Evidencia 3 – Recopilación de datos.

Apellidos: García García

Nombre: Jorge

Grupo: Grupo 1

Horas totales: 5 horas

Evidencias:

NOTA: Para la realización de este trabajo he empleado 2 horas en búsqueda de fuentes e investigación y 3 horas en redacción y formateado del documento.

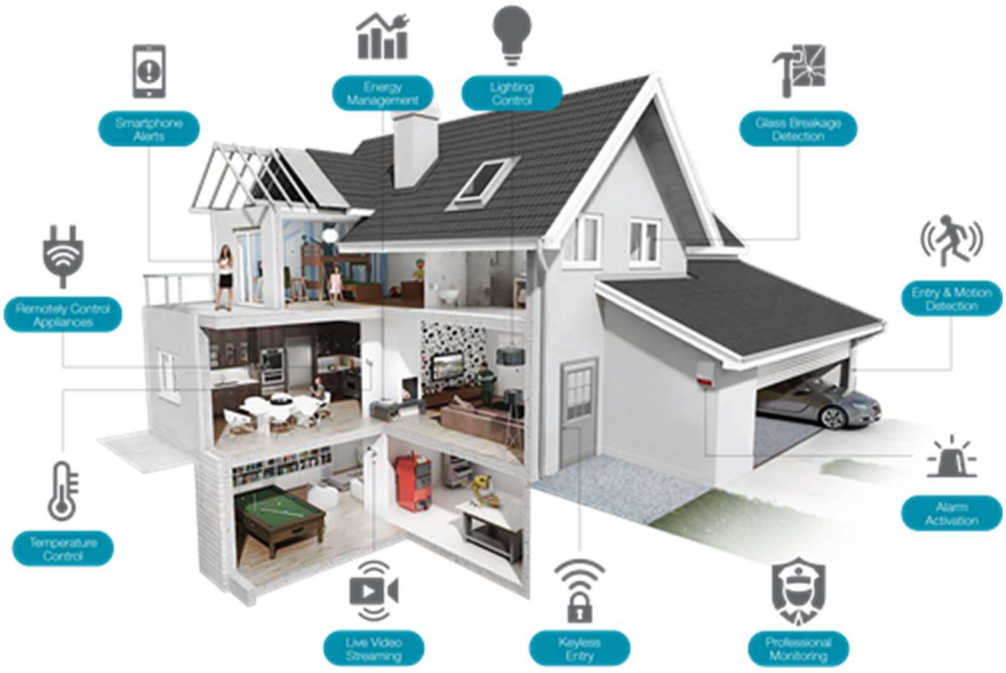
Introducción

Que sabe internet de ti fue el título de la conferencia a la que asistí el pasado 9 de noviembre, cuyo ponente fue Jorge Coronado. La ponencia, tal y como su nombre indica, trató principalmente sobre la gran cantidad de datos que es almacenado de cada uno de nosotros en la red. Datos, que son accesibles y pueden aportar mucha información a la hora de "clasificar" a una persona, conocer sus amistades e incluso sus hábitos de vida, y todo al alcance de unos pocos clics y un poco de conocimiento. Además, Jorge nos mostró diversos usos positivos que se le podía dar a esta información, como puede ser la búsqueda de personas desaparecidas. Este trabajo se centrará sobre todo en la capacidad de las grandes empresas para recopilar y tratar dichos datos a menudo sin que sus usuarios sean conscientes.

Principio del problema

Actualmente, vivimos en una sociedad "conectada" que no puede vivir sin relacionarse con el mundo. La forma en la que nos comunicamos ha cambiado completamente, sobre todo en los últimos años. Hemos pasado de enviar cartas manuscritas a enviar múltiples correos electrónicos, de anotar nuestras citas en una agenda a anotar e incluso programar alarmas en calendarios en la nube o de buscar en enciclopedias información a buscar en navegadores que nos proporcionan millones de resultados en décimas de segundos, y todo ello con una simpleza pasmosa. Para realizar todas estas acciones cotidianas adaptándonos a la forma actual de hacer las cosas necesitamos estar "conectados", conectados mediante dispositivos a internet. Comúnmente suele pensarse que con no utilizar el ordenador o desconectar los datos móviles de nuestro smartphone ya estamos fuera de línea, pero lo que no mucha gente sabe

es que **no solo los ordenadores o los smartphones tienen la capacidad de estar conectados**. A día de hoy, desde televisiones, frigoríficos, robots de limpieza hasta luces que puedes encender desde cualquier parte del mundo, tienen acceso a internet y están conectados prácticamente 24/7, sin descanso. Así nació el término conocido como ***IoT (Internet of Things)***. El *Internet of Things* o *Internet de las Cosas* consiste en que todos los dispositivos estén conectados entre sí de forma que puedan trabajar de forma inteligente y siempre pudiendo mantener el control del aparato estés donde estés.



A priori esto puede parecer fantástico, que lo es, pero también tiene una serie de "problemas" que la gente desconoce. De los problemas que presentan los dispositivos englobados en este término y para relacionarlo con el tema de la conferencia expuesta por Jorge Coronado, nos centraremos en la problemática existente en que estos dispositivos monitoricen, de forma indirecta, tantos datos sobre nosotros.

La recopilación de datos en el uso cotidiano en la actualidad.

Los dispositivos que pertenecen al llamado *Internet de las Cosas* **necesitan estar conectados**, bien vía ethernet o vía WiFi, a internet. Gracias a esa conectividad se nos permite a nosotros como usuarios manejarlos remotamente, por ejemplo, desde nuestro smartphone. Claro está que para que esto funcione, habitualmente es necesario vincular el dispositivo inteligente a una nuestra cuenta correspondiente de la empresa fabricante del producto. Por ejemplo, si nos compramos el asistente de voz de Google, *Google Dot*, para poder utilizarlo necesitaremos vincularlo a nuestra cuenta de Google y además deberá de tener acceso a internet para poder usarlo desde cualquier dispositivo desde el que tengas acceso a tu cuenta. Tecnológicamente hablando el ejemplo anterior lleva consigo un mensaje implícito, para que este funcionamiento sea posible **las órdenes tienen que pasar primero por los servidores** de Google, donde **quedarán registradas** y acto seguido serán dirigidas al o los dispositivos vinculados a tu cuenta. Existen cientos de ejemplos similares al anterior y no solo Google realiza este tipo de operaciones. Cualquier empresa que proporcione dispositivos inteligentes necesitará de estos métodos para que todo funcione correctamente.

Hasta este punto todo pinta genial, tenemos empresas que nos permiten conectar nuestros aparatos para automatizar y facilitar su uso desde cualquier lugar. Pero como era de esperar, en el afán de las empresas por "clasificarnos", por conocer nuestros hábitos y con el fin de tener un mayor control de sus usuarios, no solo utilizan nuestros dispositivos para lo que están destinados. Para comprender mejor la gravedad del asunto, expondré a continuación varias situaciones cotidianas en las que se recaba información sin que nos demos cuenta.

Volviendo al ejemplo anteriormente mencionado del *Google Dot*, al vincularlo a tu cuenta aceptas los términos y condiciones de Google en los que se indica que toda conversación que se mantenga con el *Google Dot* será registrada y almacenada para su tratamiento y de esta forma mejorar su funcionamiento. Es decir, toda pregunta que se le realice quedará guardada de forma que si, por ejemplo, se le pregunta algo como *¿qué tiempo hará mañana en Madrid?* les permitirá conocer la existencia de algún interés por parte del usuario en Madrid, por lo que indirectamente les acabas de regalar una información muy jugosa.

Pongamos que una persona compra unas bombillas inteligentes para su dormitorio. Estas bombillas, no solo permiten apagar y encender las bombillas desde el teléfono móvil, si no que nos permite programar que se enciendan por ejemplo a la hora de despertarnos. Esos datos son almacenados en los servidores de la compañía fabricante de las bombillas permitiéndole conocer sus hábitos de sueño. A simple vista se puede pensar, *¿qué importancia le puede suponer a una empresa saber a qué horas duermo?* Pues bien, gracias a esto la empresa podría conocer más acerca de tu forma de vida, si duermes las horas necesarias o no, si sueles ir a dormir a siempre a la misma hora o no, si tienes un trabajo fijo o por el contrario te encuentras en el desempleo.

Como último ejemplo, existen frigoríficos inteligentes que proporcionan al usuario información sobre las temperaturas a las que se encuentra el interior, permiten regular la temperatura de

los compartimentos por separado y ocultamente pueden registran las veces que se abre y se cierra el frigorífico a lo largo del día. Con esas funcionalidades pueden saber sobre qué horas sueles encontrarte en casa, cada cuanto visitas el frigorífico y demás información fruto del tratamiento de tal cantidad de datos.

Todos estos datos son utilizados por las empresas para conocer más acerca de las necesidades de sus usuarios y por si no fuera poco **puede extrapolarse a cualquier dispositivo** que este acuñado bajo el termino *IoT*.

La recopilación de datos por otros métodos

Llegados a este punto es cuando uno comienza a plantearse si realmente merece la pena el usar dichos aparatos tan avanzados, cómodos y a la par desconocidos o plantearse elegir lo malo conocido.

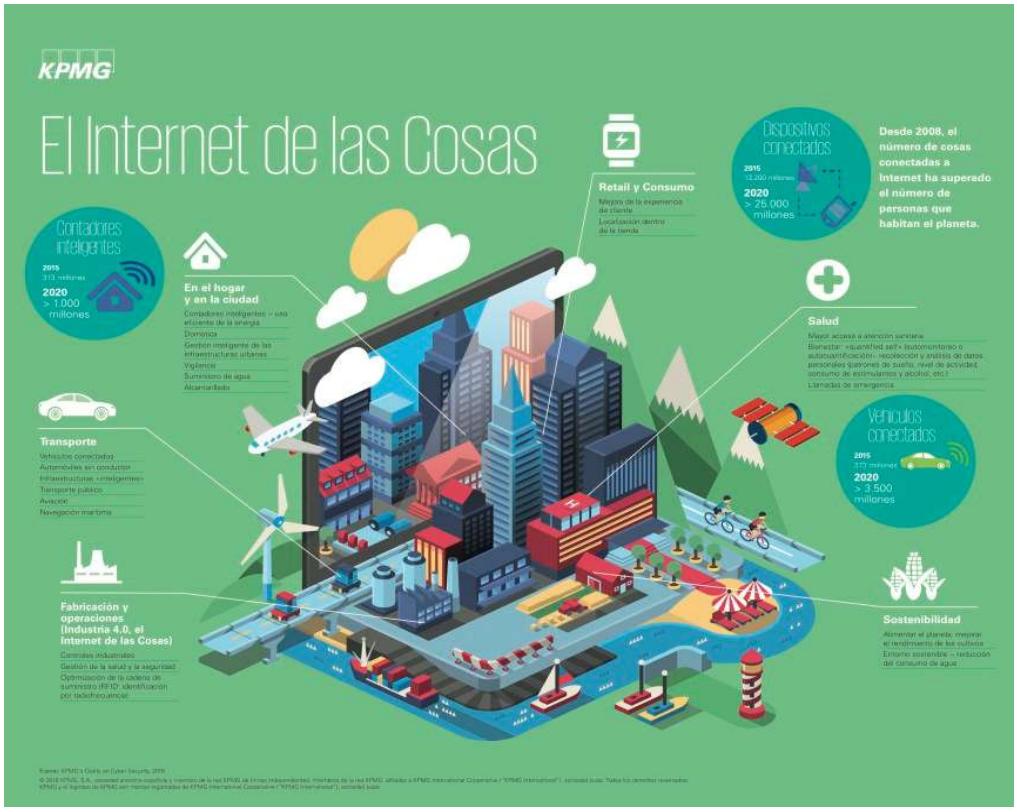
Lo cierto es que antes de que se comenzase a recopilar datos con los nuevos dispositivos inteligentes, muchas compañías ya se las apañaban para averiguar todo acerca de la vida de sus usuarios. Por este motivo **no es correcto pensar que si no utilizas dispositivos inteligentes no correrás el riesgo** de que se sepa de ti. Para ejemplificar este hecho voy a hacer referencia al caso real que vivió el político alemán Malte Spitz, cuando en 2009 preocupado por no saber qué información almacenaba su compañía de teléfono, exigió legalmente que le cediesen todos los datos que tenían almacenado sobre él. Tras varias demandas interpuestas a la compañía ante la negativa de cederle los datos, el juez le dio la razón a Spitz y la compañía se vio obligada a darle las 35.830 líneas de código referentes a los 6 últimos meses de Spitz como cliente de la operadora.

Spitz, decidido a descubrir que significaban todas esas líneas de código, se las entregó a una empresa que pudiese sacar algo en claro de esa maraña de datos. Poco tiempo después, con dichos datos, la empresa consiguió crear un mapa en el que **podía verse al detalle todos los movimientos del político** durante esos 6 meses (mapa interactivo adjunto en la bibliografía). En el mapa podía observarse donde estaba su casa, a qué hora iba a trabajar, que rutas seguía para ir al trabajo, las llamadas que realizaba, a quien las realizaba, la duración de las mismas, etc. Sin la necesidad de tener nuestro teléfono conectado a internet, solo con el uso de las antenas telefónicas por parte de nuestro móvil, las teleoperadoras **también pueden conocer dónde y sobre todo cómo vivimos**. Si ampliamos un poco la vista podremos darnos cuenta de que además saben a quién llamamos, por lo que saben con quién nos relacionamos. De esta forma y teniendo en cuenta que también almacenan datos del resto de usuarios **las compañías crean una red de vínculos y datos** que puede llegar a resultar alarmante.

A día de hoy, Malte Spitz, sigue su guerra contra este poder de las compañías para recoger datos y se dedica a dar conferencias por todo el mundo dando a conocer su caso. Su objetivo no es dejar de usar la tecnología, si no instar a los usuarios a ser conscientes del peligro y concienciar de que todo usuario debería de poder tener derecho a la autodeterminación sobre sus datos.

Presente y futuro próximo del tratamiento de datos

¿Conocemos realmente la magnitud del tratamiento de datos que existe en la actualidad? Cabe destacar que según las previsiones de estima que para el año 2020, los dispositivos del *Internet de las Cosas* triplicarán a la población mundial, lo que **supone más de 21.000 millones de aparatos conectados** a la red. Todo ello sin contar aparatos como teléfonos móviles antiguos que a pesar de carecer de la esencia *IoT*, también pueden recopilar datos como hemos visto anteriormente. La magnitud de datos es tal, que ya han surgido ramas de la tecnología que se encargan de tratamiento inteligente de dichos datos.



Jorge Coronado nos explicó la técnica conocida como ***Doxing***, que consiste en la búsqueda de datos centrándose en un objetivo concreto (por ejemplo, una persona pérdida). Además, existen muchas otras técnicas, pero quizás la más conocida es la del *BigData*. El ***BigData*** consiste en **buscar inteligentemente y de forma automatizada entre miles de millones de bytes** de información encontrando relaciones que puedan resultar interesantes para cualquier fin. Aunque parezca casi de ciencia ficción el *BigData* ya se está utilizando para diversos fines. Un ejemplo muy sonado fue el ocurrido en las pasadas elecciones de los Estados Unidos por parte del partido republicano, en el que varias empresas expertas en el área fueron contratadas para encontrar a personas que fueran partidarias de las ideas del ahora presidente Trump. Tras analizar millones de datos, encontraron que la audiencia de la serie *The Walking Dead* era más propensa a estar en contra de la inmigración. O los espectadores de *NCIS* eran

partidarios de eliminar el *ObamaCare.* De esta manera incluyeron anuncios de alto impacto en las pausas publicitarias de estos programas televisivos con el fin de aumentar el número de votantes.

Conclusión

Todo el desarrollo de este trabajo da a entender que el mundo tecnológico, y en concreto el sector de *Internet de las Cosas*, avanza a pasos agigantados. Fruto de este avance surgen nuevos peligros, pero eso no quiere decir que debamos abandonar el uso de la tecnología. Como dice Chema Alonso, ***"El problema no es ceder datos, es saber a quién se le ceden, y si merece la pena por el servicio que te ofrecen."*** Pero como bien es sabido**, el conocimiento es poder** y los datos que generamos tienen mucho valor.

Bibliografía

Internet de las cosas, Wikipedia, 1 de diciembre de 2017. Disponible en: https://es.wikipedia.org/wiki/Internet_de_las_cosas

Así es como venden las grandes empresas tus datos personales, El Confidencial, 14 de septiembre de 2015. Disponible en: https://www.elconfidencial.com/tecnologia/2015-09-14/asi-es-como-venden-tus-datos-personales-en-internet_1011071/

Tu compañía telefónica te está mirando, TED Global, junio de 2012. Disponible en: https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=es

Mapa interactivo de las ubicaciones de Malte Spitz, Zeit, 2011. Disponible en: http://www.zeit.de/datenschutz/malte-spitz-data-retention

Información acerca del doxing, Pabloyglesias, 5 de noviembre de 2015. Disponible en: https://www.pabloyglesias.com/mundohacker-el-doxing/

BigData, Wikipedia, 22 de noviembre de 2017. Disponible en: https://es.wikipedia.org/wiki/Big_data

Así ayudó "The walking dead" a Donald Trump a ganar las elecciones, 24 de noviembre de 2016. Disponible en: http://www.lavanguardia.com/internacional/20161124/412135674496/walking-dead-ayudo-trump-ganar-elecciones.html