsabilidad en la Internet de las cosas (IoT)

Paloma Llaneza González

Wolters Kluwer

BOSCH

Seguridad y responsabilidad en la Internet de las cosas (IoT)

Paloma Llaneza González

Wolters Kluwer

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 - Fax: 902 250 502
***e-mail*:** clientes@wolterskluwer.com
http://www.wolterskluwer.es

Primera edición: abril 2018

Depósito Legal: M-11009-2018
ISBN versión impresa: 978-84-9090-292-9
ISBN versión electrónica: 978-84-9090-293-6

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

5.1.1. Transporte inteligente

Dentro de las distintas definiciones que distintas entidades han dado al concepto de «transporte inteligente» nosotros optamos por la facilitada por ENISA[2] en su documento de buenas prácticas. Se considera transporte inteligente la aplicación de tecnologías de información y comunicación al transporte para mejorar los niveles de servicio y eficiencia. Por su parte, el transporte público inteligente (Intelligent Public Transport o IPT) es definido como la aplicación de las tecnologías de la información y la comunicación a las redes de transporte público para mejorar los niveles de servicio y eficiencia. Por último, serían sistemas de transporte inteligentes (Intelligent Transport Systems, o ITS) la aplicación de tecnologías de información y comunicación a la gestión en tiempo real de vehículos y redes que implican el movimiento de personas y mercancías.

La UE no cuenta con instrumentos específicos para ninguno de estos entornos, si bien existen una serie de directivas cuyas competencias más amplias son, en diferentes grados, aplicables a los IPT. Estas Directivas[3] y Reglamentos cubren la protección de datos personales, el tratamiento de datos personales en el sector de las comunicaciones electrónicas, la promoción de vehículos de transporte por carretera limpios y energéticamente eficientes, creando la interoperabilidad de los sistemas ferroviarios nacionales en toda la Comunidad Europea, y el despliegue de sistemas de transporte inteligentes en el ámbito del transporte por carretera.

En conjunto, estas Directivas demuestran que, si bien actualmente no existe una legislación de la UE que se centre específicamente en el funcionamiento de IPT a nivel de la UE, existen elementos de las operaciones de IPT que están sujetos a cierta regulación. A pesar de ello, cuando hablamos de ciberseguridad, los requisitos y/o directrices en la materia para IPT establecidos por estas Directivas tienen muy poco que decir más allá de una mención superficial de la seguridad general, la necesidad de proteger las comunicaciones a bordo (como en el caso de la Directiva 2010/40/ UE) o la necesidad de proteger los derechos de privacidad de los ciudadanos.

Por su parte, la ya mencionada Directiva NIS[4] impone un deber a los operadores de infraestructuras críticas (incluido el transporte) de gestionar los riesgos que plantean para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones, si bien ya existía desde hace tiempo normativa y agencias encargadas de la seguridad de las infraestructuras críticas. Esta norma está muy lejos de ser lo suficientemente específica como para aplicarse a los operadores de IPT, a los dispositivos IoT y a los sistemas ciberfísicos.

---

2. Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations. ENISA. Diciembre 2015.

3. Directiva 2009/33/EC (http://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1440673932348&uri=CELEX:32009L0033), Directiva 2008/57/EC (http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008L0057), y Directiva 2010/40/EU (http://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1440674103143&uri=CELEX:32010L0040).

4. DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Paralelamente a estas Directivas, hay una serie de documentos de política de la UE publicados con la finalidad de impulsar el desarrollo futuro de IPT desde finales de los 2000, centrados en el Transporte Inteligente y su integración dentro de las ciudades inteligentes[5]:

- Plan continúo para la normalización de las TIC: este plan proporciona una visión general plurianual de las necesidades de actividades preliminares o complementarias de normalización de las TIC para emprender actividades de apoyo de la UE.
- *Ciudades inteligentes and Communities – European Innovation Partnership*: son asociaciones en las áreas de energía, transporte e información y comunicación con el objetivo de catalizar el progreso en áreas donde el uso de energía, la movilidad y el transporte, y las TIC están íntimamente vinculadas.
- Plan de acción para el despliegue de sistemas de transporte inteligentes en Europa: este plan de acción tiene como objetivo acelerar y coordinar el despliegue de sistemas de transporte inteligentes (STI) en el transporte por carretera, incluidas las interfaces con otros modos de transporte.
- Hoja de ruta hacia un espacio único europeo de transporte «Hacia un sistema de transporte competitivo y eficiente»[6]. Este documento tiene como objetivo determinar cómo eliminar las barreras y los cuellos de botella para completar el mercado interno del transporte creando un mercado de transporte competitivo y sostenible dentro de la UE.

Centrándonos en la Estrategia (de ahora en adelante, la Estrategia) europea sobre los sistemas de transporte inteligentes cooperativos (STI cooperativos)[7] trata, principalmente, el desarrollo y los aspectos prácticos y legales del desarrollo de los sistemas de transporte cooperativos, incluidos los vehículos conectados o automáticos así como las infraestructuras de transporte. Conforme este documento, es de señalar que Los servicios de los STI cooperativos se basarán en normas comunes y se implantarán a partir de 2019. Se fundamentan en la comunicación entre vehículos y entre los vehículos y la infraestructura, y no pasan necesariamente por prescindir de la figura del conductor.

Es importante destacar que el desarrollo de los STI cooperativos constituye un primer paso hacia los vehículos automatizados sin el cual estos no serían viables a gran escala.

La Estrategia define una serie de servicios de los STI cooperativos que se pueden implantar inmediatamente (conocida como lista inicial de servicios de los STI coope-

---

5. Internet of Things - An action plan for Europe - COM(2009) 278 final. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF

6. Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system - COM(2011) 144 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:tr0054

7. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones – Estrategia europea sobre los sistemas de transporte inteligentes cooperativos, un hito hacia la movilidad cooperativa, conectada y automatizada. [COM(2016) 766 final] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016DC0766

rativos) y otros servicios que se implantarían en una segunda fase, ya que, probablemente, no todas las normas y especificaciones estén listas para la implantación a partir de 2019 (segunda lista de servicios de los STI cooperativos).

La lista de implantación temprana de los STI cooperativos más avanzados o «lista inicial de servicios de los STI cooperativos» (Day 1 C-ITS services list, en inglés) comprende los siguientes servicios:

- Notificaciones de ubicación peligrosa:
  - avisos de circulación lenta o congestionada y avisos sobre el tráfico;
  - avisos de obras en la carretera;
  - condiciones meteorológicas;
  - luz de frenado de emergencia;
  - vehículo de emergencia aproximándose;
  - otros peligros.
- Aplicaciones de señalización:
  - señalización en el vehículo;
  - límites de velocidad en el vehículo;
  - incumplimiento de la señalización / seguridad en los cruces;
  - solicitud de señalización prioritaria por parte de los vehículos designados;
  - señal luminosa verde para la velocidad óptima recomendada;
  - datos compartidos por el vehículo; y
  - amortiguador de movimientos sísmicos (forma parte de la categoría «advertencia de peligro local» del Instituto Europeo de Normas de Telecomunicación, ETSI).

La segunda lista de servicios de los STI cooperativos (Day 1.5 C-ITS services list, en inglés) comprende aquellos servicios en los que probablemente no todas las normas y especificaciones estén preparadas para la implantación a gran escala a partir de 2019, aunque en general se considera que están bastante avanzadas. Incluyen los siguientes:

- información sobre estaciones de repostaje y de recarga para los vehículos que utilicen combustibles alternativos;
- protección de los usuarios vulnerables de la vía pública;
- gestión e información de los aparcamientos en la vía pública;
- información sobre los aparcamientos que no se encuentran en la vía pública;
- información sobre aparcamientos disuasorios;
- navegación conectada y cooperativa para entrar y salir de las ciudades (primer y último kilómetro, aparcamiento, consejos sobre la ruta, semáforos coordinados); y
- información sobre el tráfico y enrutamiento inteligente.

Se han establecido diversas medidas específicas para aplicar la Estrategia, que comprenden los ocho ámbitos siguientes.

- Implantación a gran escala en 2019 de, como mínimo, los servicios iniciales mediante la actuación de los Estados miembros, las autoridades locales, los fabri-

cantes de vehículos, los operadores de las infraestructuras viales y la industria de los STI con ayuda financiera (Mecanismo «Conectar Europa», FEIE, Fondos EIE).

La segunda lista de servicios y el desarrollo adicional de los STI cooperativos aún no están listos; su desarrollo recibirá el apoyo de la Comisión a través del programa Horizonte 2020 y de los Fondos EIE, en su caso, y la lista de servicios se actualizará mediante un proceso continuado de la plataforma C-ITS.

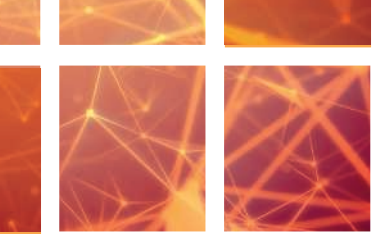
- Se procurará lograr una política de certificación y seguridad común a través de la cooperación entre la Comisión y todas las partes interesadas pertinentes.
  También constituirá la base para abordar un mejor nivel de servicio (entre vehículos y entre los vehículos y la infraestructura).
  La Comisión va a analizar las funciones y las responsabilidades de un modelo de confianza europeo de los STI cooperativos, así como la conveniencia de asumir una posible función de gobernanza.
- Los proveedores de servicios de los STI cooperativos han de ofrecer condiciones claras y comprensibles a los usuarios finales.

La Comisión publicará un primer conjunto de pautas sobre protección de la privacidad en 2018 y las iniciativas para implantar los STI cooperativos deben servir para informar y crear confianza entre los usuarios finales, demostrar el valor añadido del uso de datos personales y consultar a las autoridades responsables de la protección de datos de la UE para desarrollar un modelo de evaluación sobre la protección de datos.

- Medidas de la Comisión y de las partes interesadas para garantizar comunicaciones que funcionen en una banda de frecuencia facilitada por la Comisión.
- Utilización de la plataforma C-Roads para coordinar la aplicación de los STI cooperativos a nivel operativo, incluidas pruebas y validaciones.
- Desarrollo y publicación, mediante iniciativas de los STI cooperativos, de un proceso de evaluación del cumplimiento para los servicios iniciales.
  La Comisión, de conformidad con la Directiva relativa a los sistemas de transporte inteligentes, adoptará actos delegados sobre la continuidad y seguridad de los servicios de los STI cooperativos, sobre la aplicación práctica del Reglamento general de protección de datos en relación con los STI cooperativos, sobre un enfoque híbrido de comunicación y sobre la interoperabilidad en los procesos de evaluación del cumplimiento.
- La Comisión desarrollará la cooperación internacional en el ámbito de los STI cooperativos.

ENISA para asegurar el transporte público inteligente[8] establece las mejores prácticas para asegurar las redes TI entendidas como medidas de seguridad efectivas que deberían implantarse para abordar las debilidades identificadas por la propia ENISA quien presenta una panoplia de buenas prácticas en tres categorías según su naturaleza inherente, nin-

8. Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations. ENISA. Diciembre 2015.



A finales de marzo de 2018, una mujer que cruzaba empujando su bicicleta a oscuras una calle de Tempe, Arizona (EEUU), fue arrollada por un coche autónomo de Uber en pruebas. Tras el volante, tal como se aprecia en el vídeo publicado por la policía local, se observa que el conductor-controlador de seguridad no prestaba atención. Aunque era de noche, los sensores Lidar del vehículo deberían haber detectado a la ciclista, pero tampoco lo hicieron. Si hubiera sido un coche no autónomo y no conectado habríamos entendido que la responsabilidad recaía en mayor o menor medida en el conductor. Sin embargo, en el caso de Tempe, la cuestión de la atribución no es tan sencilla como no lo es, en general, en cualquier daño que las cosas conectadas o (o Internet of Things —IoT—) puedan ocasionar.

La alta complejidad del ecosistema IoT (objetos físicos, software, infraestructura de Internet, datos personales y no personales, comportamiento del usuario final, analítica de datos, etc.), y la variedad de actores implicados (fabricantes de productos, fabricantes de sensores, productores de software, proveedores de infraestructura, otros actores involucrados en el suministro de diferentes servicios, usuarios finales, etc.), hace que la labor de atribuir responsabilidades en caso de daño sea una tarea de enorme complejidad.

El lector encontrará en esta obra una guía para entender la tecnología, su complejidad e interacciones, el estado del arte de la legislación y de la ciberseguridad de la IoT, y las propuestas legislativas que están encima de la mesa sobre la seguridad de las cosas conectadas y la responsabilidad por los daños que causen.

ISBN: 978-84-9090-292-9
9 788490 902929 3652K28326

Wolters Kluwer