Boletín mexicano de derecho comparado
ISSN: 0041-8633
ISSN: 2448-4873
Instituto de Investigaciones Jurídicas, UNAM

García Segura, Luis A.; Cayón Peña, Juan
Retos jurídicos de los vehículos conectados en la era del internet de las cosas
Boletín mexicano de derecho comparado, vol. LII, núm. 154, 2019, Enero-Abril, pp. 457-488
Instituto de Investigaciones Jurídicas, UNAM

DOI: https://doi.org/10.22201/iij.24484873e.2019.154.14150

Disponible en: https://www.redalyc.org/articulo.oa?id=42771664015

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

RETOS JURÍDICOS DE LOS VEHÍCULOS CONECTADOS EN LA ERA DEL INTERNET DE LAS COSAS*

Luis A. García Segura**
Juan Cayón Peña***

I. Introducción

Según una reciente encuesta realizada por la consultora Accenture (2016), en la cual se contestaba a la pregunta de *¿cuál es su previsión sobre el cambio de ritmo de la tecnología en su industria durante los próximos tres años?*, los resultados fueron:

I. 58%: aumentará rápidamente.
II. 28%: aumentará a un ritmo sin precedentes.
III. 12%: aumentará lentamente.
IV. 1%: permanecerá estable.
V. 1%: disminuirá.

Las dos primeras respuestas reflejan el estado de expectación y alerta que tienen los directivos de las grandes empresas multinacionales, incluyendo por supuesto no sólo las gigantes tecnológicas, sino también a las pequeñas y medianas empresas. Este estado de expectación es compartido

* Artículo recibido el 19 de diciembre de 2016 y aceptado para su publicación el 31 de mayo de 2018.
** ORCID: 0000-0001-7074-4396. Profesor en la Universidad Antonio de Nebrija, España. Correo electrónico: *lgarcise@nebrija.es*.
*** ORCID: 0000-0001-7399-7778. Rector de la Universidad Antonio de Nebrija, España. Correo electrónico: *jcayon@nebrija.es*.

Boletín Mexicano de Derecho Comparado, nueva serie, año LI, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

igualmente por la mayoría de los investigadores jurídicos que nos hemos especializado en temas relacionados con las tecnologías de la información y comunicación (TIC), ciberseguridad y derecho informático.

Este ritmo vertiginoso de desarrollo despliegue y adopción de TIC hace que los legisladores pierdan el compás, legislen tarde y terminen aprobando normas que rápidamente quedan desfasadas y, a la vez, desprovistas de disposiciones que permitan una actualización más rápida y efectiva a futuro.

Según el Consejo Económico y Social de las Naciones Unidas (Unidas) y la Comisión de Ciencia y Tecnología para el Desarrollo del Consejo Económico y Social de las Naciones Unidas (Unidas, 2015b), existen cinco conceptos que están influyendo de manera considerable la forma en que los consumidores se desenvuelven en el ecosistema digital a nivel mundial:

1) La datificación: este término describe el proceso por el cual los datos se convierten en un recurso fundamental y en un factor determinante de los resultados de las actividades empresariales y gubernamentales. La información y el conocimiento se sitúan en el centro del gobierno y las empresas (Unidas, 2014: 8).
2) Los macrodatos o *Big Data*: este término describe la acumulación y el análisis de recursos de información considerablemente mayores, más allá de la capacidad analítica y de almacenamiento de los recursos de los equipos y programa informáticos (Unidas, 2014: 9).
3) La computación en la nube: ofrece importantes recursos para la datificación y el análisis de macrodatos. En este modelo, no únicamente los datos de los usuarios sino también las aplicaciones se almacenan en centros de datos gestionados por empresas de TIC en lugar de o a la vez que en los propios dispositivos de los usuarios y se accede a ellos en línea como y cuando se requiera (Unidas, 2014: 11).
4) El Internet de la Cosas o Internet of Things (IoT): amplía el alcance de la conectividad más allá de las personas y las organizaciones para incluir objetos y dispositivos (Unidas, 2014: 14).
5) Los sistemas inteligentes: son procesos posibilitados por las TIC que facilitan la producción, distribución y consumo de bienes y

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

servicios de una forma más eficiente. Abarca las siguientes aplicaciones (Unidas, 2014: 14):

a) Motores inteligentes: automatización y control durante la fabricación.
b) Logística inteligente: gestión del transporte y del almacenamiento.
c) Edificios inteligentes: diseño, gestión y automatización de edificios.
d) Redes inteligentes: gestión de la generación y distribución de electricidad.

En la presente contribución vamos a enfocarnos en el IoT y la relación que guarda con los *smart cars*/coches inteligentes/vehículos conectados, para luego analizar los principales retos de seguridad y privacidad que afrontan dichas industrias, para concluir con una serie de reflexiones y recomendaciones de cara a dar pistas a los legisladores para afrontar los retos jurídicos identificados.

II. El Internet de las cosas

1. *En qué consiste*

Según Vermesan (2013), el IoT es una nueva revolución de Internet en la cual los objetos electrónicos se identifican en la red y toman decisiones en respuesta a su contexto relacional, basadas en la inteligencia obtenida mediante el intercambio de información con la red y con los demás objetos conectados a la misma.

Una segunda definición la aporta la Fundación de la Innovación Bankinter (Bankinter, 2011), que dice que el IoT consiste en que los objetos o productos cotidianos que utilizamos en determinadas ocasiones tengan conexión a Internet en cualquier momento y lugar, mediante la integración de sensores y dispositivos que quedan conectados a Internet a través de redes fijas e inalámbricas.

Una tercera definición la encontramos en la Unión Internacional de Telecomunicaciones (Telecomunicaciones) que afirma lo siguiente:

> Infraestructura mundial al servicio de la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión (física y

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

virtual) de las cosas gracias al interfuncionamiento de tecnologías de la información y la comunicación (existentes y en evolución) (Telecomunicaciones, 2012: 2).

Es decir, estamos hablando de la conectividad de los aparatos electrónicos de uso cotidiano tanto en el hogar como en la empresa, y que se les ha incorporado al *hardware* interno una conexión a Internet, la cual permite la transmisión de datos, entre otras funciones. Por aparatos electrónicos nos referimos a un televisor, refrigerador, impresora, lavadora, etcétera, pero también a los vehículos de motor, que no dejan hoy en día de ser aparatos electrónicos con sistemas informáticos integrados, como veremos más adelante.

Según algunos cálculos, el impacto proyectado que tiene la IoT queda reflejado en las siguientes cifras (Deloitte, 2016):

- Aproximadamente 44 trillones de GB de información se emitirán a través de estos dispositivos.
- 4.4 billones de personas estarán conectadas a través de IoT en los próximos años.
- El valor del mercado total de IoT alcanzará 4.3 trillones de dólares estadounidenses para 2024.

A estos efectos, la propia Unión Internacional de Telecomunicaciones ha creado una Comisión de Estudio para el "Internet de las cosas y sus aplicaciones, incluidas las ciudades inteligentes",[1] la cual trabaja para elaborar normas internacionales que faciliten el desarrollo coordinado de

[1] La decisión de crear la CE20 fue tomada por el Grupo Asesor de Normalización de las Telecomunicaciones (GANT) en su reunión celebrada en la Sede de la UIT en Ginebra del 2 al 5 de junio de 2015, en ejercicio de la autoridad conferida al GANT para modificar la estructura y el programa de trabajo del UIT-T (Comisiones del Estudio del Sector de Normalización de las Telecomunicaciones) durante los cuatro años que transcurren entre dos asambleas mundiales de normalización de las telecomunicaciones. Cabe aclarar que la finalidad última del GANT es conseguir que el UIT-T se convierta en el foro más interesante para llevar a cabo la normalización. Para esto, el GANT asesora las comisiones estudio, los miembros y el personal del UIT-T teniendo en cuenta las necesidades de todos los miembros, tanto de los países en desarrollo como de los desarrollados, de la industria y de los gobiernos. El portal de la Comisión de Estudio en cuestión es: *http://www.itu.int/es/ITU-T/about/groups/Pages/sg20.aspx*.

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

tecnologías IoT, incluidas las comunicaciones de máquina a máquina y redes de sensores ubicuos.

2. *Beneficios*

Se espera que el despliegue de tecnologías IoT permita conectar unos 50,000 millones de dispositivos a la red antes de 2020, lo que tendrá consecuencias inevitables en casi todos los aspectos de nuestra vida cotidiana (Telecomunicaciones, 2016). Serán los consumidores los encargados, en primera instancia, de evaluar los aspectos negativos y positivos de la adopción del IoT en sus vidas, si bien "prima facie" las ventajas propuestas por los profetas de la conectividad total son espectaculares.

Con criterio más empresarial, para la consultora PWC (2015: 6), los principales beneficios que aportan el IoT pueden clasificarse en tres grandes categorías:

- Mayor accesibilidad: por ejemplo, a través de redes móviles se puede asegurar la prestación de servicios en lugares muy remotos.[2]
- Mayor eficiencia: las empresas aprovechan datos internos, visibilidad y control de maquinaria, personal y equipos.[3]

[2] La empresa Honeywell, famosa por los termostatos para manejar las calderas en el hogar, está aprovechando las tecnologías de acceso remoto de IoT para mejorar sus productos industriales. Por ejemplo, su producto Orion Console integra una serie de sensores y plataformas del IoT que permiten monitorizar el estado de una planta o fábrica remotamente, sin tener que estar físicamente delante de la pantalla en la localidad de la empresa. Para más información: *https://www.good-design.com/entry/honeywell-experion-orion-console/* y *http://www.fastcompany.com/3052936/the-future-of-work/how-the-internet-of-things-is-changing-work*.

[3] Un ejemplo de las posibilidades que ofrece el IoT en términos de mayor eficiencia lo tenemos con los servicios y productos que ofrece la empresa AggreGate. Su producto estrella es una plataforma digital que integra servicios de monitorización remota y gestión inteligente de dispositivos a través de tecnología M2M (Machine-to-Machine). Según la propia empresa, un ejemplo aplicado a la industria de la agricultura lo tenemos con la posibilidad de poder monitorizar remotamente maquinaria y vehículos agropecuarios. Para más información: *http://aggregate.tibbo.com/industries.html* y *http://www.theinternetofthings.eu/victor-polyakov-what's-inside-internet-or-things-tibbo-aggregate-iot-platform-concept*.

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

- Personalización: mediante el análisis de los datos aportados por los clientes, las empresas podrán comprenderlos mejor y transformar la experiencia del servicio prestado.[4]

Estas tres categorías de beneficios son aplicables tanto a los consumidores como a las empresas detrás de los productos y los servicios. Del lado de los consumidores, una de las ventajas principales que ofrece IoT es que puede resultar en una tarificación más transparente de los servicios que consumen. El hecho de tener sensores en nuestros aparatos o aplicaciones que registran constantemente las actividades, puede llevar a tomar decisiones con base en dichos resultados, como controlar el gasto en agua o en la luz, según vimos (Bankinter, 2011).

En el caso de las pymes, el IoT en general puede ayudar a reducir los costos operacionales, ampliar la cuota de mercado, aumentar la sostenibilidad y la rentabilidad de las mismas. A estos efectos, dichas pymes pueden llegar a competir en lugares de bajos ingresos, cuando de otra manera podrían ser expulsadas del mercado por las grandes empresas (Unidas, 2015).

Si las empresas en cuestión además comercializan productos relacionados con servicios básicos, estaríamos ante un posible caso de aumento del nivel o calidad de vida, según lo afirmado por el Consejo Económico y Social de las Naciones Unidas:

> Los partidarios de la Internet de las cosas prevén que dará lugar a un gran número de aplicaciones y servicios innovadores, que mejorarán la calidad de vida y reducirán las desigualdades, al tiempo que ofrecen nuevas oportunidades de ingresos para muchas empresas emprendedoras, por ejemplo en los ámbitos del diagnóstico y tratamiento médicos, el abastecimiento de agua más limpia, la mejora del saneamiento, la producción de energía, la exportación de productos básicos y la seguridad alimentaria (Unidas, 2014: 13).

[4] La empresa PhotonStar LED Group plc, mediante tecnología proporcionada por IBM, ha desarrollado un producto llamado PhotonStar Halcyon, integrado por luces LED, sensores y un sistema de gestión. Las luces proporcionan una iluminación optimizada según la hora del día y la actividad que el usuario esté realizando en ese momento. De esta forma, según la empresa, se proporciona un servicio más completo, ya que repercute directamente en la salud, productividad y bienestar del usuario. Para más información véase *http://www.ibm.com/internet-of-things/images/CaseStudy_PhotonStar_halcyon_Dec2015_FinalNew.pdf y http://www.halcyon-lighting.co.uk.*

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

En un estudio reciente realizado a directivos españoles (Zamora y Vergara, 2015), los principales beneficios del IoT que ellos percibían eran: mejora de la experiencia del cliente (72%), reducción de gastos operativos (70%) y la optimización del uso de los activos (66%).

Otra de las aplicaciones destacadas, que repercuten directamente en los consumidores y también en el tejido empresarial, es la aplicación efectiva del IoT en las *smart cities*, mediante la integración de dispositivos inteligentes conectados y servicios con base en la nube, los cuales pueden ayudar a combatir la congestión de tráfico, la gestión de residuos, la eficiencia energética y la seguridad ciudadana (PWC, 2015).

Sigamos el hilo de la primera conexión y mención expresa de la relación del IoT y transporte. Sobre esta relación, Jeremy Rifkin afirmó lo siguiente:

> La convergencia de la comunicación vía Internet, la energía vía Internet y el transporte y la logística vía Internet en un solo núcleo constituye el cerebro global de la estructura cognitiva del Internet de las cosas. Esta nueva plataforma digital cambia fundamentalmente el modo en el que gestionamos la actividad económica a lo largo de las numerosas cadenas y redes de valor que constituyen la economía global. La plataforma digitalizada del Internet de las cosas es el núcleo de la Tercera Revolución Industrial (Rifkin, 2015: 1).

Compartimos totalmente el reconocimiento que hace Rifkin al potencial transformador del IoT en la gestión del transporte durante las próximas décadas. Pero nuestro entusiasmo viene acompañado de mucha cautela, especialmente frente a los riesgos potenciales —y ya probados— que trae consigo la ola de IoT.

3. *Retos de seguridad y privacidad*

Según lo expuesto hasta ahora, se puede afirmar que la industria basada en los servicios y productos digitales hará que las empresas detrás de los mismos afronten riesgos a los que los negocios tradicionales nunca se han visto expuestos, como los nuevos parámetros de seguridad, la responsabilidad respecto a la privacidad del consumidor, la exigencia de un uso transparente de los datos y cuestiones relativas a la utilización ética de las nuevas tecnologías (Accenture, 2016).

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

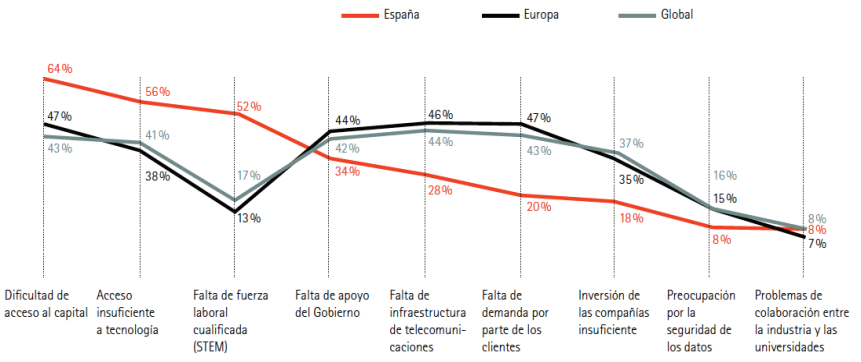
DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

Según un estudio publicado por el Centro de Seguridad TIC de la Comunidad Valenciana (2014: 10), los riesgos asociados a la evolución del IoT varían en función de la criticidad del dispositivo u objeto, ya sea por la función que realizan o por la dependencia que se tenga del mismo. Así, las amenazas a las que están expuestos dichos objetos pueden afectar:

- Accesibilidad del objeto.
- Integridad de la información que contiene.
- Identidad del usuario, la cual puede ser suplantada.

Estas tres categorías de amenazas son perfectamente aplicables a todos los objetos y dispositivos dentro del IoT, incluyendo los vehículos. No obstante, como podemos observar en el siguiente gráfico, la percepción a nivel global entre los empresarios es que la seguridad de los datos es uno de los obstáculos menos importantes a la hora de desarrollar productos dentro de la ola del IoT:

Figura 1. ¿Cuáles son los principales obstáculos para el desarrollo del Internet de las cosas?



Fuente: Zamora y Vergara (2015: 13).

A nuestro entender, los resultados de este estudio muestran que los empresarios no tienen una comprensión adecuada del paradigma del IoT, y mucho menos sobre retos de seguridad y privacidad asociados a los mis-

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

mos. Las siguientes palabras de Hathaway *et al.* (2015: 5) en el estudio titulado "Índice de preparación cibernética 2.0" corroboran la preponderancia que sin embargo ostenta a ciertos niveles gubernamentales y académicos los retos de seguridad y privacidad aludidos, englobados dentro de la ciberseguridad:

> …la inseguridad cibernética es un impuesto al crecimiento… El volumen, alcance, velocidad y sofisticación de las amenazas a nuestros sistemas e infraestructuras en red son reales y están creciendo. Las violaciones de datos, actividad delictiva, interrupciones de servicio y la destrucción de la propiedad se están convirtiendo en algo común y amenazan la economía de Internet. Los líderes mundiales entienden que el aumento de la conectividad a Internet conduce al crecimiento económico sólo si la infraestructura subyacente y los dispositivos conectados a ella están a salvo y seguros. Por lo tanto, los países deben alinear sus visiones económicas con sus prioridades de seguridad nacional (Hathaway *et al.*, 2015).

Como afirma la cita, la alineación de las políticas públicas relativas a la economía debe hacerse siempre tomando en cuenta las prioridades de seguridad nacional.[5] Aplicando este argumento al desarrollo de IoT, Friess (2013) concluyó que los principales retos sociales y de políticas relacionados con este fenómeno son:

1) Promoción de un universo del IoT consistente, interoperable y accesible de forma transversal a través de diferentes industrias, incluyendo las prácticas de estandarización.
2) Dirigir el esfuerzo y los recursos hacia las aplicaciones sociales de mayor trascendencia, como la salud y el medio ambiente.

[5] En un artículo publicado en 2015, afirmamos lo siguiente sobre la importancia de la ciberseguridad en términos económicos para una nación: "Ya en el año 2011 el Congreso de EUA reconocía la gravedad de los incidentes de ciberseguridad en las empresas privadas, específicamente las del sector financiero, al punto de que afirmaban categóricamente que el fraude financiero y el robo de identidad digital ponían en peligro la seguridad económica nacional" (Cayón y García 2015). Partiendo de la experiencia de EUA, España aprobó en 2013 su Estrategia de Ciberseguridad Nacional, cuyo objetivo general número dos contemplaba el fortalecimiento de las capacidades de prevención, defensa, detección y respuesta a los ciberataques contra las empresas y las infraestructuras críticas españolas. Para más información: *http://www.dsn.gob.es/es/sistema-seguridad-nacional/qué-es-seguridad-nacional/ámbitos-seguridad-nacional/ciberseguridad*.

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

3) Ofrecer orientación sobre seguridad, privacidad, confianza y ética de la industria con base en la legislación actual y el desarrollo futuro de la misma en torno a la normativa de protección de datos de carácter personal.
4) Proporcionar recursos para un servicio pan-europeo que elimine las barreras de servicios como el roaming.
5) Convertir el IoT en un eje de cooperación internacional.

De estas cinco categorías de retos, la industria del transporte y a su vez los vehículos conectados se ven particularmente afectados por las amenazas englobadas en la segunda y tercera categoría, como veremos más adelante.

Con relación a la privacidad y el anonimato, el Foro Económico Mundial (Foro, 2016b) publicó datos de una encuesta afirmando que estos temas eran muy importantes para el 69% de los usuarios de Internet. La misma encuesta revela que el 75% de los usuarios cree que es importante tener control y decisión total de qué datos personales son almacenados y utilizados por las marcas, productos y servicios dentro de las redes sociales.

Dentro de este panorama, las redes sociales se han convertido en entidades comerciales diseñadas para que millones de personas puedan intercambiar simultáneamente todo tipo de información, especialmente videos e imágenes. Sin embargo, este contenido es monitorizado, analizado y clasificado por los gobiernos, y diversas empresas asociadas del ecosistema digital,[6] con el fin de encontrar las publicaciones más relevantes y re-pu-

[6] El Consejo Económico y Social de las Naciones Unidas define el ecosistema digital como: "…el espacio formado por la convergencia de las industrias de los medios de comunicación, las telecomunicaciones y las tecnologías de la información. Tal ecosistema está integrado por componentes como la infraestructura tecnológica, la infraestructura de datos, la infraestructura financiera, la infraestructura institucional y la infraestructura humana. El ecosistema digital proporciona las aportaciones necesarias para crear las bases técnicas, y las aplicaciones sociales y técnicas, necesarias para el desarrollo digital" (Unidas, 2015a: 13). De forma similar, Katz afirma lo siguiente: "…el ecosistema digital es uno de los conceptos utilizados para comprender el conjunto de fenómenos industriales y de impacto económico asociados con el despliegue y adopción de las Tecnologías de la Información y la Comunicación, y más específicamente con Internet. Estos cambios conllevan una transformación en cómo firmas participantes en la producción de bienes y servicios digitales se interrelacionan para ofrecer una proposición de valor al mercado…. estos cambios implican no sólo una modificación de firmas que preexistían al ecosistema (por ejemplo, medios de comunicación y operadores de telecomunicaciones), sino también

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

blicarlas en otros canales digitales. De esta forma, los usuarios de las redes sociales publican contenidos inicialmente dirigidos a su entorno de amigos o familiares, pero la mayoría no toma en cuenta que dichos contenidos pueden llegar a millones de personas ajenas a este entorno (Foro, 2016a).

La propia popularidad de las redes sociales en la actualidad revela el paradigma contradictorio sobre el control y supervisión efectiva de los datos, imágenes y videos propiedad de los usuarios de las redes. A gran parte de los usuarios/consumidores les preocupa el tema, pero muchos renuncian a una tutela más consciente con el fin de acceder a los servicios de la red social en cuestión.

No obstante, según el propio Foro Económico Mundial (2016a), solamente a través de la integración en los canales de redes sociales, podrá el IoT convertirse en un medio verdaderamente transformativo de la vida cotidiana, dado el hecho de que la comunicación entre los individuos se efectúa cada vez más a través de dichas comunidades digitales.

Por todo ello, Saif *et al*. (2015) concluyen que se deben tomar las siguientes medidas para salvaguardar el ecosistema del IoT:

- Definir estándares de interoperabilidad: es necesario —dicen— desarrollar una serie de estándares entre todos los consorcios envueltos, de forma que los dispositivos conectados a la red puedan comunicarse y coordinarse de una forma más segura y efectiva.
- Establecer responsabilidades claras para los actores de cada industria.
- Establecer el buen gobierno de la información o datos: los actores deben tener claro qué datos son críticos y por lo tanto necesitan un mayor nivel de protección respecto a los demás.

Sin embargo, ya para finales del siglo pasado la Directiva europea 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Parlamento, 1995) entendía por dato de carácter personal toda información sobre una persona física identificada o identificable, por lo que cualquier tratamiento de los mismos requiere el consentimiento del afectado. Indudablemente, la actual legislación europea y su aplicabilidad

la aparición de nuevas empresas que despliegan funciones productivas de intermediación" (Katz, 2015: 5).

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

a un mundo totalmente interconectado, plantea retos jurídicos de difícil solución práctica.[7]

En el caso de los vehículos conectados, vamos a ver cómo los actores principales de la industria, los fabricantes de coches han dado pasos hacia el establecimiento de un mejor gobierno de los datos de sus usuarios. Sentadas las bases más generales respecto del IoT y sus retos, demos paso entonces a la segunda parte de nuestro artículo dedicada al conocimiento de los vehículos conectados.

III. Vehículos conectados a la red

1. *En qué consisten*

Un coche promedio hoy día tiene 70 sistemas informáticos incorporados, los cuales contienen aproximadamente 100 millones de líneas de programación, el doble que el sistema operativo de Windows Vista (Saif *et al.*, 2015). Bajo esta premisa, no cabe duda de que un coche moderno, además de coche, es a la vez un dispositivo digital con bastante capacidad de computación, lo cual conlleva que se preste a casi todas las aplicaciones y utilidades que un ordenador convencional —una táblet o un móvil— pueda realizar.[8]

[7] A principios de abril de 2016 se aprobó definitivamente el Reglamento Europeo de Protección de Datos, el cual se comenzará a aplicar a mediados de 2018. La nota de prensa emitida luego de la aprobación afirmaba lo siguiente: "La reforma pretende devolver a los ciudadanos el control de sus datos personales y garantizar en toda la UE unos estándares de protección elevados y adaptados al entorno digital… Entre otras disposiciones, las nuevas reglas incluyen: el derecho al "olvido", mediante la rectificación o supresión de datos personales; la necesidad de "consentimiento claro y afirmativo" de la persona concernida al tratamiento de sus datos personales; la "portabilidad" o el derecho a trasladar los datos a otro proveedor de servicios; el derecho a ser informado si los datos personales han sido pirateados; lenguaje claro y comprensible sobre las cláusulas de privacidad, y multas de hasta el 4% de la facturación global de las empresas en caso de infracción" (Parlamento, 2016: 1). El texto completo del Reglamento se encuentra disponible en: *http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/es/pdf*.

[8] En una entrevista en 2015, Danny Shapiro, director de Automotive Operations, fabricante de productos informáticos Nvidia, afirmó que el coche del futuro tendrá a bordo el ordenador más poderoso que jamás hayamos tenido: *Today, there are 8m cars on the road with Nvidia's processors inside – including models from Telsa, Volkswagen, Honda and Mercedes as well as Audi – but Danny Shapiro, senior director of automotive at Nvidia, claims the company is just getting*

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

Un vehículo conectado a la red es aquel que dispone de un mecanismo para conectar a Internet sus unidades de control de motor (Electronic Control Unit o ECU) junto con sus sistemas de navegación y entretenimiento (Zurich, 2014).

Según Lawson *et al.* (2015), los mecanismos para conectar un coche a Internet se pueden agrupar en tres renglones:

1) De fábrica: el vehículo viene con una tarjeta SIM y un módem integrado que le sirve para conectarse a la red. Ejemplo: sistema OnStar de General Motors.[9]
2) Integrados: la conexión a la red proviene del dispositivo móvil del conductor, el cual se conecta mediante un puerto electrónico dentro del vehículo. Ejemplo: sistema Entune de Toyota.[10]
3) Híbridos: la conexión a Internet puede hacerse mediante una combinación de los dispositivos mencionados anteriormente: tarjeta SIM, módem o dispositivo móvil. Ejemplo: sistema SYNC de Ford.[11]

---

started. "We have contracts with a lot of automakers, so over the next several years we're going to grow that number by over 25m," he said. "Younger first-time car buyers have grown up with iPhones and iPads, so the expectation is that if you're going to spend this much money on a car, the electronics in the car should be at least as good as your tablet". Para más información: *http://www.telegraph.co.uk/technology/news/11609406/The-car-of-the-future-is-the-most-powerful-computer-you-will-ever-own.html, http://www.businessinsider.com/us-processor-company-the-car-of-the-future-is-the-most-powerful-computer-you-will-ever-own-2015-5* y *http://recode.net/2016/01/14/the-hottest-computing-device-cars/.*

[9] A través de asesores altamente capacitados, OnStar le ofrece apoyo personalizado a los conductores ante casi cualquier situación que puedan encontrar mientras conducen, incluyendo: servicios de emergencia, asistencia en el camino, navegación paso a paso y diagnósticos del vehículo. Sobre estos diagnósticos, el sistema envía un correo electrónico al propietario cada mes, el cual contiene un informe sobre los indicadores más importantes del vehículo. También permite obtener un diagnóstico en tiempo real mientras se va conduciendo, simplemente oprimiendo un botón que llama por teléfono a un asesor de OnStar, el cual puede tener acceso a la información transmitida por los ECU en dicho momento. Para más información: *https://www.onstar.com.mx/inicio.html.*

[10] Mediante una aplicación que se descarga al dispositivo móvil, el conductor puede disfrutar a través de los mandos y la pantalla del vehículo, una serie de servicios que incluye: llamadas, streaming de música, navegación, etcétera. Para más información: *http://www.toyota.com/entune/.*

[11] Este sistema permite hacer llamadas, reproducir música sin usar las manos, leer mensajes SMS entrantes y asistencia en casos de emergencia. La asistencia de emergencia

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

Parte de la información transmitida por estos mecanismos de conexión proviene de los ECU, que no son más que las unidades de control electrónico que regulan el funcionamiento del motor. Vienen a ser el corazón de todo el sistema electrónico del vehículo, que a su vez está compuesto por sensores y actuadores, los cuales registran diversos parámetros de funcionamiento, como las revoluciones del motor, temperatura de los sistemas, señal de la posición del acelerador, etcétera (Panadero, 2012).

Parte de esta información puede ser transmitida luego de forma automática al fabricante del vehículo o una empresa de servicio técnico, según hemos podido ver en algunos de los ejemplos de sistemas de navegación y entretenimiento. Se calcula que un vehículo hoy día puede llegar a tener hasta 70 ECU (Lawson *et al.*, 2015).

2. *Relación con IoT*

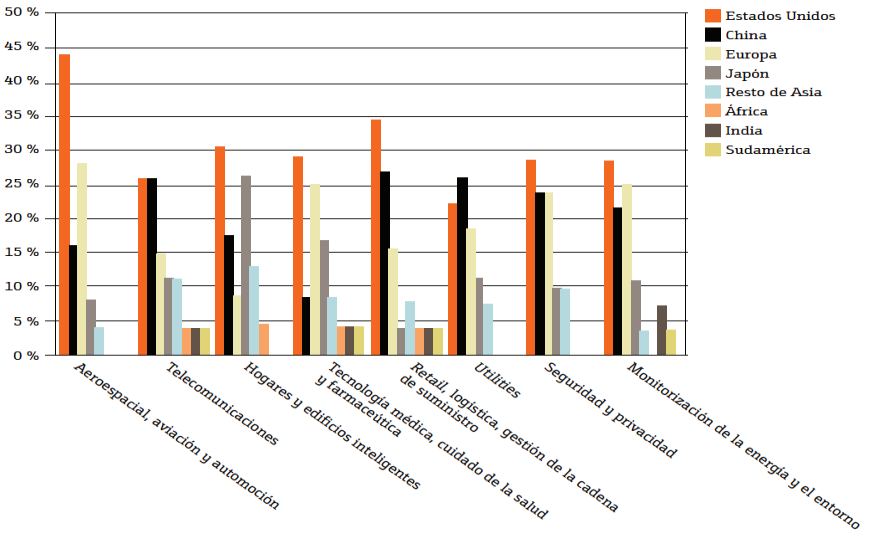
Como consecuencia del impacto ocasionado por la convergencia del IoT, se espera que todos los sectores industriales generen nuevas oportunidades de crecimiento y diferenciación para las marcas, creando a la vez una tendencia opuesta al actual enfoque dominante de servicios genéricos y estáticos diseñados para el consumo masivo, favorecer servicios inteligentes capaces de adaptarse y transformarse según las preferencias del consumidor (Fjord y Accenture, 2015).

Tratándose el sector automotriz de un segmento económico de consumo masivo, ya desde 2011 teníamos evidencia de que el mismo sería impactado de forma importante por la convergencia de IoT, según podemos ver en la siguiente figura 2.

se activa cuando se despliega la bolsa de aire o se corta la bomba de combustible, marcando al teléfono preconfigurado de emergencias. Para más información: *http://www.ford.es/AcercadeFord/Tecnologia/fordsync*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

Figura 2. Velocidad de adopción del Internet de las cosas en las distintas industrias.



Fuente: Fundación de la Innovación Bankinter (2011: 65)

Según los datos mostrados en la figura 2, las industrias aeroespacial, aviación y automoción son de las que más rápido adoptarían el IoT en EUA y Europa. A estos efectos, las previsiones de la consultora Groupe Speciale Mobile Association (2013) afirmaron que el mercado del vehículo generará para 2018, 39 mil millones de euros frente los 13 mil millones de euros generados en 2012. Recientemente, el Foro Económico Mundial y Accenture (Foro y Accenture, 2016) calcularon que el valor aproximado de todos los proyectos relacionados con las TIC en la industria automotriz mundial será de 700 millones de dólares para los próximos 10 años, lo cual supone una previsión más conservadora.

Aun así, cabe señalar que este mercado no solamente se circunscribe a los vehículos de transporte tanto públicos (autobuses) como privados (coches, motos, etcétera), sino que abarca los "sistemas de transporte inteligentes", que según la Unión Internacional de Comunicaciones (Telecomunicaciones, 2011) comprenden ocho categorías de sistemas avanzados:

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

1) Control de vehículos: complementan gran parte del trabajo del conductor. Ejemplo: prevención de colisiones y mejora de visión.
2) Gestión de tráfico: mejoran el flujo de tráfico y logran una utilización más eficaz de los sistemas en carretera. Ejemplo: gestión de la demanda de viajes y de los espacios de estacionamiento.
3) Información al viajero: asisten a los viajeros en la programación del viaje y durante su transcurso, así como con respecto a las condiciones de tráfico. Ejemplo: información de ruta al conductor y orientación de itinerarios.
4) Transporte público: mejoran la eficiencia del mismo mediante la indicación de horarios en tiempo real y el suministro de informaciones al pasajero. Ejemplo: transportes públicos personalizados que ofrecen rutas flexibles para un mejor servicio al cliente.
5) Gestión de la flota: mejoran la eficacia y productividad de las operaciones comerciales con los vehículos. Ejemplo: automatización de las inspecciones de seguridad de tránsito.
6) Gestión de situaciones de emergencia: logran la intervención más rápida de todos los vehículos de socorro en caso de accidentes de tráfico o de otro tipo. Ejemplo: gestión de vehículos de socorro.
7) Pagos electrónicos: permiten a los viajeros abonar los servicios de transporte por medios electrónicos basados en comunicaciones de corto alcance entre vehículos e infraestructura.
8) Apoyo a peatones: prestan servicios a los peatones en cuestiones de tráfico, como el cruce de calles.

Según PWC (2015), el IoT ha ayudado introducir al sector automovilístico los siguientes servicios:

- Mejora de logística y seguridad de los vehículos.
- Reducción de tiempos de viaje.
- Reducción de costes de mantenimiento y titularidad.
- Prestación de servicios de info-entretenimiento.

De forma similar, Saif *et al.* (2015) destacan que las principales aplicaciones del IoT en los coches conectados comprende los siguientes servicios:

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

- Sistemas de info-entretenimiento.
- Acceso remoto a:
  - Los seguros de las puertas del coche.
  - El encendido del motor.
  - La apertura de puertas de garaje.
  - El encendido de las luces del hogar.

Los llamados sistemas de info-entretenimiento agrupan una serie de aplicaciones, programas y dispositivos que de alguna manera mejoran o hacen más placentera la experiencia de conducir y/o ser pasajero en un coche. Las principales aplicaciones comprenden servicios de música, navegación, vídeo, asistencia de aparcamiento, acceso al teléfono móvil, acceso a Internet y acceso a información detallada del estado y desempeño del vehículo (gasolina, aceite, presión de las ruedas, etcétera).[12] La última ola de innovación en este segmento son las aplicaciones desarrolladas por Android[13] y Apple,[14] las cuales buscan integrar la interfaz del teléfono móvil junto con el centro de info-entretenimiento del coche, siguiendo los ejemplos vistos anteriormente.

El hecho de que estos dos gigantes tecnológicos estén apostando por la integración de sus móviles a los sistemas digitales de nuestros coches,

[12] La organización estadounidense Consumer Reports publica cada año una guía detallada donde prueban y evalúan los sistemas de info-entretenimiento de los principales fabricantes de vehículos del mercado de Estados Unidos. Para la edición del 2015, la guía concluyó que los fabricantes cuyos sistemas tenían más fallos fueron: Cadillac, Chrysler e Infiniti. Para más información: *http://www.consumerreports.org/cro/magazine/2015/04/infotainment-systems/index.htm*, así como, otras guías similares: *http://www.pcmag.com/category2/0,2806,2426316,00.asp*, *http://www.digitaltrends.com/infotainment-system-reviews/* y *http://www.tomshardware.com/t/automotive/*.

[13] Android Auto es el servicio que ofrece esta marca, el cual busca integrar al coche una serie de funciones y aplicaciones para los usuarios del sistema operativo Android. Los vehículos y los equipos compatibles con Android Auto están disponibles actualmente en los siguientes países: Alemania, Australia, Canadá, España, Estados Unidos, Francia, Irlanda, Italia, México, Nueva Zelanda y Reino Unido. Para más información: *https://www.android.com/intl/es_es/auto/*.

[14] Apple CarPlay es el producto de esta marca que busca integrar las funciones y aplicaciones de sus productos a los coches. Según el propio portal, "CarPlay está pensado para ser tu mejor copiloto. No sólo hablar con Siri y pedir lo que quieras, también puedes usar los mandos del coche (diales, botones y pantalla táctil)… sin apartar las manos del volante ni los ojos de la carretera". Para más información: *http://www.apple.com/es/ios/carplay/*.

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

evidencia lo afirmado por Accenture (2016), de que la automatización inteligente es la plataforma de lanzamiento para el nuevo crecimiento e innovación en los grandes segmentos de consumo, incluyendo los vehículos.

A estos efectos, el gran hito que se vislumbra en el horizonte tecnológico es el vehículo conectado que pueda conducir sin asistencia humana, lo cual se convertiría en el mayor paso hacia delante de la tecnología automovilística en la historia. Las principales ventajas que ofrecen estos vehículos autónomos, según el secretario ejecutivo de la Comisión Económica de las Naciones Unidas para Europa, Christian Friis Bach (2015) son:

- Crearían desplazamientos más seguros: tienen el potencial de salvar miles de vidas, ya que los accidentes de carretera provocan 1.24 millones de muertos y 50 millones de heridos al año. Al tener el coche una visión constante a 360 grados, es capaz de adquirir más información y relacionar más de prisa que cualquier conductor humano.
- Crearían desplazamientos más eficientes, ya que estos coches pueden comunicarse entre ellos; pueden colaborar para limitar los atascos regulando el tráfico, determinando la velocidad óptima y minimizando los acelerones y frenazos constantes en los atascos que aumentan el consumo de combustible y la contaminación del aire.
- Más inclusión social: estos coches pueden fomentar la integración social ofreciendo a las personas discapacitadas un nuevo medio de acceder al mercado del laboral y a la sociedad en general. De la misma manera, las personas mayores podrían desplazarse fácilmente y mantener sus contactos sociales.

Estos grandes avances sólo podrían ser posibles, a nuestro entender, con la aplicación de las tecnologías de IoT. Por ejemplo, según la Association of Global Automakers (Safety Benefits of Connected Vehicles, 2013), una de las principales tecnologías relacionadas con el IoT que contribuiría a mejorar la seguridad de los vehículos en general son las Vehicle-to-Vehicle (V2V) y Vehicle-to-Infrastructure (V2I). Estas dos tecnologías permiten conectar mediante redes inalámbricas a todos los vehículos de

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

una zona con un sistema central, de forma que puedan evitar accidentes, evitar atascos y ahorrar combustible.[15]

Un claro ejemplo que pone de relieve la simbiosis existente entre el IoT y el vehículo conectado, es la aplicación MY SEAT, desarrollada por el fabricante SEAT junto con la consultora Accenture, y lanzada en febrero de 2016.[16] Dicha aplicación ofrece las siguientes posibilidades:

1) Conectar el coche y el hogar: a través de la geolocalización se puede replicar la temperatura del coche de manera automática en el momento en que éste se encuentre a cierta distancia del hogar. También permite la programación remota del termostato que controla la temperatura central de la casa, así como las luces o las cámaras de seguridad.
2) Alertar al conductor del estado del automóvil: permite la visualización de variables como los niveles de aceite y gasolina durante el viaje o cuando el coche está aparcado.
3) Monitorizar el comportamiento del conductor: ofrece consejos sobre cómo mejorar su conducción, recomendaciones para mejorar el funcionamiento del coche y pautas sobre cómo conducir de una manera más respetuosa con el medio ambiente.

Otro ejemplo en el que participa SEAT, pero esta vez con la colaboración de Samsung y SAP, tiene que ver con la garantía de que los usuarios permanezcan conectados al ciberespacio de manera segura cuando están al volante. En febrero de 2016,[17] dichas empresas anunciaron dos proyectos novedosos:

---

15 En relación con el apoyo que están recibiendo estas tecnologías, el gobierno federal de EUA anunció recientemente un plan de 10 años y cuatro billones de dólares para acelerar el avance de las tecnologías de seguridad en los vehículos. Para más información: *https://www.transportation.gov/briefing-room/secretary-foxx-unveils-president-obama's-fy17-budget-proposal-nearly-4-billion.*

16 Para más información: *https://www.accenture.com/es-es/company-newsroom-spain-ndp-accenture-y-seat* y *http://www.eleconomista.es/ecomotor/motor/noticias/7370807/02/16/Seat-y-Accenture-crean-una-app-que-avisa-del-estado-del-coche-y-lo-conecta-con-el-hogar.html.*

17 Para más información: *http://www.eleconomista.es/ecomotor/coches/noticias /7365403/02/16/SEAT-y-Samsung-alianza-tecnologica-con-SAP-para-el-coche-del-futuro.html* y *http://www.autobild.es/noticias/seat-samsung-sap-unidos-para-lograr-coche-conectado-282159.*

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

1) Reserva, guía y aparca remoto: mediante una aplicación se puede reservar una plaza de aparcamiento desde cualquier ubicación mediante el reconocimiento de la huella dactilar. Luego, el conductor es guiado hasta el parking reservado, abriéndose la barrera de seguridad de manera automática al reconocer el coche. Al finalizar el periodo de aparcamiento, el conductor puede pagar directamente desde la aplicación y sin salir del coche.
2) Digital Key Sharing: propuesta que permite hacer un duplicado de la llave de nuestro coche, pero de forma virtual con un simple gesto. Es decir, es una autorización del uso del coche sin tener que estar en posesión de la llave, incluso estando las personas en países diferentes, mediante un procedimiento de autorización seguro que transfiere una copia virtual de la llave digital del coche al Smartphone de la otra persona. La llave digital creada puede configurarse para durar un tiempo máximo e incluso se podría restringir una serie de prestaciones del coche como limitar la velocidad máxima.

Estos productos abren un mundo de posibilidades para los usuarios, pero también abren la puerta a amenazas que ya existen en este momento. Por ejemplo, ¿qué pasaría si un hacker astuto logra crear una llave digital maestra y pueda robarse coches que tengan esta tecnología? O ¿qué pasaría si un hacker decide atacar el sistema de pago conectado a nuestro coche, de forma que se transfiera dinero desde nuestra cuenta o desde la cuenta de la empresa del aparcamiento? Estas dos preguntas nos encaminan a la tercera parte de nuestro artículo, donde esbozamos los principales retos jurídicos identificados hasta el momento para los vehículos conectados.

IV. Retos jurídicos de los vehículos conectados

1. *Los retos de seguridad*

La expansión de los servicios de las TIC ha difuminado las fronteras con otros servicios, como el transporte, agricultura, educación y energía. El IoT, así como otros progresos en las esferas de tecnología y la regula-

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

ción[18] han multiplicado el potencial de contribución de las TIC al desarrollo social y económico, pero también han obligado a prestar más atención a cuestiones como ciberseguridad y la protección de datos (Unidas, 2015 y Desarrollo, 2015).

En el caso de la ciberdelincuencia, las dimensiones del mercado delictivo —en ámbitos como la extorsión en línea, las ventas ilícitas en línea y la violación y venta de datos— no dejan de crecer a medida que aumenta la proporción de la población mundial que se conecta a Internet (Unidas, 2015: 20).

Los ciberdelincuentes muchas veces están en búsqueda de información y datos de carácter personal que puedan rentabilizar en el corto plazo. Así, para Saif *et al.* (2015), la información más sensible recogida por los sensores y dispositivos conectados al coche incluye:

1) Hábitos de conducción.
2) Geolocalización.
3) Preferencias de entretenimiento.
4) Rutina diaria.

Nosotros añadiríamos al listado anterior la escucha del sonido interior vía los sistemas de telefonía de manos libres, así como las imágenes de video (tanto interior como exterior) de los conductores y los vehículos, provenientes de la multiplicación de cámaras para la acreditación probatoria en caso de siniestros.

Todos estos datos son propiedad del dueño del vehículo. No obstante, el acceso y utilización de los mismos, específicamente los renglones del listado anterior, pueden ser accedidos por los fabricantes y/o empresas sin necesidad de notificarlo (Consumer Privacy Protection Principles, 2014).

Toda esta información se transmite a través de tecnologías del IoT, como aplicaciones de teléfonos móviles, redes de telefonía móvil y servicios de comunicación SMS, los cuales ofrecen un nivel de seguridad bas-

[18] Un debate jurídico surgido como consecuencia de la introducción de las TIC en nuestra sociedad es en relación con los derechos fundamentales, el cual se concentra en la necesidad de potenciar la implantación de las TIC para el avance social, siempre dentro de un marco jurídico que permita proteger a los individuos de un posible uso abusivo (Salomón y Delgado, 2008).

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

tante deficiente en la mayoría de los casos,[19] haciéndolos vulnerables para todo tipo de ataques.

La cadena de transmisión de datos entre la empresa de la marca del coche, el concesionario, centros de datos de terceras partes, GPS, dispositivos inteligentes del hogar y los dispositivos de diagnóstico del coche, es donde se generan los puntos vulnerables y críticos en la seguridad del vehículo conectado (Saif *et al.*, 2015).

Para Pastor Pérez y Coz Fernández (Pérez y Coz, 2015), esta situación se debe en parte a que la competitividad actual de las empresas exige un rápido despliegue de los productos en el mercado, lo cual implica que algunos fabricantes con menos escrúpulos dejan la seguridad para el final del desarrollo o no la tienen en cuenta en absoluto. Así, el producto funciona y produce el resultado esperado, pero sin las medidas de seguridad apropiadas.

Un claro ejemplo de lo afirmado en el párrafo anterior, lo tenemos con el caso Jeep Cherokee acontecido en el verano de 2015. Se trata de una intrusión remota vía el sistema info-entretenimiento del vehículo Jeep Cherokee, modelo 2014, llevada a cabo por dos expertos en ciberseguridad, Charlie Miller y Chris Valasek. Mediante dicha intrusión, estos hackers lograron acceder a varios ECU del vehículo, controlando el aire acondicionado, la radio, las ventanas, los limpiavidrios, el acelerador y los frenos. La experiencia fue en realidad un experimento controlado por parte de los hackers, que luego fue documentado y publicado en un reportaje para la revista *Wired*[20] y que derivó también en un artículo[21] en donde Miller y Valasek exponían todos los detalles técnicos del mismo.

El resultado principal de este experimento fue que la empresa automotriz Fiat Chrysler llamó a revisión a 1.4 millones de vehículos ya vendidos, incluyendo no sólo el modelo Jeep Cherokee año 2014, sino también

[19] Según una entrevista con la BBC en octubre de 2015, Edward Snowden advirtió que los servicios secretos de varios países poseían herramientas capaces de infiltrar nuestros móviles de forma remota y sin que nos diéramos cuenta. Para más información: *http://www.bbc.com/news/uk-34444233*.

[20] Reportaje original disponible en: *http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/*.

[21] El artículo publicado por Miller y Valasek se encuentra disponible en: *http://illmatics.com/Remote%20Car%20Hacking.pdf*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

a otros cinco modelos del fabricante.[22] La revisión incluyó la sustitución del programa informático de info-entretenimiento, a través del cual Miller y Valasek pudieron acceder a los controles del vehículo.[23]

Relacionando este caso con los vehículos autónomos que ya han empezado a develarse,[24] la posibilidad de que los mismos sean objeto de intrusiones para provocar lesiones o daños tanto a sus pasajeros como a otros conductores, cobra mucha fuerza y se convierte en una amenaza real que debe ser la principal preocupación de los fabricantes de dichos automóviles.

A estos efectos, el FBI publicó en marzo de 2016 un informe sobre los peligros inherentes a los sistemas informáticos de los vehículos conectados, afirmando que la gran mayoría de los actuales vehículos conectados pueden llegar a ser controlados remotamente en determinadas circunstancias:

a) Vehículos conectados objetos de ataque, circulando a bajas velocidades (5-10 millas por hora):

- Apagado del motor.
- Inhabilitación de los frenos.
- Cambio de dirección en el guía.

b) Vehículos conectados objetos de ataque, circulando a cualquier velocidad:

- Seguros de las puertas.
- Señal de giro.
- Tacómetro.
- Radio y GPS.

22 Para más información: *http://www.bbc.com/mundo/noticias/2015/07/150723_fiat_chrysler_hackeo_revision_cch.*

23 Para más información: *http://www.computerworld.com/article/2952186/mobile-security/chrysler-recalls-14m-vehicles-after-jeep-hack.html.*

24 Véase el Model 3 de Tesla: *http://www.abc.es/motor/abci-tesla-revela-model-3-quiere-primer-vehiculo-electrico-masas-201604011009_noticia.html.*

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

2. *Los retos de la privacidad*

A finales de 2014, el Consejo de Derechos Humanos de las Naciones Unidas celebró una mesa redonda en la que se trató el tema del derecho a la privacidad en la era digital, y una de las conclusiones anotadas con relación a la protección legal de dicho derecho expresaba lo siguiente:

> Varias delegaciones señalaron que los Estados tenían preocupaciones legítimas de seguridad, incluida la amenaza del terrorismo y la ciberdelincuencia. Una delegación señaló que el uso de Internet para actividades delictivas y antisociales iba en aumento. Otra delegación señaló que la seguridad requería información, en particular con respecto a las comunicaciones digitales para combatir el terrorismo, mientras que otra afirmó que los gobiernos tenían la responsabilidad de proteger a las personas, y que la vigilancia de datos podía ser una medida eficaz y legítima con fines policiales. Había un amplio consenso, sin embargo, en que había que abordar las preocupaciones legítimas de seguridad en el marco del derecho internacional de los derechos humanos, incluido el derecho a la privacidad (Unidas, 2014).

En esta misma línea, la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (Unidas, 2015 y Desarrollo, 2015) expresó que una de las principales dificultades al elaborar ciber-legislación es encontrar un equilibrio entre la protección de los datos, la facilitación de su circulación y la libertad de información. Por un lado, la protección de datos de carácter personal cobra cada vez más vigencia debido al daño que puede ocasionar para los consumidores el robo, extravío o uso indebido de los mismos. Por otro lado, es fundamental para el comercio electrónico que exista un nivel adecuado de facilidad para la circulación de estos datos, condición necesaria para que los consumidores y las empresas puedan intercambiar servicios y productos de una manera rápida y eficiente.[25]

Para afrontar este dilema de tratamiento de la privacidad de los consumidores de los vehículos conectados, la Alliance of Automobile Manu-

[25] Los esfuerzos relacionados con el desarrollo del ecosistema digital y el comercio electrónico en la Unión Europea vienen trazados desde hace varios años en el proyecto de la Agenda Digital Europea, con sus aplicaciones subsecuentes en cada país miembro de la Unión. Para más información: *https://ec.europa.eu/digital-single-market/ y http://www.agendadigital.gob.es/Paginas/Index.aspx.*

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

facturers[26] redactó siete principios fundamentales relativos a la privacidad de los clientes de los fabricantes que forman parte de la entidad:

1) Transparencia: compromiso con la notificación y explicación oportuna de la recopilación, uso y transmisión de los datos personales de los propietarios y usuarios registrados de los vehículos.
2) Opción: se le ofrecerá a los propietarios y usuarios registrados ciertas opciones respecto a la recopilación, uso y transmisión de sus datos personales.
3) Respeto del contexto: el uso y la transmisión de los datos personales se hará siempre tomando en cuenta el impacto que pueda tener sobre los propietarios y usuarios registrados.
4) Almacenamiento de datos: los datos personales sólo serán recolectados y almacenados en función de necesidades legítimas del consumidor.
5) Seguridad de los datos: se implementarán medidas razonables de seguridad para salvaguardar los datos personales en caso de uso, acceso inapropiado o pérdida de los mismos.
6) Integridad y acceso: los propietarios y usuarios registrados tendrán medios razonables a su disposición que permitan el acceso y rectificación de sus datos personales.
7) Responsabilidad: los fabricantes se comprometen a implementar medidas para asegurar que tanto ellos como otras entidades que reciban los datos personales cumplan también estos principios de privacidad.

Este proyecto nos parece bastante interesante, ya que cuenta con un enfoque que abarca las principales preocupaciones que tienen los consumidores respecto a sus datos y que ya hemos mencionado anteriormente. No obstante, traemos a colación lo que Alonso *et al.* (1991) identificaron como los siete fallos primordiales en el mercado de los datos de carácter personal:

[26] Consumer Privacy Protection Principles (2014) es una entidad sin ánimo de lucro radicada en Washington DC, EUA, la cual agrupa a los siguientes fabricantes: Grupo BMW, Fiat Chrysler, Ford, General Motors, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi, Porsche, Toyota, Volkswagen América y Volvo América. Para más información: *http://www.autoalliance.org/about-the-alliance/overview.*

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

1) Falta de formación en la ciudadanía sobre protección de datos de carácter personal.
2) Impacto en los hábitos del consumidor ante brechas de seguridad o uso inadecuado de los datos de carácter personal.
3) Existencia de políticas de privacidad de difícil comprensión.
4) Existencia de regulación que refuerza la posición de dominio de grandes empresas en el uso de los datos.
5) Inexistencia de métricas que permitan conocer el beneficio neto que recibe el consumidor al compartir sus datos.
6) Existencia de normas sobre privacidad regresivas.
7) Dificultades para ejercer el derecho de no participar en el mercado.

En el caso de los vehículos conectados, dependiendo del servicio que el usuario o propietario del vehículo contrate, se pueden dar varias de las situaciones anteriores. Por ejemplo, el registro de los hábitos de conducción y geolocalización, recopilado por una red social y cuya información puede ser comercializada a terceros. Este es el caso de las aplicaciones de Google Maps y Google Traffic, las cuales recopilan información de hábitos de conducción, rutas y geolocalización que luego puede ser vendida a otras empresas para fines comerciales.[27]

No hablamos en este caso de las violaciones de la intimidad que sean delito o se cometan para propiciar delitos, sino más bien de los retos que para la ciudadanía supone el mando de la privacidad por las empresas y los estados en un entorno de economía de mercado capitalista.

3. *Distintas iniciativas recientes para afrontar los retos*

La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo afirmó lo siguiente respecto a la confianza de los consumidores en línea:

> …era necesario que conocieran el valor y las posibilidades de comercialización de sus datos y comprendieran la forma en que éstos se gestionaban. También debían conocer los medios a su disposición para garantizar la protección de los datos. Ese mayor conocimiento reduciría su vulnerabilidad a la ciberdelincuencia y haría que los consumidores pudieran reclamar activa-

[27] Para más información: *http://www.techinsider.io/how-google-maps-knows-about-traffic-2015-11*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

mente su privacidad. Con el tiempo, los usuarios también podrían compartir el valor de su información personal (Unidas, 2015 y Desarrollo, 2015).

Partiendo de la necesidad de reducir los niveles de vulnerabilidad de cara a la ciberdelincuencia, la propia Organización de las Naciones Unidas (Unidas, 2015) afirmó recientemente que la adopción de respuestas nacionales de carácter legislativo y normativo debe darse en los siguientes ámbito:

1) Tipificación de delitos y competencias procesales.
2) Capacidad de las autoridades encargadas de hacer cumplir la ley y de la justicia penal para investigar la ciberdelincuencia, las técnicas forenses digitales y el manejo de pruebas electrónicas.
3) Mecanismos judiciales de cooperación internacional en asuntos penales.

Precisamente los delitos cibernéticos no son cuestiones de índole interna en cada país, sino que trascienden las fronteras nacionales y, por tanto, requieren soluciones transnacionales. En la gran mayoría de los casos, estas soluciones se traducen en la participación activa en los foros internacionales dedicados a abordar las cuestiones de ciberseguridad (Hathaway *et al.*, 2015).

De igual forma, la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (Unidas, 2015 y Desarrollo, 2015) concluyó que el impulso para la reforma de la ciber-legislación implica que los gobiernos establezcan amplias horas de ruta en las que se detallaran objetivos y plazos, los cuales faciliten el seguimiento y la notificación de toda novedad a las instituciones regionales y organizaciones internacionales.

Las medidas políticas para luchar contra la ciberdelincuencia implican el fortalecimiento de los organismos de ciberseguridad y la difusión de la conciencia de la ciberdelincuencia, de forma que se pueda aprobar una legislación adecuada para que los derechos humanos universales se respeten tanto en línea como fuera de línea (Unidas, 2015).

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

Desde EUA, la Auto Alliance[28] destaca las siguientes iniciativas que se están desarrollando desde dicho país para afrontar proactivamente los retos de ciberseguridad que afronta la industria:

- La organización anual de eventos tipo *hackathon*, como la SAE Battelle CyberAuto Challenge,[29] organizada por la asociación internacional SAE International, que agrupa a más de 138,000 ingenieros y expertos técnicos aeroespaciales y automotrices.
- La creación de organismos e instituciones de diversa índole:
  - El Cyber-Physical Systems Task Force.[30]
  - El Automotive Consortium for Embedded Security (ACES),[31] cuya misión principal es investigar los temas relacionados con la seguridad, fiabilidad, imagen y privacidad para los clientes de coches.

Finalmente, el estado de California (Summary of Draft Autonomous Vehicles Depoyment Regulations, 2015) ha propuesto en el borrador de reglamento para la regulación de los vehículos conectados y autónomos, que los mismos tendrán que tener un sistema de auto-diagnóstico de alto estándar que sea capaz de detectar, responder y alertar el operador del vehículo en relación con un ciber ataque o una intrusión no autorizada.

Muchos son los aspectos sobre los que habrá que profundizar a futuro, pero debemos ahora dar por finalizada esta contribución cerrando algunas conclusiones para la reflexión.

V. Conclusiones

1) El futuro inmediato nos traerá una enorme cantidad de servicios a través del IoT, que progresivamente, aunque con velocidad exponencial, se irá manifestando. Dichos servicios se distribuirán allá donde el usuario se encuentre, sea en su casa o lugar de trabajo, o mientras se desplaza de un lugar a otro, también en su medio de locomoción.

28 *http://www.autoalliance.org/auto-issues/cybersecurity*.

29 *http://www.sae.org/events/cyberauto/*.

30 *http://www.uscar.org/guest/teams/43/Cyber-Physical-Systems-Task-Force*.

31 *http://www.swri.org/4org/d10/comm/aces/*.

Boletín Mexicano de Derecho Comparado, núm. 154, enero-abril de 2019, pp. 457-488.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

2) La utilización masiva de IoT acarrea la asunción de una serie de riesgos y amenazas por la permeabilidad de las redes de comunicación y dispositivos que sustentan el IoT. Dichos compromisos de seguridad pueden afectar a la seguridad física y lógica propiamente dicha, o también a la privacidad de los usuarios, bien sea para la comisión de delitos o simplemente para su explotación en el mercado de *Big Data*.
3) Los legisladores no deben ignorar el ritmo de la evolución tecnológica para no tolerar quebrantos en la seguridad y privacidad de las personas, del mismo modo no deberían utilizar dichas tecnologías ilegítimamente por sí mismos y sin control.
4) La educación y la inversión en I+D a manos de universidades y empresas debería ayudar a reducir los riesgos cibernéticos derivados del IoT, así como de la utilización masiva de vehículos conectados a la red.

VI. Bibliografía

ACCENTURE, 2016, *Accenture Technology Vision 2016*, Nueva York, Accenture.

ACCENTURE, "Digital Transformation of Industries", *Foro Económico Mundial*. Disponible en: *https://www.weforum.org/global-challenges/future-of-the-internet/projects/ digital-transformation-of-industries*.

ASSOCIATION, GROUPE SPECIALE MOBILE, 2013, "Connected Car Forecast: Global Connected Car Market to Grow Threefold within Five Years". Disponible en: *http://www.gsma.com/connectedliving/wp-content/uploads/ 2013/06/cl_ma_forecast_06_13.pdf.*

ASSOCIATION OF GLOBAL AUTOMAKERS, "Safety Benefits of Connected Vehicles", 2013, *http://www.globalautomakers.org/topic/vehicle-vehicle-technology.*

BACH, Christian Friss, 2015, "La cooperación internacional debe fomentar los coches autónomos". Disponible en: *https://itu4u.wordpress.com/spanish/international-cooperation-must-drive-autonomous-cars/*.

BANKINTER, FUNDACIÓN DE LA INNOVACIÓN, 2011, "El Internet de las cosas en un mundo conectado de objetos inteligentes". Disponible en: *https://www.fundacionbankinter.org/ftf/iot*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

California Department of Motor Vehicles, 2015, "Summary of Draft Autonomous Vehicles Depoyment Regulations". Disponible en: *https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/auto.*

Cayón Peña, Juan y García Segura, Luis Armando, 2015, "Hacia un nuevo enfoque del conflicto ciber en el ámbito empresarial", *Diario La Ley*.

Centro de Seguridad Tic de la Comunidad Valenciana, 2014, "Seguridad en internet de las cosas. estado del arte". Disponible en: *http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D Informe-Internet_de_las_Cosas.pdf.*

Alliance of Automobile Manufacturers, 2014, "Consumer Privacy Protection Principles". Disponoible en: *http://www.autoalliance.org/auto-issues/automotive-privacy/principles*.

Deloitte, "Capitalizando en la promesa y el poder del internet de las cosas". Disponible en: *http://www2.deloitte.com/co/es/pages/strategy/articles/cfoiot.html#.*

Desarrollo, Conferencia de las Naciones Unidas sobre Comercio, 2015, "Informe de la reunión de expertos sobre ciberlegislación y regulación para promover el comercio electrónico, con estudios de casos y análisis de experiencias, TD/B/C.II/EM.5/3". Disponible en: *http://unctad.org/meetings/es/SessionalDocuments/ciiem5d3_es.pdf.*

Estrada Alonso, Eduardo, 1991, *Las uniones extramatrimoniales en el derecho civil español*. Madrid.

Parlamento Europeo, 1995, *Directiva 95/46/CE Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,* Diario Oficial, núm. L 281 de 23/11/1995.

Parlamento Europeo, 2016, "Reforma de la protección de datos – nuevas reglas adaptadas a la era digital". Disponible en: *http://www.europarl.europa.eu/news/es/news-room/20160407IPR21776/Reforma-de-la-protección-de-datos-—-Nuevas-reglas-adaptadas-a-la-era-digital.*

FBI, "Motor Vehicles Increasingly Vulnerable to Remote Exploits. Alert num. I-031716-PSA". Disponible en: *http://www.ic3.gov/media/2016/160317.aspx*.

Fjord & Accenture, 2015, "The Era of Living Services". Disponible en: *https://www.accenture.com/t20151012T100130__w__/usen/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_22/The-Era-ofLiving-Services-Accenture-Digital.pdf#zoom=50*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

FRIESS, Peter, 2013, "Driving European Internet of Things Research", en VERMESAN, Peter (ed.), *Internet of Things- Converging Technologies for Smart Environments and Integrated Ecosystems*, Dinamarca, Ovidiu & Friess, River Publisher.

HATHAWAY, Melissa *et al.*, 2015, "Índice de Preparación Cibernética 2.0 (Arlington: Potomac Institute for Policy Studies)".

INTERACTIVE ADVERTISING BUREAU, 2014, "Estudio anual de coches conectados". Disponible en: *http://www.iabspain.net/wp-content/uploads/downloads/2014/07/Informe-coches-cpnectados-2014.pdf.*

KATZ, Raúl, 2015, "El ecosistema y la economía digital en América Latina", Madrid, Fundación Telefónica.

LAWSON, Philippa *et al.*, 2015, *The Connected Car: Who Is in the Driver's Seat?*, Vancouver.

FORO ECONÓMICO MUNDIAL, 2016, "Digital Media and Society: Implications in a Hyperconnected Era", Ginebra.

FORO ECONÓMICO MUNDIAL, "The Impact of Digital Content: Opportunities and Risks of Creating and Sharing Information Online", Ginebra, Global Agenda Council on Social Media & Foro Económico Mundial.

PANADERO, José, 2012, "ECU, qué es y el porqué de su existencia". Disponible en: *http://www.diariomotor.com/tecmovia/2012/07/03/ecu-que-es-y-el-porque-de-su-existencia/.*

PASTOR PÉREZ, Vicente José y COZ FERNÁNDEZ, José Ramón, 2015, "La ciberdefensa militar ante el reto de internet de las cosas", *Revista SIC,* 116, septiembre.

PWC, 2015, "Cómo aprovechar los beneficios de las soluciones sobre Internet de las cosas". Disponible en: *http://www.gsma.com/connectedliving/wp-content/uploads/2015/05/Web-Realising-the-benefits-of-mobile-IoTsolutions-ES.pdf.*

RIFKIN, Jeremy, 2015, "El auge del Internet de las cosas y la carrera por una sociedad con coste marginal cero". Disponible en: *http://www.huffingtonpost.es/jeremy-rifkin/internet-de-las-cosas_b_8416822.html# %0A%0A.*

SAIF, I. *et al.*, 2015, "Safeguarding the Internet of Thing", *Deloitte Review.*

SALOMÓN SANCHO, Lourdes y DELGADO GARCÍA, Ana María, 2008, "Algunas reflexiones en torno a los aspectos jurídicos de la sociedad de la información", *Anuario Da Facultade de Dereito Da Universidade Da Coruña.*

DOI: http://dx.doi.org/10.22201/iij.24484873e.2019.154.14150

Unión Internacional de Telecomunicaciones, 2011, "Recomendación UIT-R M.1890". Disponible en: *http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1890-0-201104-I!!PDF-S.pdf.*

Consejo De Derechos Humanos De Las Naciones, Unidas, 2014, "Resumen de la mesa redonda del Consejo de Derechos Humanos sobre el Derecho a la Privacidad en la Era Digital, A/HRC/28/39". Disponible en: *http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Documents/A_HRC_28_39_SPA.doc.*

Consejo De Derechos Humanos De Las Naciones, Unidas, 2014, "Tecnologías de la información y las comunicaciones para un desarrollo social y económico incluyente. E/CN.16/2014/3". Disponible en: *http://unctad.org/meetings/es/SessionalDocuments/ecn162014d3_es.pdf.*

Consejo De Derechos Humanos De Las Naciones, Unidas, 2015, "Progresos Realizados en la aplicación y el seguimiento de los resultados de la Cumbre Mundial sobre la Sociedad de la Información a Nivel Regional e Internacional, A/70/63-E/2015/10". Disponible en: *http://unctad.org/es/PublicationsLibrary/a70d63_es.pdf.*

Organización De Las Naciones Unidas, 2015, "13 Congreso de las Naciones Unidas sobre Prevención del Delito y la Justicia Penal, A/CONF.222/12". Disponible en: *http://www.un.org/es/events/crimecongress2015/.*

Zamora, Alberto y Vergara, Miguel, 2015, *El Internet de las cosas en la estrategia de los ejecutivos españoles*, Madrid.

Zurich, 2014, "Smart Cars and Connected Vehicles. Zurich Insurance Company". Disponible en: *https://www.zurichcanada.com/en-ca/knowledge-hub/articles/2015/11/smart-cars-and-connected-vehicles*.