

PROYECTO TECHNOS

Internet of Things y su impacto en los Recursos Humanos y en el Marco Regulatorio de las Relaciones Laborales



CUATRECASAS
Instituto de
Estrategia Legal
en RRHH

■ LA LEY



CUATRECASAS



Wolters Kluwer

PROYECTO TECHNOS

Internet of Things y su impacto
en los Recursos Humanos
y en el Marco Regulatorio
de las Relaciones Laborales


CUATRECASAS
Instituto de
Estrategia Legal
en RRHH

Consulte en la web de Wolters Kluwer (<http://digital.wke.es>) posibles actualizaciones, gratuitas, de esta obra, posteriores a su publicación.

© Instituto Cuatrecasas, 2017

© Wolters Kluwer España, S.A.

Wolters Kluwer

C/ Collado Mediano, 9

28231 Las Rozas (Madrid)

Tel: 902 250 500 – Fax: 902 250 502

e-mail: clientes@wolterskluwer.com

Primera edición: Octubre 2017

Edición electrónica: <http://www.wolterskluwer.es>

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

Printed in Spain

© **Wolters Kluwer España, S.A.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, Wolters Kluwer España, S.A., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **Wolters Kluwer España, S.A.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

PROYECTO TECHNOS

INTERNET OF THINGS Y SU IMPACTO EN LOS RECURSOS HUMANOS Y EN EL MARCO REGULATORIO DE LAS RELACIONES LABORALES

Cuatrecasas

Director

Salvador DEL REY GUANTER

Presidente

Instituto Cuatrecasas de Estrategia Legal en RRHH

Socio de Cuatrecasas

*Catedrático de Derecho del Trabajo y de la Seguridad Social
(ESADE Law School)*

Coordinador

Guillermo TENA PLANAS

Director

Instituto Cuatrecasas de Estrategia Legal en RRHH

Consejero de Cuatrecasas

C. Aspectos nuevos que aparecen en IoT

Más interesante quizá que profundizar en los aspectos tecnológicos, es identificar qué cuestiones están cambiando y, en algunos casos, surgiendo de manera reveladora para la sociedad con el desarrollo de IoT respecto a la situación pre-IoT.

Podría entenderse que IoT es en definitiva una red para los objetos. Es decir, una red de dispositivos IoT que son el sujeto y objeto de los servicios que son proporcionados entre ellos sin intervención humana, como sería el telecontrol de una válvula remota desde un ordenador de control. O que un medidor del nivel del agua se conectara con el centro de control para proporcionar las mediciones de pantanos o de la red de distribución de manera automática. Suelen ser configuraciones con una baja o nula presencia humana. Pero en otros casos, estos dispositivos forman parte del entorno de las personas y proporcionan servicios que tienen relación con las personas en sus diferentes facetas privadas, laborales y sociales. En estos casos, que son muchos, el despliegue de IoT tiene una serie de repercusiones en el ámbito social que son nuevos con respecto a una red Internet más clásica. Se presentan en las siguientes secciones algunos de estos aspectos.

1. *Comportamiento de las personas en la Red*

Una de las repercusiones más obvias es que IoT supone una transformación con respecto a cómo las personas se comportan para usar los servicios de la red. Para los servicios más clásicos de Internet, como descargarse unos contenidos, ver una película, realizar una llamada o enviar un mensaje, la actividad requiere de acciones explícitas, conscientes, y normalmente acotadas en un espacio temporal. Con la IoT, la interacción se realiza muchas veces con una baja intervención humana, de manera imperceptible. Las personas no son realmente conscientes de que se está produciendo una actividad, ni suele ser relevante el espacio temporal de cuándo sucede. Que nuestro móvil haga un *roaming* desde la red celular a la red wifi cuando llegamos a la oficina, que nuestra tableta vaya saltando de punto de acceso a punto de acceso mientras nos desplazamos por la fábrica, que nuestro vehículo (o móvil) esté enviando información con su posición y velocidad, o que nuestra pulsera (o una cámara) esté registrando nuestra actividad, y quizá compartiéndola, son algunos ejemplos que ilustran esta transformación en el modo de interacción. Y esto se multiplica a medida que se multiplica la "inteligencia ambiental" y las personas nos equipamos con más y más dispositivos inteligentes.

2. *Las esferas privadas, sociales y laborales se superponen*

Por un lado, los terminales clásicos de acceso a la red se han ido desvinculando del modo de para qué se usan. Con respecto a lo que ocurría en la red Internet del siglo XX, cuando el terminal estaba fundamentalmente asociado a un determinado rol, nuestros portátiles, tabletas o móviles actuales pueden usarse tanto para uso laboral como personal independientemente de cuál sea su propietario: llamadas, mensajería, mensajes, contenidos...

Pero sobre todo, porque estos dispositivos establecen vinculaciones y conexiones con otros dispositivos del espacio personal, público o profesional, generando una compleja red de relaciones entre los dispositivos entre sí, entre dispositivos y personas, y entre personas que mezclan todas las esferas.

3. *Un nuevo desafío a las expectativas de privacidad*

Otro elemento de repercusión tiene relación con la privacidad, porque IoT impone nuevos desafíos a las expectativas de privacidad de las personas. Toda esa información que se genera o se consume en un dispositivo IoT de nuestro entorno, sea de nuestra propiedad o no, toda la información acerca de la interacción que tenemos con ellos, consciente e inconscientemente, y toda la información acerca de las relaciones y vinculaciones de nuestros dispositivos, queramos o no queramos, estará en algún lugar de la nube. Junto con los de otras muchas personas y dispositivos. Tanto la información que produce un termómetro IoT como la que produce un dispositivo personal vinculado, por ejemplo, a nuestra salud. O la que produce el vehículo de alguno de nuestros compañeros de viaje. O la que produce un punto de acceso wifi en la oficina y la cámara de control de acceso. Sin una perfecta distinción de qué información es privada, social o profesional. Ni un conocimiento profundo de cómo se utiliza, analiza, gestiona, comercializa o trata. Ni siquiera por quién lo hace, más allá de las aplicaciones explícitas o evidentes.

4. *Responsabilidad sobre la seguridad*

La expansión de IoT irá impregnando todas las facetas de nuestra vida cotidiana y de los sistemas que operan el mundo hasta convertirse en una parte esencial para el funcionamiento de cualquier servicio. Si nuestros vehículos, los sistemas de tráfico, las cerraduras, los cajeros, etc., están conectados, garantizar la protección respecto a ciberataques resulta un

aspecto crítico. Lo más importante es que una intervención malintencionada puede producir daños incalculables, como podría ser un ataque a un sistema de señalización ferroviario o a un sistema de control de una central energética. Pero además de estas cuestiones de seguridad tan graves, es importante contemplar que los dispositivos IoT sean también robustos para evitar el robo y apropiamiento de información sensible, como contraseñas, claves, contactos, datos privados o confidenciales. Que muchas veces es la vía para poder pasar a otros planos de agresión.

La extensión de IoT a multitud de objetos cotidianos interconectados entre sí incrementará los puntos de vulnerabilidad. Algunos de estos sistemas podrán protegerse mejor. Por ejemplo, cuando el producto sea suficientemente potente y tenga la capacidad para hacerlo. Sin embargo, muchos dispositivos IoT se fundamentan en componentes sencillos por motivos de coste de implantación, componentes que son fácilmente vulnerables a ataques que también pueden causar un alto impacto. A finales de 2016, un ciberataque masivo a cámaras de videovigilancia se utilizó para dejar sin servicio a un conjunto de webs con mayor tráfico del mundo.

Pero hay que considerar que muy probablemente la protección total y absoluta es imposible. Ante esto, la responsabilidad de mitigar el riesgo se está compartiendo entre muchos actores, como fabricantes de dispositivos, operadores de infraestructuras, proveedores de servicios y reguladores. Y también parte de esta responsabilidad se está trasladando implícitamente, incluso a veces explícitamente, a los propios usuarios. Pero debido a la densidad de interrelaciones y operaciones que existen en la red y lo difíciles que son tanto de conocerlas como de percibir las implicaciones que tienen, resulta para las personas prácticamente imposible comprender el riesgo y actuar consecuentemente para mitigar la vulnerabilidad.

5. *Responsabilidades sobre aspectos regulatorios y legales*

El flujo de información se mueve en Internet sin ninguna restricción con respecto a las fronteras naturales y políticas. Los requisitos legales aplicables en el lugar donde se produce parte de los servicios de un sistema IoT pueden ser diferentes o, incluso, incompatibles, con los que se aplican en el lugar donde se produce otra parte del servicio, como podría ser el almacenamiento de determinados datos. En otros casos puede tratarse de dos servicios diferentes que, a través del propio dispositivo IoT del usuario, o entre dispositivos asociados a cada servicio pero interconectados entre sí, por ejemplo en un entorno de operación del usuario, se intercambian información que debe ser

tratada desde el punto legal de una manera diferente. Son operaciones que ocurren con un bajo conocimiento y baja consciencia por parte de los usuarios, por lo que trasladar la responsabilidad a estos usuarios para cumplir los requisitos legales puede resultar impracticable.

6. *Posibilidad de opción, quizá no para todos*

El histórico de información que recolectan muchos dispositivos IoT y su análisis profundo aporta un conocimiento muy valioso acerca de los hábitos, costumbres y condiciones de las personas relacionadas con estos dispositivos. Un sistema de tracking para personas mayores, los propios datos de posición, velocidad y aceleración del coche, contadores de consumo, pulseras de actividad... Muchas empresas, especialmente aseguradoras, están estudiando y, en algunos casos, aplicando sistemas de incentivos económicos para acceder a esta información para aplicar condiciones personalizadas. Aunque estos incentivos sean de momento opcionales, para aquellas personas en condiciones económicas más precarias puede que no lo sean de facto, ya que deben acogerse necesariamente a las condiciones impuestas para conseguir las ventajas financieras.

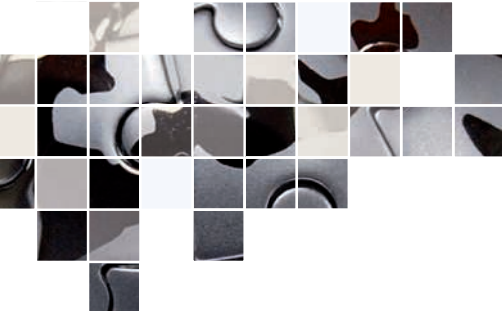
Quizá este aspecto se amplifique aún más en el mundo laboral, especialmente necesitado ahora por optimizar costes e incrementar la productividad. La IoT es una poderosa herramienta para mejorar la competitividad.

7. *IoT como vehículo de prestación de servicios*

La instrumentación de los productos físicos para convertirlos en productos conectados con servicios digitales abre la vía a la prestación de servicios. Forma parte de una corriente denominada "servitización", entendida como la prestación de servicios por estas empresas en conjunción o no con sus productos físicos. Es una manera de añadir valor a través de fórmulas intangibles que representan una ganancia o beneficio para un cliente, consumidor, usuario o paciente. Aunque no es un fenómeno nuevo, la extensión de IoT va a suponer sin duda una extensión y aceleración de la propuesta de servitización, porque incrementa los canales y puntos de interacción con el entorno del cliente.

Algunos ejemplos ilustrativos pueden ser AMAZON *Dash Buttons* y AMAZON *Dash Replenishment Service*⁽¹⁰⁾. El primero consiste en un dispositivo en forma de botón que puede ser instalado en cualquier lugar, por ejemplo,

(10) www.amazon.es Innovaciones.



Como es conocido, en la actualidad nos encontramos ante una revolución de los datos masivos (Big Data) derivada de la revolución de internet y el crecimiento exponencial de los avances tecnológicos, que está cambiando radicalmente cómo nos comunicamos, socializamos, nos entretenemos y, desde luego, la forma en la que trabajamos.

Esta explosión de datos se ve reforzada por el desarrollo de *Internet of Things* (IoT), el cual además se inscribe en la “gran convergencia” de tecnologías disruptivas como son, entre otras, la Inteligencia Artificial, la Robótica o la Impresión en 3D, que unido al aumento de la capacidad de procesamiento y almacenaje de datos provenientes de fuentes dispares, hace que tales cambios tecnológicos desarrollen unos efectos sobre la organización del trabajo y los recursos humanos sin precedentes. Esas tecnologías disruptivas están confluyendo y suponen cada vez una mayor complejidad en la red de relaciones entre los dispositivos tecnológicos entre sí, entre dispositivos y personas, y, por último, entre personas, lo cual conlleva una superposición de las esferas privada, social y laboral.

El *Instituto Cuatrecasas de Estrategia Legal en RRHH* presenta, en el marco del **PROYECTO TECHNOS**, proyecto que está desarrollando el Instituto (2016-2019) y que tiene como objetivo identificar la incidencia en el entorno laboral de diferentes tecnologías disruptivas, su **Segundo Informe** que en esta ocasión está dedicado a “**INTERNET OF THINGS Y SU IMPACTO EN LOS RECURSOS HUMANOS Y EN EL MARCO REGULATORIO DE LAS RELACIONES LABORALES**”.

Aplicada en el lugar de trabajo, la tecnología de IoT implica una hiperconectividad de carácter multilateral que impacta en la organización de la empresa, en la gestión de los recursos humanos y en el mercado laboral.

