Facultad de Ciencias Económicas y Empresariales

EL POTENCIAL DE MEJORA DEL BIG DATA

Estudio de la Ética en el uso del Big Data.

Autor: José Juan González Martínez
Tutor: Raúl González Fabre

MADRID | Abril y 2022

RESUMEN

El Big Data es una herramienta que ha revolucionado el mundo empresarial en los últimos años. Cada vez es mayor el número de compañías que usan esta herramienta a diario, y consecuentemente la demanda de especialistas en este sector también ha incrementado. Pero lo que pocos han planteado son todos los dilemas éticos que conlleva el uso de esta tecnología. Ya hemos ido presenciando varios incidentes producidos por el Big Data en los últimos años, y seguramente vayamos a seguir viendo más en un futuro próximo. La legislación al respecto aborda de manera extensa ciertas materias, y apenas se preocupa por regular los graves problemas que estamos enfrentando. En el siguiente trabajo abordaremos la ética en el uso del Big Data y la regulación legal al respecto, contrastando la investigación con una serie de entrevistas a especialistas en el tema.

PALABRAS CLAVE

Big Data, ética, regulación legal del Big Data, protección de datos, recolección de datos, Inteligencia Artificial, código deontológico.

ABSTRACT

The Big Data is a tool that has revolutionized the business world in the recent years. The number of companies that use this tool on a daily basis is increasing, and consequently the demand of specialists in this sector has also increased. But what few have thought about are all the ethical dilemmas that the use of this technology entails. We have already been witnesses to several incidents caused by Big Data in recent years, and we will probably continue to see more in the near future. The legislation in this regard deals extensively with certain matters, and hardly cares about regulating the serious problems that we are facing. In the following work we will address the ethics in the use of Big Data, and the legal regulation in this regard, contrasting the investigation with a series of interviews with specialists on the subject.

KEYWORDS

Big Data, ethics, legal regulation of Big Data, data protection, data collection, artificial intelligence, code of ethics.

LISTADO DE ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
CE	Comisión Europea
IA	Inteligencia Artificial
UE	Unión Europea

ÍNDICE

I. INTRODUCCIÓN

1.1 Objetivos

En las últimas décadas, ha habido un crecimiento exponencial del uso de las nuevas tecnologías digitales en las empresas. Dicho crecimiento ha traído consigo una revolución en la vida empresarial, la cual ha creado una nueva concepción de trabajo.

Entre todos los avances que han ido surgiendo, uno de los más notables es el Big Data. Esta herramienta de trabajo la podríamos definir como el conjunto de tecnologías específicas para el análisis de datos, entre las que destacan el Business Intelligence y el Data Mining, y que sirve para estructurar y ordenar grandes volúmenes de datos, con la mayor brevedad posible. El Big Data ofrece una gran cantidad de posibilidades, las cuales han provocado una revolución en todo tipo de ámbitos como el empresarial, el financiero, o incluso el sanitario. Esta tecnología destinada al procesamiento y análisis de datos, ha facilitado la toma de decisiones, a la vez que nos brinda una serie de ventajas competitivas, que hace apenas unos años, eran inimaginables (Blázquez, 2021).

Las ventajas del Big Data están basadas en el potencial de procesamiento de información. El aprovechamiento de esta herramienta supone una gran mejora en la toma de decisiones y ofrece la posibilidad de recibir datos en tiempo real para un mejor conocimiento del mercado.

El enfoque que se quiso dar a este trabajo fue dirigido a estudiar las diferentes problemáticas que tiene esta herramienta. El uso del Big Data conlleva una serie de inconvenientes, siendo el más destacable la discriminación y marginación de datos y perfiles por parte de algoritmos, no solo porque todavía no sabemos cómo evitarlo y solucionarlo, sino además por la insignificante regulación que existe sobre el tema (Hernández, Polanco Medina, 2020). A medida que crece el uso de esta herramienta, crece el debate sobre la ética en la discriminación empresarial de datos.

El análisis de datos, usando Big Data, puede llevar a las compañías a enfocarse en los grupos que los algoritmos consideren más rentables. Por esta misma razón, la misma herramienta puede llegar a considerar que es mejor no prestar un crédito a una persona, por la simple razón de ser mujer, negro, soltero, por vivir en una ciudad de baja densidad de población, o incluso porque un análisis estadístico así lo ordena. Si un banco decidiese denegar un crédito por una de estas razones, el escándalo sería enorme, pero si la

discriminación es producida por un algoritmo, que simplemente analiza los datos, no habría nadie a quien recriminar una actitud discriminatoria (Nieto, 2016).

Ya tenemos una buena regulación y sabemos cómo manejar situaciones de discriminación por prejuicios de individuos, pero el gran riesgo que estamos afrontando, es que nunca hemos luchado contra una discriminación que nace de los criterios de un algoritmo. Como sociedad, somos capaces de poner en duda lo que diga cualquier persona, pero confiamos en exceso en lo que nos dice un algoritmo, como si las máquinas no pudiesen fallar. Un claro ejemplo de ello podría ser el caso Google. En 2008, Google lanzó un algoritmo que predecía las epidemias de gripe, utilizando las búsquedas de sus usuarios. Esta solución fue medianamente útil los primeros tres años, hasta que en la campaña de 2011/12 sobrestimó en más del cincuenta por ciento el número de visitas al hospital, pudiendo haber causado un caos absoluto, si no se hubiese frenado su uso antes de otro fallo de ese nivel. (Intxusta, 2020).

Otro ejemplo evidente de la discriminación de datos, es el caso del algoritmo *COMPAS*. Esta herramienta es utilizada en los tribunales de Wisconsin, para aconsejar a los jueces la duración que debería tener una pena, basándose en las características y situación del preso. Esta herramienta funciona de manera simple, pues calcula la probabilidad de que una persona vaya a cometer otro crimen, en función de su historial, una encuesta que realizan los condenados y las características personales de estos. Pero en ese perfil que se crea de cada reo, se tiene en cuenta el género, la edad, la raza o incluso la religión. (González, 2016). La polémica surgió cuando se dieron cuenta de las discriminaciones injustificadas que estaba llevando a cabo, como puede ser el ejemplo de la agencia de noticias ProPublica, que en marzo de 2016 publicó un análisis sobre el uso de este algoritmo en el condado de Florida, y se dieron cuenta de que las personas de raza negra tenían el doble de posibilidades de ser consideradas por la máquina, como personas de alto riesgo. (Larson, Mattu, Kirchner and Angwin, 2016) Aquí podemos contemplar otro ejemplo de discriminación debida al uso de datos sesgados.

Con este proyecto se busca dar a conocer el mundo del Big Data, todos los riesgos que esta herramienta conlleva, las medidas preventivas y la regulación legal al respecto. Al mismo tiempo se lleva a cabo una investigación de cómo se gestionan los datos y el Big Data en las empresas, a través de una serie de entrevistas anónimas a un grupo de expertos sobre el tema. Con esto se trata de llevar a cabo una investigación práctica, para demostrar la grave y creciente preocupación que existe

en el mundo empresarial sobre la gestión y el uso de datos y perfiles, desde la llegada del Big Data, y la urgente necesidad de crear herramientas para la prevención de riesgos.

1.2 Metodología

La metodología que se utilizó para el trabajo fin de grado se puede dividir en dos partes. En la primera parte, a través de fuentes como Google Scholar, la biblioteca o los repositorios de la universidad, se recogió la información necesaria para la parte teórica del trabajo. La primera parte del trabajo aborda la investigación y estudio del Big Data, la gestión ética del uso de datos en las empresas y la regulación legal sobre la discriminación de datos.

Y la segunda parte del trabajo, que consiste en la parte analítica del proyecto, busca demostrar el creciente riesgo que existe en él uso de datos, basándose en una serie de entrevistas a varios expertos en Big Data. Para evitar sesgos de información, que pueden producirse cuando se habla con miembros de cualquier compañía, todas las entrevistas fueron anónimas, con el único fin de que los entrevistados fuesen honestos a la hora de responder.

Por último, en las conclusiones se llevó a cabo una comparación entre la investigación que se hizo en la primera parte, y las entrevistas con expertos, con el fin de contrastar la información.

1.3. Estructura

La estructura que se siguió en este proyecto se divide en dos partes. La primera parte es la teórica, que a su vez de divide en tres capítulos, empezando con un estudio del origen, evolución y perspectiva de futuro del Big Data, para entender cómo funciona está herramienta, y el potencial de uso y los riesgos que atañe. Después de dicho estudio, se continuó con un enfoque de la ética y la responsabilidad social por parte de las compañías a la hora de recoger y gestionar los datos; y el último capítulo aborda la regulación legal que existe sobre el uso del Big Data, que lagunas existen, y que propuestas hay al respecto.

La segunda parte consistió en una investigación empírica, que se basó en analizar las entrevistas con los expertos en Big Data, para entender en profundidad la manera de gestión de las empresas, los perfiles de sus clientes y todos los datos que recogen a diario.

II. BIG DATA

2.1 El concepto del Big Data

Es complicado encontrar una definición adecuada del Big Data, debido a que muchas técnicas usadas de base o apoyo para las bases de datos masivos eran conocidas como “Data Mining”. Cuando usamos el término de Big Data, nos referimos a la construcción, utilización y organización de cantidades inmensas de información para obtener y entablar relaciones nuevas para aumentar el valor de mercados, organizaciones, etc. (Giner, 2018).

Pero esta descripción del Big Data se queda escueta, sabiendo el gran potencial que posee. Para empezar, cuando se habla de Big Data, lo primero que se piensa es en grandes cantidades de datos. En segundo lugar, lo que implica este concepto es la agregación de datos provenientes de diversas fuentes, dotando de gran relevancia los procesos de gestión y fusión de información. Esta información se caracteriza, no solo de la diversidad de fuentes de la que se obtiene, sino además por la falta de estructuración. Y, por último, la tercera idea que se plantea cuando se nombra al Big Data es el objetivo que tiene, que no es el de descubrir causalidades sino desarrollar modelos predictivos a tiempo real. En el Big Data es clave la correlación de datos actualizados al instante. Esta herramienta ha producido un cambio de mentalidad, al crear la posibilidad de analizar una cantidad ingente de información, sin necesidad de limitarnos a una muestra, en cuestión de segundos (Gil, 2015).

Por lo tanto, el concepto de Big Data hace referencia a un proceso que podemos repartir en tres partes, y que incluye conceptos de matemáticas, estadística, e informática. La primera es el procedimiento de captura y manipulación de información. Para este cometido es necesario el uso de procesos en paralelo y programas específicos para reducir dimensiones. La segunda parte del proceso implica el análisis de datos para hallar relaciones predictivas que sean útiles, usando herramientas de estadística y de Machine Learning, conceptos que pueden llegar a confundirse pero que se encargan de tareas diferentes. La estadística se aplica imponiendo un modelo para captar el origen de la relación entre los inputs y los outputs; mientras tanto el Machine Learning busca encontrar la función que, en base a los inputs, permita predecir un resultado sin la necesidad de utilizar ningún modelo sobre dicha relación. Y la última parte del proceso

concluye con el uso de técnicas de visualización con el fin de obtener los resultados y comunicarlos a los usuarios finales (Gil, 2015).

2.2 El Big Data en la actualidad

Hay que empezar remarcando la relevancia que tiene el Big Data a nivel mundial, no solo por los retos que implica, sino además por los efectos intangibles que están transformando nuestro estilo de vida en todos los aspectos. Podríamos destacar tres grandes puntos, correlacionados entre ellos, en donde el Big Data ha revolucionado nuestro estilo de vida.

2.2.1 El Big Data y el New Data

En 2018 se estimó que cada día se crean más de 2,5 quintillones de bytes de datos, y cada persona de la Tierra crea por segundo una media de 1,7MB de datos. Obviamente, esto genera una cantidad de información que un sistema tradicional es incapaz de procesar, hasta el punto de que antes de la llegada del Big Data, gran parte de esta información se desperdiciaba, e incluso se desconocía. La gran mayoría de datos que obtenemos a través del Big Data tienen un contenido nuevo. (Landi, 2022).

Como ejemplo, en el comercio electrónico hemos pasado de recoger datos transaccionales a capturar los flujos de clics, estudiando la ruta que realiza el cliente antes de finalizar su compra o abandonar el carrito. Estos datos contienen la información tangible del consumidor, como la información que consultó durante su compra, pudiendo poner de ejemplo desde que colores y estilos busca, hasta la sensación que tuvo con el producto, el trato recibido o la información que se consultó durante el proceso (Landi, 2022). El análisis del flujo de clics nos ha permitido conocer de mejor manera al cliente, y los procesos de compra o consumo del ser humano, para ir adaptando cualquier servicio electrónico a nuestros gustos y necesidades. (Sánchez, 2020).

2.2.2 El Big Data y el Unlocking Value

Otra gran aportación del Big Data la podemos apreciar a través del análisis automático que es capaz de hacer. Ha desarrollado una capacidad para poder recoger cantidades inmensas de datos y transformarlos en nueva información, la cual se lleva para la toma de decisiones inteligentes, y poder así analizar todos esos datos y descubrir el valor que encierran. El Business Inteligencie es capaz de buscar entre todo el historial de transacciones de cualquier compañía, con el fin de modelar tendencias, proporcionar

nuevas estadísticas del rendimiento de un sistema o generar nuevos informes. El Big Data, aparte de ampliar la cantidad de datos disponibles para el Business Intelligence, también incrementa el nivel de complejidad para ampliar las fronteras de los análisis. (Sánchez, 2020).

Por ejemplo, cuando un usuario realiza una búsqueda o hace una pregunta en internet o en una base de datos, y el ordenador automáticamente le da una respuesta, el Big Data puede ir un paso más allá a través de las distintas búsquedas y preguntas que ha realizado el usuario, hasta llegar a enviarle sugerencias de búsquedas, que posiblemente se le hubiesen acabado ocurriendo al usuario, adelantándose a su propio pensamiento. (Moreno, 2016).

2.2.3 El Big Data y Shaping The Future

Tradicionalmente, el Business Intelligence realizaba analíticas de los historiales, para aprender del pasado y así mejorar la eficiencia en el futuro, pero era trabajo de un especialista el tener que estructurar, procesar y almacenar todos esos datos, antes de conseguir la predicción que se buscaba. En este proceso de estructurar y almacenar información podían suceder cientos de acontecimientos que cambiaban por completo el panorama, e invalidaba dichas predicciones, haciendo que el trabajo perdiese toda su efectividad. Gracias a los nuevos análisis predictivos, esta herramienta es capaz de capturar y procesar grandes cantidades de información en tiempo real, independientemente de que estén o no estructurados los datos. Con ello podemos realizar análisis predictivos que nos responden a preguntas como qué va a suceder en un futuro cercano, qué ocurriría si cierta tendencia se mantuviera en el tiempo, o porqué ocurre un acontecimiento y cómo poder cambiarlo (ayudaley, 2020).

Los análisis predictivos permiten influir y modelar el futuro, evitando que acontezcan ciertos hechos, y de esta manera poder cambiar el rumbo de cualquier estrategia. También nos permiten prever futuras tendencias y preferencias de clientes, y darles recomendaciones. Un claro ejemplo de esto sería la página web de venta de libros de Amazon. La importancia de esto no solo viene de la capacidad de conocer el hecho, sino también entender los pensamientos y comportamientos de cada persona, a niveles muy profundos, en tiempo real. Los análisis de Big Data cada vez se están volviendo más predictivos, y con mayor nivel de exactitud, convirtiéndose en una herramienta

indispensable para sobrevivir en el mercado actual, y transformando realmente la forma en que trabajamos y vivimos. (BBVA, 2021).

2.3 Próximos avances del Big Data

2.3.1 Tendencias futuras

Entre las primeras tendencias que se prevén este campo, estaría el *dark data* (datos oscuros), o *dusty data* (datos polvorientos). Estos son datos de origen no digital, o descartados por su falta de valor. La evolución de esta herramienta ha dado a pensar que estos datos descartados en un pasado, van a llegar a ser un gran activo en el futuro, cuando se desarrollen las herramientas necesarias para su estudio (Redacción España, 2019)

También hay que valorar que, a causa de la irrupción de las nuevas tecnologías en la sociedad, las IoT o "el internet de las cosas" (que se refiere a una interconexión digital de internet con objetos cotidianos) se han introducido en nuestra vida cotidiana. Como ejemplo se podría pensar en los relojes inteligentes o vehículos autónomos, capaces de recopilar datos de forma masiva. Estas herramientas que utilizamos a diario han ido creando un entorno ideal para nutrir el Big Data (Herrero, 2018).

El Big Data también está empezando a introducirse en nuevos campos, destacando la gran repercusión que está teniendo en el mundo de la salud. Este sector genera grandes cantidades de datos por paciente. Antiguamente los médicos utilizaban sus conocimientos y experiencia para decidir sobre los tratamientos que se debían aplicar a cada situación, y gracias al Big Data, estas decisiones están cambiando de manera radical, pasando a tomar las decisiones en base a los datos de millones de pacientes, compartiendo su experiencia a niveles mucho más altos que lo que tradicionalmente eran capaces de hacer. (Economía 3, 2021).

Un claro ejemplo de esto sería el Smart Visual Data, un software con el cual las empresas, a través de videowalls colocados en lugares estratégicos, pueden ver su actividad en tiempo real, para que así llegue la información a todo el equipo, no solo permitiéndoles estar informados en todo momento de la situación, sino además motivándoles y haciendo les sentir parte del proyecto. Este nuevo sistema de gestión está revolucionado el mundo del análisis de datos, pues permite el acceso a información a

cualquier trabajador, permitiendo a toda la plantilla de empleados participar en la toma de decisiones de la compañía (Fernández, 2017).

Otro ejemplo claro serían las Smart Cities. Con el propósito de crear y desarrollar ciudades sostenibles social, económica y medioambientalmente, se ha creado este proyecto, en donde las nuevas tecnologías son utilizadas para fomentar un desarrollo sostenible, mejorar la calidad de vida y la eficacia en el uso de los recursos disponibles, reducir la contaminación y facilitar la participación ciudadana. En estos proyectos, el uso del Big Data está siendo esencial, pues es la herramienta base para gestionar el comportamiento, los hábitos y la movilidad de los ciudadanos, y en base a ellos poder llevar a cabo todos los propósitos planteados. Con esto creo que queda demostrado el increíble potencial de esta herramienta. (Martín, 2021).

2.3.2 Futuros desafíos

También es necesario hablar de los tres desafíos más llamativos que va a tener que afrontar la tecnología actual, para poder avanzar en el mundo del Big Data:

a) **El primer gran obstáculo, el volumen:** ya hemos comentado la gran cantidad de datos que se generan a diario, y como la capacidad de recoger estos datos también ha aumentado, pero no al mismo ritmo. Esto ha producido que las compañías empiecen a tener inconvenientes para poder almacenar todo ese volumen de información. Además, también se deberá afrontar el problema de estructuración de grandes cantidades de datos, que agravará dicha situación en mayor medida (Sierra, 2019).

b) **El segundo gran problema, la falta de personal cualificado**: para utilizar estas herramientas se requiere que previamente se dé una formación técnica, complicada de encontrar en el mercado laboral. En el 2020, la demanda de personal cualificado para poder trabajar con Big Data aumentó en un 128%, mientras que solo hubo un 68% de crecimiento en el número de profesionales de este campo. A pesar de nuevos avances, como el Smart Visual Data, la velocidad con la que avanza el Big Data, supera con creces la velocidad que tenemos de aprendizaje y adaptación. (Accenture, 2021).

c) **Y el último gran problema, la seguridad**: en el contexto actual, las amenazas contra la privacidad, la seguridad de los datos de usuarios, y el aseguramiento de estas debe ser clave para las compañías, sobre todo por la gran cantidad de datos que manejan desde la entrada del Big Data, y el gran peligro que existe en que se comercie con ellos de manera inadecuada (Martín, 2018).

En conclusión, el Big Data se ha introducido en nuestra sociedad para quedarse por un largo periodo de tiempo. Y por lo tanto podemos sacar dos conclusiones, que vamos a tener que aprender a convivir con él Big Data en nuestro día a día, y que necesitará una regulación para limitar sus actuaciones y proteger a los ciudadanos.

III. ÉTICA Y RESPONSABILIDAD SOCIAL EN EL USO DEL BIG DATA

3.1 Razones para preocuparse por el uso del Big Data

El Big Data ha conseguido introducirse en casi todos los ámbitos de la sociedad, y es cuestión de tiempo que acabe estando en todos. Su uso nos permite desde valorar el conceder o no la libertad condicional, calcular una pena en un tribunal o hacer investigaciones médicas, hasta estudiar las preferencias de un cliente o decidir qué tipo de ofertas proponerle. A pesar de que actualmente las máquinas continúan sin tener una inteligencia generalista, no significa que debamos ignorar su gran potencial; una cifra insignificante de algoritmos es capaz de desarrollar suficiente inteligencia para tareas increíblemente específicas y concretas, y desarrollarlas a niveles inalcanzables para el trabajador medio (Eureka Marketing, 2021).

Toda esa colección de datos e información está disputada entre grandes gigantes como Facebook, Microsoft, IBM, Google o Amazon, hasta el punto de que llegan a primar sus intereses comerciales por encima de ninguna consideración ética. Esto ha empezado a producir un descontento entre los usuarios, que ha empujado a muchas firmas a crear comités éticos, sobre todo enfocados hacía la privacidad de los datos de los usuarios y hacía el uso sin autorización ni la debida supervisión de algunas aplicaciones. (Eureka Marketing, 2021).

El problema de la ética del Big Data es que está en una fase incipiente de desarrollo, y no está lo suficientemente preparada para afrontar la llamada “dictadura de los algoritmos”, en donde encontramos perpetuadas injusticias sociales por un algoritmo

matemático, y como este es resultado de una máquina y no de una persona, no se considera discriminatorio, ilegal, ni injusto. Por ejemplo, un algoritmo puede llegar a micro segmentar a la población, lo que puede conducir a que se limite la libertad de los individuos. Esto podría llegar a perjudicar hasta el punto de que, cuando una persona es clasificada en un grupo de clase media, automáticamente el algoritmo solo le mandará ofertas de trabajo de bajo nivel, pisos en venta de barrios marginales, reduciendo las posibilidades de ascender de clase social, propuestas de formación para puestos bajos y limitándole su libertad de cambiar de estilo de vida. Y este es uno de los muchos ejemplos que se podría poner para mostrar las diferentes maneras de las que puede llegar a afectar el Big Data y la IA, si no son controlados, y no nos aseguramos que sus procesos sean transparentes (Hernando, 2019).

3.2 Valoración ética en la recopilación y gestión de datos

3.2.1 ¿La recopilación de datos está legitimada por la gratuidad del servicio?

La recopilación de datos es un proceso sumamente fácil, con un coste muy bajo o incluso nulo. Los métodos de recopilación son variados, pero los más habituales son el uso de información pública o la recolección de datos personales a través del consentimiento del usuario. Este último método es muy simple, y consiste en ofrecer al cliente un servicio que al principio parece gratuito, pero que realmente está dándole el servicio a cambio de su consentimiento, para recolectar y tratar sus datos con fines lucrativos (Tablado, 2021).

El uso de cualquier servicio digital supone ceder información, y consecuentemente permitimos que una empresa acceda a nuestros datos privados, pudiendo comprometer nuestros derechos. Un ejemplo podría ser cualquier búsqueda realizada con Google, pues es considerado un servicio gratuito, pero que, en realidad, como método de pago le cedemos nuestros datos con nuestro historial de búsqueda, para que así pueda crear perfiles y parámetros en función de nuestra actividad, que serán utilizados por Google de forma comercial para conseguir beneficios a través de transferir a terceros esa información. Los ejemplos de supuestos negocios que ofrecen servicios gratuitos, que contratamos con un simple clic, y que realmente nos están cobrando con toda nuestra información privada, son innumerables, como por ejemplo las redes sociales. Las redes sociales, que en un principio parecen gratuitas, nos cobran accediendo a

nuestros datos personales, tras aceptar los términos de uso cuando crearnos un perfil en dicha página (Tablado, 2021).

Lo peor de estas prácticas no es el robo de los datos, sino la doble exposición a la que nos vemos expuestos, primero por la cesión de datos que damos a la compañía que nos ha dado a entender que es gratuita, y una segunda vez por la compañía que compre los datos para lucrarse. La información es uno de los activos más atractivos y demandados por las compañías a día de hoy (Fernández-Lasquetty Quintana, 2020) y, por ello, se están empezando a desarrollar distintos reglamentos para protegerla. No obstante, a pesar de ello, la sociedad sigue sin preocuparse por las políticas de privacidad y los riesgos derivados de la cesión de datos, lo que supone un problema adicional. Este problema no atenta contra el ordenamiento jurídico vigente (tema que abordaremos más adelante), sino contra el orden moral.

Para que el consentimiento para la cesión y tratamiento de datos sea válido, ha de cumplir los requisitos de libertad, información y especificidad. Por desgracia las empresas, en vez de entender qué estos requisitos están motivados en base al respeto a la dignidad y la intimidad de sus usuarios, buscan maneras de eludir la ética, sin infringir a la ley. La intencionalidad detrás de estas actuaciones no es otra que el aprovechamiento de la situación vulnerable de los usuarios y la maximización de los beneficios, demostrando la falta de moral en sus actuaciones (datos.gob.es, 2017). Un ejemplo sería la sanción impuesta a Facebook y a WhatsApp en 2014 por procesar datos que no estaban autorizados, bajo la excusa de que sus usuarios aceptaron unos términos excesivamente generales. La Agencia Española de Protección de Datos les sancionó con una multa de 600.000€ (Masterlegal, 2020).

Tras este análisis, concluimos que se debería investigar en más profundidad, por parte de las autoridades competentes, si los términos y condiciones de uso que aceptamos a diario, a pesar de estar dentro de la legalidad vigente, realmente lo están dentro del sentido deontológico y ético que el legislador tenía cuando promulgó dichas normas. El problema central de este punto se encuentra en que los términos de uso que aceptamos a diario se redactan de manera larga y enrevesada, con un lenguaje excesivamente técnico para el usuario medio pero valido ante tribunales. Como resultado, se aceptan sin leer y otorgan a la empresa el derecho a usarlos, sin que el cliente pueda llegar realmente a saber para que se usarán. No es una cuestión legal, sino que está dirigida a cuestionar si

realmente esta legislación garantiza que las empresas no lleven a cabo actuaciones inmorales con el fin de obtener beneficio.

3.2.2 El derecho al Olvido

El derecho al olvido es el derecho de cada persona que haya cedido sus datos personales, a que el cesionario elimine o modifique ciertos datos que incumban al cedente, si este así lo exige. En relación con este derecho encontramos la sentencia del Tribunal de Justicia de la Unión Europea (en adelante UE) sobre el caso Google (STJUE C-131/12, 13 de mayo de 2014), en donde se defendió que aquel que cediese información relativa a su persona y a su vida íntima, no apareciera vinculado a dicha información en ninguna búsqueda. Esto se consiguió gracias a la Carta de Derechos Fundamentales de la UE, pues en sus artículos 7 y 8 se estableció el derecho a la protección de la vida familiar y los datos personales, que fue la base para el fallo de dicha sentencia (Carta de Derechos Fundamentales de la Unión Europa. 2000/C 364/01). En el tema legal entraremos más adelante, pero por ahora solo se planteará en qué principios éticos se basaron para legislar este derecho.

Siguiendo el punto anterior, estamos ante una garantía que debería verse reforzada, debido a la realidad que estamos viviendo, donde a diario se procesan millones de datos de manera indiscriminada. En el caso Google, se demostró que un motor de búsqueda manejó datos sin ningún tipo de precaución, obligando a miles de usuarios a exigir que se borrase su información, porque sin saberlo habían cedido información de toda índole (sanciones disciplinarias, datos relativos de violencia de género, etc.) que se asoció a sus perfiles, y llegó incluso a perjudicarles en su vida diaria (Llamas, 2014).

Esta herramienta se ha de regular de manera que se garantice su uso y disponibilidad para el usuario en todo momento, para evitar el mayor número de abusos y vulneraciones por parte de las compañías. Estamos ante el peligro de permitir a las empresas jugar con la imagen de los usuarios, como si su información personal fuese un activo empresarial, cuando en realidad están negociando con la compilación de todos los acontecimientos de la vida de un ser humano. Se ha de garantizar que las empresas protejan la intimidad y la dignidad de sus clientes y usuarios, y no tratando les como cifras, sino como personas.

Los datos no son estáticos, al igual que tampoco lo son los usuarios, y por lo tanto cualquier individuo ha de estar en su derecho de rectificar la información publicada a lo

largo de su vida, o de lo contrario podríamos ver ataques al honor y la dignidad del usuario. Por eso mismo, cualquier ordenamiento jurídico de la UE debe contemplar esta posibilidad, procurando proveer del mayor número de herramientas para la protección de datos de cada usuario (Noain Sánchez, 2016).

3.2.3 El uso de algoritmos e Inteligencia Artificial para tratar los datos

Uno de los problemas que más preocupa a nivel legal sobre el uso del Big Data, es la discriminación de datos realizada por los algoritmos. Se supone que la tecnología nos permitía eludir los típicos errores humanos, permitiéndonos obtener soluciones correctas y rápidas. Debido a esta opinión generalizada, hemos dejado al Big Data la responsabilidad de tomar decisiones trascendentales, cuando sabemos que se ve influenciado por intereses humanos plasmados en los algoritmos que se usan a diario. Los parámetros creados para la toma de decisiones de cualquier herramienta han sido creados por una persona, y por lo tanto vienen marcados por sus intereses y prejuicios (González, s. f.).

La Inteligencia Artificial y el Big Data se alimentan de esas decisiones humanas y se emplean para poder utilizar un mecanismo de análisis y respuesta para dar resultados rápidos, pero no siempre justos. Dos de los campos donde más polémicas ha habido tras la irrupción de la tecnología, han sido el de los recursos humanos y el del derecho. Estos campos jamás se han entendido como una disciplina matemática, sino que, al contrario, se basaban en el casuismo, y el entendimiento del contexto especifico antes de dar una respuesta. Y a continuación se expondrán los dos ejemplos:

a. El uso de la Inteligencia Artificial para contratar y despedir

Hace tiempo que se implantó en varias empresas el uso de la IA para estudiar si un trabajador era productivo o no, y con las respuestas que se obtenían se llegaba a la conclusión de que para aumentar el rendimiento empresarial se debían llevar a cabo varios despidos. Fue famoso el caso publicado por la revista The Verge, en que Amazon despidió a decenas de trabajadores debido a la falta de productividad. Esta conclusión se obtuvo tras recopilar y tratar cientos de datos de sus trabajadores, y despidiendo a los que hubieran tenido más bajo nivel de productividad en el último año. Estos despidos no pasaban por ningún supervisor ni encargado, dejándolos totalmente a la elección del algoritmo, el cual no tenía en cuenta la situación personal del trabajador, o su potencial de mejora (Pérez, 2019).

Pese a este riesgo, es cada vez más habitual el uso de esta tecnología a la hora de llevar a cabo decisiones laborales de este nivel, pretendiendo dejar de lado los prejuicios y la imparcialidad. Pero el uso de algoritmos e IA producen una falsa idea de neutralidad ya que, por ser una elección producida por una máquina, parece que no existe ningún prejuicio humano. Pero nada más lejos de la verdad, pues al ser creados por humanos, los prejuicios de estos acaban dejando huella en sus creaciones (Pérez, 2019). Un ejemplo es como un algoritmo puede descartar a mujeres casadas, por su mayor probabilidad de pedir una baja de maternidad, y por ende representan una menor productividad, lo que deriva en un comportamiento machista y discriminatorio (Echarri, 2021).

En el ámbito laboral, debería estar regulado que la toma de decisiones de una máquina a estar supervisada en todo momento por un encargado, o un comité, para evitar discriminaciones injustificadas u olvidar tomar en cuenta información personal relevante. (Echarri, 2021).

b. La función judicial y la Inteligencia Artificial

No solo el ámbito laboral, sino que la función judicial también ha caído en el avance del Big Data y la IA. Como ya hemos comentado, en algunos países como Estados Unidos, se ha empezado a introducir el uso de estas tecnologías en algunos procesos y fases judiciales, destacando el uso para la predicción de resultados de litigios. En España también se ha empezado a desarrollar un software de predicción llamado *Legal Data* desarrollado por la empresa española Legal Innovation, que puede elaborar, a través del análisis jurisprudencial de miles de sentencias, el resultado de un litigio futuro, e incluso el tiempo aproximado para una resolución (Europa Press, 2017).

Este tipo de herramientas son de gran utilidad para que los abogados puedan preparar mejor sus juicios y plantear a sus clientes las diferentes posibilidades del litigio, e incluso ayudar a los Tribunales a la hora de tomar decisiones en juicios de menor relevancia, para reducir la acumulación de asuntos en la justicia española. Un ejemplo es el uso del *e-descovery* en los tribunales de Estados Unidos. Esta herramienta usa el Big Data y la IA para recopilar información relevante de sentencias pasadas, analizarlas, y obtener conclusiones, para facilitar el manejo de pruebas en los litigios. (Byte Ti, 2017).

Además, en Estados Unidos también se emplean ciertos instrumentos relacionados con el Big Data, en relación con el C*riminal Rating* para elaborar perfiles y estadísticas criminales, basándose en sentencias de otros litigios. Un ejemplo sería el

programa *COMPAS,* utilizado para analizar los perfiles criminales. Este programa funciona calculando la posibilidad de reincidencia, y en base al resultado, facilitar la toma de decisiones judiciales (BBC News Mundo, 2016).

Pero el problema surge cuando las conclusiones para la sentencia son tomadas por predicciones que plantean inconvenientes a la hora de justificar la decisión ante un posible recurso. Además, otro problema que surge debido al uso de estas herramientas es que se ha demostrado que este sistema no garantiza la imparcialidad, pues se basa en información que puede estar sesgada, anulando así su objetividad. Uno de los casos más relevantes sobre este asunto, fue el de State vs Loomis (State vs Loomis, 2016). En este caso, el Tribunal Supremo de Wisconsin rechazó el recurso, y el acusado fue condenado en base al criterio que aplicó el sistema C*OMPAS,* y por ello pidió tener acceso al algoritmo empleado. El Sr. Loomis apeló hasta la Corte Suprema de Wisconsin, pues consideró que el uso de dicho software violaba su derecho a un debido proceso, pues le impedían comprobar y demostrar la precisión de la herramienta y su validez científica, a la vez que se vulneraba el derecho de no ser discriminado, por haberse tenido en cuenta su género y raza a la hora de determinar la sentencia. (Moreno, 2021).

Por otro lado, la UE ya se está preparando, y en la Comisión Europea para la Eficiencia de la Justicia ya se ha adoptado la Carta Europea para el uso ético de IA dentro de los tribunales, (CEPEJ, 2018). En ella se destacan los principios que habrá que respetar, para garantizar el respeto a todas las garantías judiciales y asegurar un buen proceso, obligando a cumplir varios principios, como son el Principio de no discriminación, el Principio de respeto a los derechos fundamentales del ciudadano, el Principio del uso de la herramienta "bajo el control del usuario", el Principio de transparencia, igualdad e imparcialidad, y el Principio de calidad y seguridad (Grupo de prensa del Parlamento Europeo, 2021).

El derecho de defensa es una de las garantías en las que más riesgo existe con la irrupción del Big Data en los tribunales. Si alguien es acusado por un algoritmo, no puede tener una defensa adecuada, pues no es posible que conozca las circunstancias que se han tenido en cuenta, y en qué datos se han basado para la decisión. El uso de la IA y el Big Data no puede suponer la exclusión de una persona que valore la situación y los hechos al detalle. Si esto no se tiene en cuenta, se pondría en grave riesgo la independencia judicial y la seguridad jurídica, pues un sistema de litigios y sentencias basadas en algoritmos, supondría una misma aplicación del derecho a varias situaciones, cuando cada

una, debido a las circunstancias, debería ser valorada de manera totalmente diferente (Hernando, 2019).

3.2.4. Las condiciones generales

El aspecto de mayor relevancia en lo que se refiere a Big Data y el flujo de información se encuentra en la manera en la que se obtienen los datos. Lo más habitual es que las redes sociales y las compañías establezcan cláusulas de autorización para la recolección y procesamiento de datos, a través de "términos de uso" o "condiciones de uso". Cuando aceptamos estos contratos sobre las condiciones de privacidad de una página web, permitimos procesar nuestra información personal, el problema es que casi nadie llega a saber el alcance de dicha concesión (Noain Sánchez, 2016).

Lo más habitual es que las compañías recurran a contratos de adhesión, entendiendo estos como una modalidad contractual cuya principal característica es la unilateralidad del contenido, y la imposibilidad del adherente de cambiar las cláusulas. En esta situación, solo nos queda contemplar qué normativa podemos aplicar, que sería la regulación sobre defensa de los consumidores, contemplada en ciertos supuestos. Para ser más concretos, se está hablando del Real Decreto para la Defensa de los Consumidores y Usuarios (Real decreto legislativo 1/2007, relativo a la Defensa de los Consumidores y Usuarios, de 16 de noviembre). Este cuerpo normativo busca garantizar la protección de las relaciones de los empresarios con los consumidores y usuarios (Crespo Mora, 2021), sin embargo, las lagunas legales de esta ley y todas las normas que se han ido desarrollando en base a ella, son las que permiten a las empresas crear dichos contratos.

Sobre el punto anterior, la parte legal se analizará más adelante, pero lo que se quiere destacar es la falta de herramientas que posé el ciudadano para defender los derechos que la misma ley contempla. Es relevante el riesgo que conllevan las situaciones en donde las cláusulas de dichos contratos pueden llegar a incumplir los requisitos de transparencia y claridad. Cuando los individuos cedemos información sin conocimiento, ponemos en riesgo nuestra privacidad, pudiendo esto afectar incluso a nuestra intimidad y honor y a nuestra vida privada (Intxusta, 2020). En el caso Facebook encontramos un claro ejemplo de cómo una compañía recopilaba datos personales de la vida íntima de sus usuarios, gracias a contratos de adhesión legales, pero poco éticos, que supusieron un grave riesgo para los usuarios. El Real Decreto, que se acaba de mencionar en el párrafo anterior, y la normativa que se desarrolló en base a él, permiten varias lagunas legales en

donde las empresas se apoyan para generar estos contratos. Y por esto mismo es considerable la posibilidad de crear una regulación más estricta sobre la concienciación y transparencia, para que el Big Data no conlleve una inclusión de cláusulas no ajustadas a la normativa vigente, y que puedan llegar a vulnerar los derechos fundamentales de sus usuarios (BBVA Data & Analytics, 2020).

3.3 Los dilemas éticos actuales en el uso del Big Data

Entre los grandes problemas que podemos encontrar en el uso de esta herramienta, podríamos destacar los que a día de hoy más preocupan, debido al impacto directo que están teniendo en la sociedad (Drozhzhin, 2017).

3.3.1 La discriminación de datos predictiva

Ya hemos hablado de las ventajas del análisis predictivo, pero apenas se han comentado los riesgos que este conlleva. El análisis predictivo toma decisiones para prever la adecuación de un usuario para una determinada tarea, ya sea solicitar un puesto de trabajo o pedir un crédito. Y por lo tanto este análisis puede afectarle negativamente cualquier tipo de asociación que los algoritmos consideren desfavorable (de la Iglesia, 2021).

El riesgo no se encuentra en los datos, sino en la asociación e interpretación de los mismos, y en la toma de decisiones que estos provocan automáticamente, que puede llegar a estar basada hasta en premisas ilícitas. La duda que nace en base a esta tesitura es sí se puede llegar a discriminar basándose solamente en predicciones realizadas por algoritmos. Para ello habría que empezar a obligar a las empresas a realizar un esfuerzo para personalizar cualquier decisión, y equilibrar los análisis, adecuándolos a cada cliente (de la Iglesia, 2021).

3.3.2 La pérdida del anonimato

Es cada vez más complicado poder hacer una acción online sin que esta deje alguna asociación a tu persona. Se nos exige identificarnos para prácticamente cualquier cosa. De hecho, es cada vez más difícil para las compañías anonimizar los datos de manera que no se pueda reidentificar a los usuarios por la inmensa cantidad de información que producimos. La clave para solucionar este problema será la implementación de sistemas de seguridad que aseguren la seguridad y privacidad de los datos, y así poder aumentar el nivel de confianza de los clientes, pues por parte de estos

cada vez se enseña más a desconfiar de la ciberseguridad, y a limitar la información que se vuelca en internet. (Suarez, 2020).

3.3.3 El mal uso por parte de gobiernos

La cantidad de información sobre los ciudadanos que tienen las instituciones públicas es abrumadora, y cada vez mayor. Esta información va desde nuestro nombre, sexo, raza o religión, hasta nuestras huellas dactilares, información financiera e incluso fotografías. A pesar de que no es la mayor preocupación que deberíamos tener, el inapropiado uso de estos datos puede llegar a ser un gran riesgo en muchos países, pudiendo poner de ejemplo más claro casos como el de el del Gobierno Ruso o el Gobierno Chino (Suarez, 2020).

3.3.4 El negocio de los datos

El Big Data ha traído nuevos modelos de negocio, incluyendo muchos de ética discutible, entre los que se podría destacar la compraventa de datos. Es cada vez mayor el número de empresas que comercian con datos segmentados, enlazados a perfiles de clientes, permitiendo a la compañía compradora, ofrecer servicios y productos increíblemente personalizados. Y a pesar de las políticas publicitarias que suponen que frenan estas prácticas, como la de Google y otras grandes compañías, cada vez estamos más expuestos a este tipo de prácticas inmorales (IKUSI velatia, 2021).

3.3.5 El peligro de los Ciberataques

El tráfico de datos y la interconectividad también incrementan los riesgos de delitos de suplantación de identidad, robo, y pérdida de datos personales, entre otros. En 2017 se incrementaron enormemente el número de ciberataques y delitos digitales, con consecuencias mucho peores que las que habitualmente este tipo de delitos habían producido hasta el momento. Con la pandemia ya no solo hubo un incremento de delitos digitales, sino que, además, se idearon nuevas maneras de delinquir, que fueron dirigidas en su mayoría hacía los colectivos más vulnerables. (Mitek, 2018).

3.3.6 La microsegmentación

Otro grave riesgo es la microsegmentación, que suelen llevar a cabo los algoritmos para estudiar a la población, lo cual puede llegar a limitar la libertad del individuo. Como ya hemos comentado en el principio de este punto, a una persona clasificada de clase media por un algoritmo, le enviaran ofertas laborales, educativas o incluso inmobiliarias,

que el algoritmo considere "adecuadas" para él. Esto conlleva que el algoritmo limite la posibilidad al individuo de decidir por sí mismo en qué tipo de ambientes quiere entrar, e impida poder llegar a plantearse aspiraciones fuera de su alcance, perpetuando una discriminación de clases. Y eso sin contar el grave riesgo de las aseguradoras de personalizarse por completo las primas de seguros, desaparecería el elemento mutual, afectando gravemente a las coberturas y las indemnizaciones (Garriga Domínguez, 2020).

3.3.7 Perpetuación de los prejuicios

Otro grave problema que encontramos en el contexto actual es la perpetuación de los prejuicios. Los algoritmos Machine Learning son alimentados a través de datos históricos, los cuales crean el riesgo de que prejuicios del pasado vuelvan a resurgir en el contexto actual. Podemos encontrar ejemplos como estudios criminológicos estadounidenses, que apuntaban a los afroamericanos como delincuentes habituales, y esa información introducida en un algoritmo que se usase en un tribunal, crea una inseguridad jurídica a una persona injustificadamente, por una razón de raza. Y esto mismo lo podemos encontrar en una gran variedad de campos, como el de la medicina, que tradicionalmente consideraba la homosexualidad como principales causantes del VIH, o en el laboral, donde no consideraban como buenas profesionales a las mujeres. (Hernando & SINC, 2019).

IV. EL MARCO REGULATORIO SOBRE EL BIG DATA Y EL USO DE DATOS

4.1 El desarrollo normativo del Big Data

4.1.1 Derecho a la protección de datos personales: Carta de los Derechos Fundamentales de la UE y Constitución Española

En el artículo 18 de la Constitución Española, encontramos la protección al honor, intimidad y a la propia imagen, y, por lo tanto, también queda protegido el derecho a la protección de datos, tal y como pone el cuarto apartado de dicho artículo, "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*." (Constitución Española, BOE núm.311, 1978). El mismo Tribunal Constitucional reafirmo como derecho constitucional la protección de datos en la Sentencia 292/2000 (STC núm. 292/2000), estableciendo que el concepto alude a toda información personal, cuyo uso no sea solo la intimidad

individual sino la información de carácter personal, y cuyo empleo por terceros pueda dañar al individuo propietario de dicha información. Además, también quedan protegidos los datos personales que identifiquen a la persona, no solo a nivel de identificación básica, sino también aquella información que permita el desarrollo de perfiles raciales, económicos, políticos, o de cualquier índole que comprometa la intimidad del usuario. Este derecho constitucional permite al ciudadano controlar la gestión y uso de sus datos personales, y la capacidad de decisión y disposición de los mismos, pudiendo incluso modificar o suprimir dicha información.

Para reforzar el derecho a la protección de datos, en España se publicó la Ley 15/1999 (Ley Orgánica de Protección de datos de Carácter Personal 15/1999), y, para desarrollar dicha ley, tiempo después se aprobó el Reglamento 1720/2007 (Real Decreto 1720/2007 de protección de datos de carácter personal). De este desarrollo normativo cabría destacar la designación de la Agencia Española de Protección de Datos (en adelante AEPD), como institución encargada de la tutela del derecho fundamental a la protección de datos.

En referencia al Derecho Internacional Europeo, este derecho fundamental también se encuentra amparado, pues está reconocido, al igual que la obligación de garantizar y promover su protección en todos los países miembros de la UE; además, la UE insta a que cada país constituya una autoridad competente especializada en la protección de datos (Grupo de prensa de la Comisión Europea, s. f.). Entre los cuerpos normativos europeos que versan sobre el tema, encontramos el Tratado de Funcionamiento de la UE, el cual tiene establecido en su artículo 16 el derecho a la protección de datos de carácter personal. Y en el apartado dos de este mismo artículo también atribuye la competencia para regular el derecho a la protección de datos al Consejo Europeo y al Parlamento Europeo. Pero, por otro lado, encomienda a los Estados miembros de la UE el deber de protección del derecho de la UE en lo referente a este derecho, a la vez que lo controla a través de una autoridad con competencia sobre el tema (Tratado Unión Europea, 1992).

También podemos encontrar en el artículo ocho de la Carta de los Derechos Fundamentales de la UE el reconocimiento a la protección de datos a todas las personas, sin tener en cuenta su país de origen. En su artículo dos se detalla que los datos deben tratarse de manera leal, concreta y con consentimiento previo de la persona afectada, y el

derecho de esta a autorizar, modificar o eliminar dicha información. (Carta de Derechos Fundamentales de la Unión Europa, 2000).

Como último punto, cuando hablamos de Big Data, estamos ante una herramienta centrada en recolectar datos de miles de fuentes, y que apenas se ha regulado, a pesar de poder llegar a obtener información de millones de personas en cuestión de segundos (PowerData, s.f.). Cuando está herramienta se usa sin las correspondientes medidas, se encuentra ante el increíble riesgo de vulnerar un derecho fundamental, con las correspondientes consecuencias que eso conlleva, y, por ende, es de urgente necesidad crear un cuerpo normativo específico para garantizar el correcto uso de esta herramienta, no solo a la hora de recoger datos, sino también a la hora de gestionarlos y utilizarlos (Gil, 2015).

4.1.2 La Directiva 95/46/CE

En el marco de la UE, se aprobó en 1995 la primera regulación específica respecto a la gestión de datos. El 24 de octubre de ese año, el Consejo y el Parlamento Europeo aprobaron la Directiva 95/46/CE, (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, de 1995) la cual se centraba sobre todo en unificar todas las regulaciones sobre protección de datos personales dentro de la UE. Las principales directrices al respecto fueron el establecimiento de protocolos de control de todos los procedimientos de procesamiento y captación de datos, y establecer límites al respecto. Por otro lado, se encomendó a los países miembros de la UE instituir órganos independientes competentes de supervisar todas aquellas actividades en donde tenga lugar cualquier recolección de datos. Por último, se estableció como pilar fundamental para la obtención de datos el consentimiento (López Escudero, 2008).

4.1.3 Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal con base en la Directiva 95/46/CE

El 13 de diciembre de 1999 se aprueba la ley sobre Protección de Datos de Carácter Personal, que no entró en vigor hasta el 14 de enero del 2000 (Ley Orgánica 15/1999 de protección de datos de carácter personal). Su objetivo principal era desarrollar el artículo 18 de la Constitución Española (Constitución Española, BOE núm.311, 1978), para proteger y garantizar, en toda actividad que conlleve el tratamiento de datos personales, las libertades públicas y los derechos fundamentales de todos los ciudadanos.

Esta ley es propuesta como consecuencia de la Directiva 95/46/CE (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, de 1995), que crea en el ámbito de la protección de datos, una protección a la intimidad de los individuos.

Además, en esta norma se crea el cargo de encargado de captación de datos. Este encargado tendrá la responsabilidad de garantizar una obtención de datos consentida adecuadamente, cerciorándose de conseguir el consentimiento inequívoco del usuario antes de recolectar sus datos. Para ello, el usuario deberá estar bien informado, en un contexto transparente y explicito y explicando de manera inequívoca de las intenciones que hay para recoger esa información. Esta explicación deberá ser precisa y expresa para que el consentimiento no se vicie, ni haya medios fraudulentos. Dentro de los límites para el uso de datos cedidos a terceros, se encuentran el deber de utilizar dichos datos para los mismos fines con los que fueron obtenidos, y además la obligación de obtener el consentimiento del interesado para la cesión (Ley Orgánica 15/1999 de protección de datos de carácter personal).

Por último, en referencia a los derechos reconocidos en esta norma, y su respectiva tutela, se asignará a la Agencia de Protección de Datos dicha función. Esta organización nació en 1992, como órgano independiente con autonomía funcional y presupuestaria, y cuyas funciones empezaron siendo principalmente presupuestarias, tal y como establece el Reglamento General de Protección de Datos (Reglamento 2016/679, relativo al tratamiento de datos personales y a la libre circulación), (*AEPD*, 2021).

4.1.4 Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo

El 27 de abril de 2016, el Consejo y el Parlamento Europeo aprobaron el Reglamento de la UE 2016/679, para garantizar la protección, gestión y libre circulación de datos personales de las personas físicas, siendo de aplicación a todos los países miembros de la UE, sin la necesidad de tener que trasponerlos. Con la entrada en vigor de este Reglamento se derogó toda la legislación vigente, comentada en los apartados anteriores. Con el Reglamento se buscaba armonizar la legislación europea en materia en protección de datos, para así garantizar una uniformidad normativa en todo el territorio (Reglamento 2016/679, relativo al tratamiento de datos personales y a la libre circulación).

Al armonizar la normativa europea se consiguió reforzar y ampliar el derecho de protección de datos, garantizándolo al nivel de un derecho fundamental. Además, como novedad, incluyó un registro para controlar la gestión de datos, teniendo que estar siempre actualizado y disponible, para que las autoridades de control independientes puedan garantizar un correcto control de las actividades de procesamiento. Por otro lado, se reforzó los requisitos para conceder el consentimiento de los usuarios para recolectar sus datos, teniendo que incluir dicho consentimiento un supuesto especifico e informado con antelación, dejando de manera clara y concisa las intenciones que existen con dicha recolección de datos (editor72, 2022).

En dicho texto se incluyó en su artículo 17 el derecho de supresión, o también apodado derecho al olvido, que protege a las personas cuya información personal haya sido tratada, y que exijan que esta se elimine. En el artículo 20 del mismo cuerpo legal se incluye el derecho a la portabilidad de datos, que permite que se reciban la información que se cedió en un momento dado, en un formato estructurado, de lectura mecánica y de uso común. También hay que comentar que en el apartado primero de dicho Reglamento se incluye la posibilidad de que los usuarios elijan si desean que su información personal sea objeto para la creación de perfiles. Esta norma da la posibilidad de regular un régimen de sanciones a los países miembros, en toda aquella situación no prevista en el artículo 83, que es donde se fijan las sanciones administrativas. (AEPD, 2021).

Para concluir, hay que argumentar que este Reglamento ha brindado una mayor protección legal a la información privada de los usuarios. La inclusión de los derechos de la portabilidad de datos, decisión sobre elaborar perfiles con sus datos y el derecho al olvido garantizan mayor seguridad jurídica. Además, el hecho de haber empleado la figura del Reglamento era de gran necesidad para poder garantizar una regulación armonizada y efectiva en el continente.

4.1.5 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Dos años después, el 27 de julio se promulga el Real Decreto-ley 5/2018, (Real Decreto-ley 5/2018, relativo a la adaptación del Derecho español) para crear soluciones para medidas urgentes en el derecho español, como respuesta a la normativa europea en materia de protección de datos, para cubrir aspectos que el Reglamento había cedido en competencia a los estados, con el fin de que estos aprobasen una ley orgánica que adaptase

cada ordenamiento a esta necesidad. El 7 de diciembre de 2018 se publicó la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. (Ley Orgánica 3/2018 de Protección de Datos Personales).

Con su aprobación se reconfiguró la legislación nacional sobre protección de información personal, y, además, en el Título X de dicha Ley, se aprobaron una serie de garantías para los derechos digitales. En el artículo 3 de esta Ley también queda establecida una regulación relativa a la cesión de datos privados de los individuos fallecidos, para dar la opción a las familias y parejas de solicitar el acceso a la información personal de los fallecidos, pudiendo exigir la supresión o rectificación de dicha información (Ley Orgánica 3/2018 de Protección de Datos Personales).

Esta Ley también regula el consentimiento de los menores de edad, que solamente podrá ser aceptado si el menor es mayor de 14 años, y en el caso contrario se exigirá la autorización de los tutores legales del menor. En el Título III encontramos garantizada la idea de información y transparencia, para que las personas puedan tener acceso a toda la información básica sobre la identidad de los responsables del tratamiento de datos, la finalidad para recoger dicha información, y la opción de defender los derechos establecidos en el Reglamento (Ley Orgánica 3/2018 de Protección de Datos Personales).

En el Título VII están reguladas las distintas las autoridades nacionales de protección de datos, siendo la principal la AEPD. Dicha institución independiente se encargará de tutelar el derecho a la protección de datos, y la capacidad de sancionar, a la vez que ostenta una función de auxilio, para proteger a los afectados del procesamiento de datos, investigando los hechos y atendiendo a las reclamaciones. Además, la AEPD tendrá un papel clave, en calidad de asesor, en aquellos procedimientos reglamentarios y legislativos que traten materia de protección de datos (Ley Orgánica 3/2018 de Protección de Datos Personales).

Para terminar, el hecho de consagrar en una norma de rango de ley orgánica los derechos de cancelación, oposición, supresión, portabilidad, acceso y rectificación supone garantizar el principio de seguridad jurídica. Al mismo tiempo, considero de gran relevancia el hecho de incluir un título especifico que prevea regular los derechos digitales, y así cubrir posibles situaciones, que no están previstas en nuestro ordenamiento.

4.1.6. Nueva regulación europea para la Inteligencia Artificial

El pasado abril de 2021, se presentó ante la CE una propuesta de regulación de IA, siendo la primera vez que se propone una Ley de IA, con el objetivo de desarrollar una regulación legal para este campo, y siendo de aplicación a todos los sectores, a excepción del militar. Diversos grupos han revisado el texto desde que fue presentado, como Panoptykon Foundation, Access Now y European Digital Rights, emitiendo un veredicto bastante crítico. Estos grupos consideraron que la propuesta legislativa se ha quedado escasa a la hora de proteger los derechos fundamentales ante el uso indiscriminado de la IA, y acto seguido publicaron un informe con toda una lista de puntos que se debería revisar (Grupo de prensa de la Comisión Europea, 2021).

Como respuesta a esto, la CE preparó otro documento en donde describía la propuesta presentada como un marco legal de confianza, en donde se centraba en los intereses de la gente para la IA. Pero, por otro lado, el documento que emitieron los grupos civiles considera que dicho marco podría resultar en varias clases de abusos, producidos por la escasez de controles que son planteados como prevención de problemas futuros. Estos mismos grupos reclaman que la CE considere revisar la propuesta de ley en cuestión, y cambiar varios apartados antes de publicar el texto definitivo. Entre esos puntos, uno de los que más destacan es la necesidad de flexibilizar la ley, para que este a prueba de futuros avances tecnológicos (Jiménez, 2021).

Otra crítica ha sido la escasa ambición de la nueva ley frente a determinados usos; entre los usos a los que se refieren dichos grupos, encontramos la oposición ante permitir el reconocimiento biométrico en espacios públicos, la creciente demanda de que se prohíba el uso de Sistemas de Crédito Social al estilo chino, de los sistemas de predicción de delitos y de los sistemas de reconocimiento de emociones. Lo que se busca es que se prohíba en si el uso de cualquier tipo de sistema que conlleve el riesgo de vulnerar un derecho fundamental (Jiménez, 2021).

Otro reclamo al respecto es que se garanticen herramientas para poder revertir aquellas situaciones en donde los ciudadanos se vean afectados por el uso del IA. Estos grupos defienden que la propuesta de ley está muy alejada de la línea jurisprudencial que había marcado el Reglamento General de Protección de Datos (Reglamento 2016/679, relativo al tratamiento de datos personales y a la libre circulación), en donde el ciudadano

era dotado de un conjunto de derechos para poder defenderse ante cualquier tipo de abuso empresarial, llevado a cabo con la IA (González, 2021).

Ante esta problemática, los grupos han propuesto que sean reconocidos dos derechos básicos, que pueden ser fundamentales para futuras resoluciones judiciales: el derecho a que se dé una explicación inteligible y clara sobre el objetivo y funcionamiento de los sistemas IA, y el derecho a que los a sistemas de IA de alto riesgo no se les permita usar datos de ningún sujeto (González, 2021).

En conclusión, es esperanzador que por fin se esté creando una regulación adecuada para proteger los derechos fundamentales del ciudadano ante los abusos del uso del Big Data y la IA por parte de las compañías, pero es preocupante la lentitud con las que las autoridades van atreviéndose al endurecer la regulación en este campo, puesto que la velocidad a la que avanza la tecnología es abrumadora a la par que imparable, algo que debería ponernos en alarma y obligarnos a desarrollar una normativa mucho más restrictiva y flexible. (Manceñido, 2021).

4.2 Códigos deontológicos empresariales y el Big Data

Los avances y descubrimientos en el Big Data están en auge, y no nos debería extrañar (debido a todas las aplicaciones que ya hemos ido analizando a lo largo de este proyecto) que este crecimiento traerá también nuevos riesgos. Por eso mismo se ha de remarcar la crucial importancia de regular este tipo de herramientas para evitar correr riesgos contra los derechos fundamentales del usuario. Cuando hablamos de regulación, no solo hay que centrarse en legislación emitida por un ente público, sino que también hay que contemplar los códigos deontológicos empresariales, que al fin y al cabo contribuyen de gran manera a crear y afirmar una conciencia colectiva dentro de un sector profesional (Noain Sánchez, 2016).

Los riesgos que se contemplan por el uso de datos de manera descontrolada en las compañías pueden conllevar decenas de conflictos legales. El Reglamento General de Protección de Datos establece una serie de normas y directrices, basadas en los principios de transparencia, información y libertad, cuya vulneración conlleva grandes sanciones económicas (Reglamento 2016/679, relativo al tratamiento de datos personales y a la libre circulación); también podemos contemplar los riesgos técnicos que enfrentan las compañías, pues un mal uso de estas tecnologías podría terminar produciendo brechas de

seguridad que acabarían perjudicando la imagen de la empresa, e incluso llegar a exponer públicamente la información de las bases de datos. Por último, podemos encontrar los riesgos éticos empresariales, de los cuales apenas se han tratado en los últimos años, y suelen ser los más desapercibidos, pero que cada vez preocupan más a las compañías. La "dictadura de los datos" está empezando a proponer retos que llegan a preocupar hasta las más altas esferas. En conclusión, una compañía enfrenta grandes riesgos cuando hace una mala gestión de estas herramientas. (Aced, Heras, Saiz, 2018).

Entrando en detalle sobre los riesgos éticos empresariales, hay que aclarar que estos tienden a pasar desapercibidos de fácil manera cuando surgen oportunidades económicas que complican su cumplimiento. Pero, como ya hemos tratado a lo largo del trabajo, cuando esto surge y no se prioriza una ética responsable, las consecuencias son bastante graves para la compañía, tanto a nivel ético, como a nivel técnico o legal. Es considerable proponer que se regule la obligación de incorporar en cada empresa un consultor o comité ético que analizase la repercusión de cada política empresarial. También sería aconsejable animar a un mayor compromiso con el principio de transparencia, para que los accionistas puedan conocer quienes están implicados en estos procesos, y que fines tienen. (Calle, 2018). Por otro lado, sería de gran ayuda, para que todo esto funcionase, el impartir formación ética a los expertos implicados en los procesos de Big Data, para que sean conscientes de los peligros de la falta de transparencia, y detecten más fácilmente una mala praxis.

En 2018, se aprobó el Código de Buenas Prácticas en protección de datos para proyectos de Big Data, elaborado por la AEPD y el ISMS *Forum Spain,* constituyendo un punto de partida para la regulación ética empresarial, e impulsar el desarrollo de códigos deontológicos para profesionales del Big Data (del Rosal, 2018).

Este código se divide en dos partes, la primera en donde se instituye un régimen de referencia y cuestiones clave, que abarca desde la definición de lo que es el responsable del tratamiento de datos o el principio de transparencia, hasta la manera de recoger y gestionar los datos y la posibilidad de los ciudadanos de ejercer sus derechos. El segundo bloque trata sobre los aspectos que hay que las entidades deben tener en cuenta al utilizar Big Data, para no perjudicar las garantías de privacidad y protección de datos personales. Además, el documento detalla otros aspectos, como la urgente necesidad de llevar a cabo

evaluaciones del impacto que puede tener estos tipos de proyectos, para así minimizar riesgos, o incluso llega a proponer que las empresas anonimizaran irreversiblemente los datos que recolecten. El Código termina con una revisión de las medidas más recientes de la tecnología moderna, y su imprescindible papel en la defensa de la seguridad y privacidad de los usuarios, para crear un entorno de confianza para las personas. (Dat, 2019).

Aunque este código supone un gran paso para la regulación ética del Big Data, es inevitable pensar que es insuficiente, pues la protección de datos y la privacidad son uno de los muchos problemas éticos que estamos afrontando desde que el Big Data llegó a nuestros días.

4.3 Necesidad de Tribunales especializados en las nuevas tecnologías

Según la legislación de la UE, los tribunales especializados serán aquellos encargados de tratar en primera instancia aquellos asuntos, que por la materia sobre la que versan, requieren de ser tratados por un órgano especializado. Este tipo de tribunales, adjuntos al Tribunal General, dependen del Tribunal de Justicia de la UE. Para poder crearlos, se debe reconocer previamente alguna razón de necesidad para abordar una materia en específico, de manera más precisa y concreta, y tras ello, se debe aprobar un reglamento por la CE, en conjunto con el Parlamento Europeo, a través de una votación aprobada por mayoría cualificada. Una vez aprobado el correspondiente Reglamento, los miembros de la Comisión deberán nombrar responsables que cumplan los requisitos de independencia, así como la especialización y capacidades necesarias para las labores que dicho tribunal necesitaría. (Parlamento Europeo, s. f.).

Ante la reciente y llamativa introducción del Big Data y al IA en nuestra sociedad, el gran alcance que tiene, y la falta de regulación sobre el tema, es más que necesario que se cree un Tribunal Especializado para tratar aquellos casos que versen sobre el tema, y en que pueda verse comprometida la UE.

Es cierto que el Tribunal de Justicia de la UE no ha brindado una protección especifica a los Derechos Humanos, y, por ende, tampoco lo ha hecho con la protección de datos. Pero, por otro lado, sí que ha protegido los intereses de la UE, creando incluso desarrollos normativos al respecto, como la Carta de Derechos Fundamentales de la UE

(Carta de Derechos Fundamentales de la Unión Europa, 2000/C), en donde, en el artículo ocho, se protege los datos de carácter personal y la circulación de estos datos, regulando aspectos como que la manera de trabajar ha de ser leal, con fines concretos y que estos se obtengan mediando el consentimiento de las personas a quienes se refieren.

Por todo lo comentado en este punto, y con la falta de regulación específica y el desconocimiento social generalizado que existe al respecto, es más que justificable la urgente necesidad de crear tribunales especializados en IA y Big Data para solucionar los cientos de litigios que surgen cada día sobre estos temas. (Glosario de las síntesis - EUR-Lex. s. f.).

4.4. Evaluación del marco jurídico

Tras haber evaluado los mayores dilemas éticos que se estamos afrontando en la actualidad, y analizar el marco jurídico vigente, podríamos concluir que, a pesar de que los usuarios han conseguido un mayor control sobre sus datos personales, y un mayor poder de decisión sobre el uso de los mismos, también tiene su parte mala. Para empezar, esta situación de protección solo se ha regulado así en Europa, ya que en EEUU no se aprobó una ley para la protección del consumidor hasta 2020 (RenterBarcelona, 2020), y, por otro lado, en países asiáticos y sudamericanos el nivel de indefensión que hay hacía la privacidad de los usuarios es cada día más grave (Stranieri, 2021). Este hecho debería hacernos sentirnos orgullosos, por defender de una manera garantista y ética los derechos fundamentales a la intimidad y la dignidad de nuestros ciudadanos. Pero, por otro lado, debido a que las empresas que operan en Europa deben esquivar mayores obstáculos para poder comercializar los resultados que obtengan en base a los datos que recolectan, nos hace menos competitivos en comparación con el resto de países.

Y un segundo punto sería la ausencia de regulación en el resto de problemas que ha traído el Big Data. La microsegmentación o la discriminación por algoritmos, entre otros temas, son conceptos inexistentes en la regulación vigente. Los ciudadanos podrán reclamar sus derechos para el uso de sus datos personales (Stranieri, 2021), pero se ven totalmente indefensos ante las consecuencias del control no supervisado e inmoralmente utilizado de su información personal.

Por lo tanto, Europa debería de dejar de centrarse en seguir regulando la protección de datos de manera tan estricta, y ponerse de acuerdo con el resto de naciones con las que comercia, alentándolas a desarrollar una legislación propia al respecto. De

esta manera conseguiría promover un comercio común más justo e igualado. Y, por último, centrarse en regular el resto de peligros, ante los cuales los ciudadanos no tenemos ninguna herramienta jurídica o administrativa para defendernos, y, por ende, nos deja en una situación de vulnerabilidad ante una serie de peligros ante los que nos vemos expuestos a diario.

V. PERCEPCIÓN POR LOS EXPERTOS DEL CUMPLIMIENTO ÉTICO-LEGAL DEL BIG DATA

Para contrastar la investigación teórica del trabajo, se llevaron a cabo una serie de entrevistas a través de cuestionarios, dirigidos especialistas en Big Data de diferentes ramas.

Esta entrevista se puede dividir en cuatro partes. La primera consiste en conocer la opinión de los expertos sobre el nivel de concienciación que tiene el ciudadano del uso y fin que dan las empresas a sus datos personales, y la capacidad que tiene de llegar a conocer el destino de dicha información. La segunda, va dirigida a conocer la opinión de los profesionales sobre la legislación vigente en materia de protección de datos. La tercera busca entender la forma de analizar los dilemas éticos sobre el uso de los datos en las empresas; y, por último, el final del cuestionario plantea qué nuevos retos podremos enfrentar en un futuro cercano, y cómo de preparados estamos para enfrentarlos.

5.1. La situación del ciudadano

Para empezar, hay que destacar que en las entrevistas ha habido un gran consenso en que los consumidores no leen, ni son capaces de llegar a entender, los contratos de términos y condiciones de uso que plantean las empresas. Sí que llegan a poder comprender que sus datos van a ser monetizados, y posiblemente lleguen a negociar con ellos, pero, tal y como están escritos los contratos de términos de uso para un usuario medio es casi imposible llegar a entender lo que aceptan. Estos contratos, en especial cuando son online, debido a que son muy extensos y con un vocabulario excesivamente técnico, con el fin de que el usuario acepte los términos sin mirarlos. Dos de los entrevistados hicieron hincapié en que la regulación en Europa, a diferencia de Estados Unidos, es muy estricta, lo que complica mucho el proceso de recolección de datos. A pesar de ello, la ley sigue sin motivar a las empresas a que empiecen a redactar los contratos de manera simple y entendible para el ciudadano para que este pueda llegar a

entender el destino de su información personal, y no esté en una situación de desconocimiento y engaño, como la actual.

Después, respecto al destino final de los datos, ha habido dos posturas. La primera defiende que depende de la compañía. Hay algunas empresas que cumplen la ley vigente de manera estricta, pero, por otro lado, hay otras compañías que hacen balance sobre si les es rentable enfrentar una posible multa por incumplir la normativa vigente, calculando el beneficio que obtendrían, y si les es beneficioso lo terminan llevando a cabo. Pero hay una segunda postura que defiende que hoy en día las grandes compañías disponen de equipos legales que acaban encontrando la manera de obtener beneficios a través de negociar con datos, sin tener en cuenta la ética ni incumplir la ley. La estricta regulación europea en estos casos lo único que ha conseguido es que haya ciertos límites que no se puedan sobrepasar, como ocurre en Estados Unidos, donde el usuario se encuentra desprotegido.

Y, por último, en referencia a la supervisión de la información recolectada a diario ha habido opiniones muy dispares. Lo único en lo que la mayoría de los entrevistados estaban de acuerdo es que por mucho que se quieran supervisar, es inevitable que los algoritmos puedan acabar produciendo algún tipo de análisis sesgado. Las razones son varias debido a que los sesgos se pueden producir bien porque los datos vienen sesgados, o bien por que los encargados de recolectarlos o los de analizarlos, voluntaria o involuntariamente, reflejen un prejuicio personal en ellos. Un entrevistado llegó a declarar que en su opinión creía que era imposible que la información estuviera libre de sesgos. Explicó que en el *Machine Learning* el error se conformaba de tres partes: la varianza, que es la dispersión de las predicciones sobre el dato real que se dio finalmente, el sesgo, que son los datos de muestra que pasan al algoritmo, y el error irreductible, que es el porcentaje de error que jamás se eliminará. Con esta estructura es evidente que es inevitable que los algoritmos produzcan análisis sesgados, pero como el mismo entrevistado dijo, es nuestra obligación controlar los y tratar de evitar las consecuencias que este sesgo puede traer al ciudadano. Por último, querría resaltar el argumento del segundo entrevistado, que también explicó que España no está suficientemente preparada para poder controlar todos los riesgos y dilemas del Big Data. Todavía nos quedan muchos obstáculos que superar para poder llegar a enfrentar y solucionar este problema.

5.2. La legislación vigente

La segunda parte de la entrevista se dirigió a conocer la opinión y conocimiento de los expertos sobre la legislación europea vigente en materia de protección de datos. En el primer punto, sobre las herramientas que el ciudadano tiene para defender sus derechos frente a las situaciones discriminatorias que acarrean los sesgos en los algoritmos, las respuestas han sido variadas, pero todas llegan a la conclusión de que no hay vías efectivas para protegerse. Todos los entrevistados proponían soluciones para los usuarios muy diversas, desde aumentar la supervisión y el control sobre las concesiones de datos personales que autorizan, las suscripciones que contratan, o las páginas que visitan, hasta usar la vía democrática y abogar por partidos políticos que defiendan esta causa. La mayoría estaban de acuerdo en que el ciudadano no tiene herramientas para defender se de estas situaciones de manera directa y efectiva, y además opinaban qué existe un completo desconocimiento de que vías legales alternativas puede haber para defenderse. En conclusión, tal y como explicaban los entrevistados segundo, cuarto y quinto, es urgente un desarrollo legislativo al respecto.

En referencia a la opinión que les generaba la legislación española sobre protección de datos, los entrevistados se dividieron en dos posturas. La primera estaba totalmente de acuerdo con la legislación vigente, y explicaban que les parecía muy adecuada y efectiva para defender los intereses del ciudadano. Incluso el cuarto y el quinto entrevistados defendieron que debería aumentar la regulación vigente para mejorar las vías de defensa para los usuarios. Pero la contraparte defendía que las leyes españolas sobre protección de datos eran demasiado estrictas y exhaustivas, y debido a ello, producen situaciones contraproducentes para el sentido teleológico que persigue la legislación. Con esto nos referimos a situaciones como los clausulados interminables que redactan las empresas, que acaban haciendo que los usuarios los firmen sin pensar. Destacaría al séptimo entrevistado, que defendió que a pesar de que España rige una de las normativas más estrictas en materia de protección de datos de la UE, también opinaba que faltaba un desarrollo mayor y más claro, así como más flexible a los cambios de la propia sociedad, pues según él, nuestra legislación tiene un retraso real sobre los datos de más de 20 años. Lo único en lo todos estuvieron de acuerdo es que la regulación europea es ejemplar, y defiende de manera más efectiva a los usuarios, en comparación con la americana, sin hablar de otras regulaciones extranjeras, que como ya se comentó, son casi inexistentes, o incluso nulas.

Y, por último, en referencia a la repercusión que ha tenido la legislación europea y española en nuestra posición como competidores con el resto de los países, a excepción de los entrevistados cuarto y quinto, hubo unanimidad en que nos volvíamos menos competitivos al tener una regulación más estricta. Las razones son obvias, ya que a mayor nivel de obstáculos que impidan a las compañías obtener beneficio en el territorio, menor interés habrá en desarrollar proyectos en Europa. El cuarto y el quinto entrevistados defendían que, en un mundo tan globalizado, la mayoría de las empresas son extranjeras, y acaban encontrando vías para saltarse los obstáculos que nuestra regulación impone. Pero el resto defendían que independientemente de que perdiésemos competitividad, no era razón para modificar la regulación para volverla más laxa, sino que, al contrario, deberíamos obligar a las empresas extranjeras a cumplir nuestra regulación cuando operen en nuestro territorio, para ayudar a que nuestras compañías compitan en igualdad de condiciones con las empresas extranjeras. Y me gustaría resaltar la respuesta del último entrevistado, quien explicó que, a pesar de perder competitividad, también ganábamos popularidad en el mercado al dar más seguridad y mejor imagen a los clientes, lo que podrá acabar trayendo una diferencia competitiva en positivo.

5.3. La ética dentro de las empresas

En este punto, se habló sobre los códigos deontológicos de las compañías, y su relevancia en el sector. Lo primero que se preguntó fue la existencia de dichos códigos en las compañías en donde trabajaban, y solo cuatro de los entrevistados confirmaron la existencia de un código ético en sus oficinas, quienes además contaron que junto a la normativa ética se impartía una formación para garantizar que los trabajadores conocían y cumplían dichas normas. Es importante remarcar que, en un sector que se está volviendo tan conocido, que está en auge, y en donde surgen dilemas éticos a diario, es preocupante el hecho de que solo la mitad de los profesionales de esta investigación tuvieran un manual de ética en sus compañías, limitándose a obedecer y cumplir la ley vigente, y sin preocuparse por perseguir una actuación ética en sus actividades.

Siguiendo con el tema, se preguntó la opinión de los entrevistados sobre si creen que el Gobierno debería instar a desarrollar códigos éticos en las empresas, para los especialistas en Big Data, y las respuestas fueron totalmente dispares. El primer entrevistado creía que era una buena propuesta, pero solo para grandes compañías, pues creía que esta medida dificultaría competir a las PYMES con las grandes compañías. El

segundo defendió que lo que debe desarrollarse son leyes, no manuales, ya que son las que realmente consiguen resultados efectivos. El tercero estaba en profundo desacuerdo con la propuesta, en base de que la ética no debería ser objeto de la ley, y, por ende, la moralidad de las actuaciones se decide en el mercado, cuando se manifiestan cambios en la oferta y la demanda tras cada actuación empresarial, y compartía la opinión del segundo entrevistado en que, si hubiera un desarrollo normativo, este tendría que ser legal. El quinto y el cuarto estaban totalmente de acuerdo con la propuesta, y, además, este último defendía que la medida tendría que llevarse al nivel de toda Europa. El sexto entrevistado sostuvo dos posiciones. Por un lado, opinaba que sería beneficioso para la protección de la información y garantizar un uso ético de la misma, pero en contraposición opinaba que esto produciría mayor burocracia, y más fricción a la hora de crear un negocio, haciendo que emprendedores y nuevos proyectos se acabasen llevando a países donde hubiera menos requisitos para comenzar un nuevo proyecto. Y para acabar, el séptimo defendía que la obligación debería establecerse en función de la actividad de la empresa.

Por último, se preguntó sobre qué creían que debería incluir un código deontológico para profesionales de su sector. Entre todas las aportaciones ofrecidas, destacaría la importancia que se dio a que estos códigos obligasen a mejorar la transparencia y facilidad de información para los usuarios, en dar formación ética a los profesionales, e incrementar el control de envío, trato, almacenamiento y acceso a los datos, para garantizar un análisis de información limpio y correcto. Querría destacar primero, la respuesta del séptimo entrevistado, quien empezó remarcando las diferencias entre IA y asistente inteligente (concepto que engloba a la mayoría de las herramientas diarias que usamos, que coloquialmente confundimos con Inteligencia Artificial), para remarcar que a día de hoy no existen realmente un gran número de herramientas de IA disponibles para el público, pero estas son disruptivas y cada vez más necesarias, en especial en el mundo laboral; este número está en aumento y cada vez nos acercamos más a la IA General, y según él, solo por este hecho sería necesario desarrollar normativa sobre el tema, para prevenir riesgos a un futuro cercano. Y, para terminar, destacaría la respuesta del cuarto entrevistado, quien defendía que no bastaría con desarrollar obligaciones éticas a través de un manual, sino que se debería crear un organismo independiente que garantizase el buen uso de los datos, dando el ejemplo de lo que sucede con el uso de Internet y la gestión de la WWW, como por ejemplo el ICANN.

5.4. Nuevos frentes en el mundo del Big Data

En este último apartado, se buscó investigar sobre dos temas: la primera trataba de conocer qué nuevos dilemas y riesgos afrontaremos en el Big Data, y la segunda fue sobre cómo los entrevistados veían de preparada a Europa para hacer frente a los nuevos peligros a nivel de regulación legal.

Sobre qué frentes más graves estamos afrontando, y cuales vendrán, el primer entrevistado consideró que una herramienta como el Big Data es demasiado incierta como para poder saberlo, debido a que hay nuevos avances y descubrimientos a diario, y eso imposibilita el poder llegar a predecirlo. El segundo y el tercer entrevistados coincidieron en que el mayor peligro que hay actualmente, y que va en aumento, era el control de las compañías y las autoridades públicas sobre los usuarios, debido a toda la información que poseen de nosotros, y el segundo problema que destacaron fueron todos los problemas psicológicos que están apareciendo, por el uso de las tecnologías, especialmente en los menores. Ambos defendieron que el Estado debería dificultar, o incluso impedir, que las autoridades públicas y las grandes compañías pudieran llegar a conocer tan a fondo la información personal de los usuarios, promoviendo el anonimato, o supervisando el uso de información. Además, propusieron que se mejorasen los servicios de psicología públicos, y aumentar la formación para el buen uso de la tecnología en la enseñanza pública. El cuarto entrevistado mostró una gran preocupación por los sesgos en los algoritmos y la falta de supervisión del comportamiento de ciertos usuarios. Propuso como solución a este problema la creación de un organismo regulador más intransigente que los actuales, y empezar a impartir formación a los usuarios sobre el buen uso de la tecnología. Y el quinto y sexto entrevistados no veían ningún peligro intrínseco al uso de esta herramienta. Defendían que el Big Data ha mejorado el mundo laboral en varios aspectos, y que el único peligro que existe es el mismo que con cualquier otra herramienta digital: que el usuario la utilice de manera inadecuada. Opinaban que la única forma de solucionarlo sería mejorando la educación y preparando más profesionales en el sector, ya que otro tipo de medidas más estrictas podrían entorpecer las actividades empresariales y dificultar la creación de nuevos proyectos a las compañías. Por último, el séptimo entrevistado defendía que los legisladores deberían prepararse para los problemas que están por venir debido al crecimiento de esta herramienta, y no esperar a que sucedan.

Y la segunda parte fue dirigida a conocer la opinión que tenían los profesionales sobre la nueva ley de IA de la Comisión Europea. La mitad de ellos apenas habían

escuchado sobre ella, en especial el tercero y el sexto que la desconocían por completo. El primer entrevistado veía esta ley como una evidencia del retraso que hay en Europa respecto a la IA y el Big Data, pero, por otro lado, era una prueba de como Europa es el único territorio que se toma realmente enserio la protección de la información personal de los usuarios. El segundo entrevistado no la conocía en profundidad, pero defendía que se debería hacer hincapié en la educación social y laboral. El cuarto, quien la había estudiado en profundidad, consideraba que le faltaban varios aspectos por reglar, y que tal y como estaba redactada, había varias lagunas legales en donde las compañías podrían tener licencia para actuar sin tener en cuenta los derechos de los ciudadanos. Él defendía que se debería regular teniendo en cuenta los derechos de las personas con necesidades especiales, ya que se encontraban en una situación de especial vulnerabilidad. El quinto entrevistado consideraba que esta ley era un buen comienzo para empezar a enfrentar los problemas de esta herramienta, pero que está mal planteada. Opinaba que esta ley se centra demasiado en regular el funcionamiento de la tecnología, cuando una ley habitualmente debería centrarse en los derechos de las personas. Además, defendió que está creciendo el miedo social a la IA por el exceso de series y películas de ciencia ficción al respecto, lo que, sumado al desconocimiento sobre este campo, está produciendo que sea complicado regular este campo, y consecuentemente las leyes sobre IA y Big Data puedan perder eficacia. Y, por último, opinaba que veía necesario que se incrementase el control en la entrega y venta de datos entre empresas. Para terminar, el séptimo entrevistado empezó explicando los puntos más importantes en su opinión de la propuesta de la Comisión Europea, la cual distingue cuatro niveles de riesgos, de los cuales resaltó el cuarto. El cuarto y último nivel es el riesgo inaceptable, es decir, aquellos sistemas de IA considerados una amenaza para la seguridad del ciudadano y sus derechos fundamentales, por ejemplo, un juguete con asistencia de voz que fomente el comportamiento peligroso de los menores o un sistema de "puntuación social" por parte de los gobiernos. En el mismo nivel de máximo riesgo se incluyen los usos de la IA en infraestructuras críticas que puedan afectar a la salud de los ciudadanos. El defendía que esta parte de la propuesta era necesaria desde hacía tiempo, pero a pesar de esto, también defendía que esta misma propuesta también debería incluir un análisis de riesgos, documentación detallada, un alto nivel de robustez y supervisión humana de la trazabilidad de los resultados.

VI. CONCLUSIONES

Las nuevas tecnologías de recolección y análisis de la información ya se han integrado en nuestra sociedad por completo. El Big Data es un claro ejemplo de cómo los nuevos sistemas de recolección y gestión de datos han revolucionado la vida empresarial y el mercado laboral. En este trabajo hemos tratado los riesgos más evidentes y las mayores consecuencias que se están produciendo desde la aparición del Big Data, focalizándonos especialmente en la protección de datos, la gestión por parte de los Gobiernos de los derechos de los usuarios y la discriminación por segmentación de datos en los algoritmos.

Tras el análisis de los problemas éticos que el Big Data pueda llegar a crear, y analizando con la investigación sobre la legislación vigente, llegamos a las conclusiones que se han descrito al final del cuarto epígrafe. Contrastando estas conclusiones con las entrevistas realizadas a especialistas en el sector podríamos concluir los siguientes puntos:

En el primer punto, habría que destacar que, en materia de protección de datos, la legislación ha empezado a excederse a la hora de limitar las actuaciones de las compañías, lo que nos está haciendo perder competitividad a nivel internacional, pero, por otro lado, ha garantizado una protección efectiva de los derechos del consumidor. En temas de regulación, podemos ver cómo la ética ha conseguido ser el pilar fundamental de la legislación europea. Se ha conseguido crear un desarrollo normativo que defiende de manera efectiva los problemas fundamentales del consumidor, en lo que a protección de datos se refiere, y que sigue desarrollándose, abarcando cada vez más campos que garanticen un uso correcto de la información privada del ciudadano por parte de las compañías. Aún debería abarcar más temas, pero la manera de llevarlo a cabo es complicada, ya que corremos el riesgo de seguir perdiendo competitividad. Y respecto a este último punto, también hay que tener en cuenta de que está pérdida de competitividad es relativa, debido a que ser el territorio con la mejor regulación en materia de protección de datos, consigue hacer sentirse seguro al consumidor, y que las compañías que operen en Europa ganen popularidad. El legislador debería centrarse en acabar de desarrollar ciertos puntos en esta materia, y empezar a regular otros problemas actuales que ha traído el Big Data (ante los cuales no existen suficientes herramientas legales para defender los derechos de los ciudadanos) de una manera progresiva, para seguir siendo competitivos a la par que éticos.

Por otro lado, el segundo punto a destacar es la falta de regulación que existe sobre el control de los sesgos en la información utilizada por los algoritmos. Los algoritmos se reprograman con la información que les introducimos y después producen reglas externas, pudiendo dicha información contener sesgos discriminatorios creados por los mismos analistas. Es decir, que la IA y el Big Data ya no son una garantía del pretendido orden y control que sugería la automatización de las empresas, justo, al contrario, son un potencial peligro de discriminación que apenas tiene supervisión. Europa es el primer continente en intentar abordar este tema de manera directa, pero carece de capacidad suficiente para controlarlo. Tal y como decían los expertos, estos sesgos habitualmente se producen de manera involuntaria, y normalmente las compañías no se dan cuenta de ellos hasta que no se ha producido el daño. Es cierto que muchas empresas han tomado la iniciativa de desarrollar distintos códigos de conducta para prevenir estos riesgos, y evitar crear conflictos con los clientes. El problema es que este peligro atenta contra el derecho de no discriminación del usuario, y tendría que ser una obligación por imperativo legal, y no por opción de la empresa. Para concluir, habría que destacar el aumento de la concienciación social sobre los problemas en el uso de esta herramienta, y, que a la vez ha crecido la importancia de los problemas que esta herramienta produce, a medida que la IA adquiere un rol más relevante en la sociedad. A pesar de ello, todavía no estamos suficientemente preparados para afrontarlos, y tampoco estamos trabajando lo suficiente como para conseguirlo.

El tercer y último punto se enfoca en los dos principales deberes que tienen los Gobiernos. El primero es que deben enfrentar los problemas que no están contemplando de cara al futuro, y el segundo, que han de obligar a las empresas extranjeras que comercian en Europa a cumplir nuestra regulación, y que estas traten los datos de los ciudadanos de acuerdo a nuestra legislación, tanto fuera como dentro del territorio. Ante lo primero, ha quedado claro por parte de los profesionales en Big Data, que no se puede conocer con certeza qué problemas están por venir ante el avance de la tecnología, pero muchos de esos problemas ya están empezando a producir pequeñas consecuencias, que son suficientes como para empezar a prepararnos. Un método sería alentar a la creación de códigos deontológicos. Obligar a imponer estos códigos podría ser una intromisión en la ética y privacidad de las compañías, como muchos entrevistados explicaban, pero una alternativa más respetuosa para las compañías, podría ser la creación de campañas y recompensas públicas (como por ejemplo beneficios fiscales), para promover la creación de estos manuales de conducta. El segundo punto es más simple, y es que, si los Gobiernos

europeos cumplen con su obligación moral de que la legislación defienda los intereses del ciudadano de manera efectiva, deberán obligar a los competidores extranjeros a que también lo hagan cuando comercien en Europa, para evitar ventajas competitivas injustas e inmorales. De esta manera conseguiríamos una protección efectiva de los derechos del usuario, y conseguiríamos una competencia más justa.

En un medio plazo, posiblemente nuestra capacidad de procesar información se incremente de gran manera, basándonos en que la capacidad para procesar datos se duplica cada dos años. Para manejar estos grandes volúmenes de datos, las soluciones que nos puede brindar el Big Data cada vez son más, y más útiles. Justo por todas estas razones, los ciudadanos debemos de seguir luchando por conseguir un mejor servicio y una mayor transparencia por parte de los Gobiernos, entes públicos y grandes organizaciones, que utilizan nuestra información personal como activos, y la aprovechan para obtener beneficios. Tras haber analizado los mayores peligros que el Big Data entraña, creo que es clave remarcar que con los derechos de los ciudadanos no se negocia, se legisla.

BIBLIOGRAFÍA:

Accenture, (2021). *El futuro de los negocios 2021: Señales de cambio.* Accenture. Recuperado 12 de diciembre de 2021, de https://www.accenture.com/es-es/insights/consulting/business-change?c=acn_glb_businessfuturesgoogle_12345351&n=psgs_0721&gclid=Cj0KCQiA_c-OBhDFARIsAIFg3eyoRPQhZkfcdyxNwY9zuDnJHPwDB7WdgcTbnC6QJyQGd_gi61xrBqEaAnTtEALw_wcB.

Aced E.; Heras M.R. Sáiz C.A., (2018). *Código De Buenas Prácticas En Protección De Datos Para Proyectos Big Data.* Agencia Española de Protección de Datos (AEPD) y a la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain. Recuperado 3 de enero de 2022, de https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf.

AEPD, (2018). *La AEPD sanciona a WhatsApp y Facebook por ceder y tratar, respectivamente, datos personales sin consentimiento.* AEPD. Recuperado 14 de enero de 2022, de https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar.

AEPD, (2021). *Derecho de supresión («al olvido»): buscadores de internet.* AEPD. Recuperado 11 de enero de 2022, de https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido.

AEPD, (2021). *Historia de la Agencia Española de Protección de datos.* Protección de Datos Zaragoza RGPD. Recuperado 6 de enero de 2022, de https://www.portalartico.es/historia-de-la-agencia-espanola-de-proteccion-de-datos-aepd/#:%7E:text=La%20AEPD%20se%20cre%C3%B3%20en,propuesta%20del%20Ministro%20de%20Justicia.

Ayudaley, (2020). Big Data vs Business Intelligence ¿cuáles son sus diferencias? *Ayuda Ley Protección Datos.* Recuperado 1 de febrero de 2022, de https://ayudaleyprotecciondatos.es/big-data/business-intelligence/.

BBVA Data & Analytics, (2020). Implicaciones Éticas en el Uso de los Datos Personales. *BBVA AI Factory*. Recuperado 1 de enero de 2022, de https://www.bbvaaifactory.com/es/ethical-implications-of-personal-data-usage-from-corporations/.

BBVA.CH, (2021). Infografía: La importancia del Big Data. La inteligencia de los datos. *BBVA*. Recuperado 1 de enero de 2022, de https://www.bbva.ch/noticia/infografia-la-importancia-del-big-data/.

Blázquez, A., (2021). La revolución del Big Data en la gestión empresarial. Usos, ventajas y herramientas. *Novicap*. Recuperado 14 de marzo de 2022, de https://novicap.com/blog/la-revolucion-del-big-data-en-la-gestion-empresarial/.

Blog Interdominios, (2015) 10 tendencias en Big Data a tener en cuenta. *Blog Interdominios.* Recuperado 15 de diciembre de 2021, de https://blog.interdominios.com/10-tendencias-en-big-data-tener-en-cuenta/.

Byte Ti, R., (2017). Legal Data, la herramienta capaz de predecir los resultados de litigios. *Revista Byte TI*. Recuperado 1 de enero de 2022, de https://revistabyte.es/actualidad-it/legal-data-resultados-litigios/.

Calle, C., (2018). ¿Cómo aplicamos la ética al Big Data y la Inteligencia Artificial? *KPMG Tendencias*. Recuperado 25 de marzo de 2022, de https://www.tendencias.kpmg.es/2018/04/etica-big-data/.

Castillo, M., (2017). Cinco diferencias entre el Smart Data y el Visual Smart Data. *U The Valley*. Recuperado el 26/10/2021 de: https://thevalley.es/blog/5-diferencias-entre-smart-data-y-smart-visual-data/.

Ceupe, (2019). Por qué el Big Data es tan importante para las empresas. *Ceupe Magazine*. Recuperado 5 de diciembre de 2021, de https://www.ceupe.com/blog/por-que-el-big-data-es-tan-importante-para-las-empresas.html.

Comisión Europea para la Eficiencia de la Justicia, Carta ética europea, del 3 de diciembre de 2018, sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno; adoptado por el CEPEJ durante su 31º reunión plenaria el 4 de diciembre de 2018. Recuperado 25 de marzo de 2022 de https://campusialab.com.ar/wp-

content/uploads/2020/07/Carta-e%CC%81tica-europea-sobre-el-uso-de-la-IA-en-los-sistemas-judiciales-.pdf.

Constitución española, de 29 de diciembre de 1978, BOE núm.311 de 29 de diciembre de 1978. Recuperado 25 de marzo de 2022, de https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Crespo Mora, M. C., (2021). *La Protección del consumidor de servicios jurídicos.* Revista de Derecho Civil, VIII (núm. 1). Recuperado 25 de marzo de 2022, de file:///C:/Users/josej/Downloads/597-3191-1-PB.pdf.

Dat, G., (2019). Riesgos del Big Data: por qué implementar códigos de buena praxis. *Gesprodat.* Recuperado 14 de enero de 2022, de https://gesprodat.com/buenas-practicas-con-big-data/.

Datos.gob.es., (2017). La ética en la gestión de los datos. *Datos.gob.es.* Recuperado 18 de febrero de 2022, de https://datos.gob.es/es/noticia/la-etica-en-la-gestion-de-los-datos-0

De la Iglesia, E. D., (2021). Big Data ¿Solución o problema? *Big Data International Campus.* Recuperado 5 de enero de 2022, de https://www.campusbigdata.com/big-data-blog/item/81-bigdata-solucion-o-problema.

Del Rosal, P., (2018). Códigos éticos empresariales: ¿'postureo' o realidad? *El País.* Recuperado 14 de enero de 2022, de https://elpais.com/economia/2018/10/25/actualidad/1540464617_238582.html.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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 n° L 281 del 23 de noviembre de 1995 p. 0031 – 0050.

Drozhzhin, A., (2017). Errores del Big Data que debemos abordar. *Kaspersky daily.* Recuperado 11 de diciembre de 2021, de https://www.kaspersky.es/blog/nine-big-data-issues/8022/.

Dynamic, (2020). Historia del Big Data. *Dynamic*. Recuperado 4 de enero de 2022, de https://www.dynamicgc.es/historia-del-big-data/.

EALDE Business School, (2020*)*, 4 riesgos de Ciberseguridad de la tecnología Big Data. *EALDE Business School*. Recuperado el 27/11/2021 en: https://www.ealde.es/riesgos-big-data/.

Echarri, M., (2021). 150 despidos en un segundo: así funcionan los algoritmos que deciden a quien echar del trabajo. *El País.* Recuperado 10 de enero de 2022, de https://elpais.com/icon/2021-10-10/150-despidos-en-un-segundo-asi-funcionan-los-algoritmos-que-deciden-a-quien-echar-del-trabajo.html.

Economía 3, (2021). Big Data en el sector sanitario: Un desafío sin precedentes. *Economia3.* Recuperado 24 de marzo de 2022, de https://economia3.com/big-data-sector-sanitario/.

El Arass, M., & Souissi, N., (2018). *Data lifecycle: From big data to smartdata. In 2018 IEEE 5th international congress on information science and technology* (CiSt) (pp. 80-87). IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8596547&casa_token=cgfisYmjYpsAAAAA:ZVOw8se7zCLYyOE-9gfCe1tBv649FTnFPw5i2FimaWw69BFGOOmDDWzMaDvnzG6hCM77Opw&tag=1.

Eureka Marketing, (2021). Sobre la sociedad de la información y el Big Data. *Eureka Marketing*. Recuperado 19 de diciembre de 2021, de https://eurekamarketing.es/la-sociedad-la-informacion-big-data/.

Europa Press, (2017). La startup Legal Innovation lanza una herramienta para conocer y predecir los resultados y el tiempo de los litigios. *europapress.es.* Recuperado 25 de marzo de 2022, de https://www.europapress.es/andalucia/noticia-startup-legal-innovation-lanza-herramienta-conocer-predecir-resultados-tiempo-litigios-20170320104953.html.

Fernández, S., (2017). Smart Visual Data, un nuevo concepto de gestión empresarial. *elconfidencial.com.* Recuperado 7 de enero de 2022, de https://www.elconfidencial.com/empresas/2017-12-08/smart-visual-data-zeus-open-spaces-bra_1488519/.

Fernández-Lasquetty Quintana, J., (2020). Los datos son el petróleo del siglo XXI. *The Conversation.* Recuperado 2 de enero de 2022, de https://theconversation.com/los-datos-son-el-petroleo-del-siglo-xxi-139115#:%7E:text=Que%20los%20datos%20son%20el,que%20extraerlo%2C%20refinarlo%20y%20distribuirlo.

Fundación Teléfonica, (2020). Ética y Big Data. *Telos Fundación Teléfonica.* Recuperado 6 de enero de 2022, de https://telos.fundaciontelefonica.com/etica-y-big-data/.

García E., (2018) Tan solo el 35% de los ejecutivos confía en el uso que su compañía hace del análisis de datos. *Grupo de prensa de KPMG*. Recuperado el 28/11/2021 de https://home.kpmg/es/es/home/sala-de-prensa/notas-de-prensa/2018/06/ejecutivos-uso-comania-analisis-datos.html.

García-Gil, D., Luengo, J., García, S. y Herrera, F., (2019). Habilitación de datos inteligentes: filtrado de ruido en la clasificación de Big Data. *Ciencias de la información*. Recuperado el 28/11/2021 de https://arxiv.org/pdf/1704.01770.pdf.

Garriga Domínguez, A., (2020). *Reflections on political marketing and the phenomenon of disinformation in the electoral context*. Universidad de Vigo. Recuperado 12 de enero de 2022, de https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-F-2020-10025100287.

Gil, E., (2015). *Big data, privacidad y protección de datos.* Agencia Española de Protección de Datos. Recuperado 25 de marzo de 2022, de https://www.aepd.es/sites/default/files/2019-10/big-data.pdf.

Giner, G. J., (2018). Minería de Datos: ¿Qué relación tiene con el Big Data? *Revista Escuela de Negocios y Dirección*. Recuperado 20 de marzo de 2022, de https://www.escueladenegociosydireccion.com/revista/business/big-data/la-mineria-de-datos-en-el-big-data/#:%7E:text=El%20Big%20Data%20se%20centra,los%20grandes%20vol%C3%BAmenes%20de%20datos.

Glosario de las síntesis - EUR-Lex., (s. f.). Tribunales especializados. *EUR-Lex.* Recuperado 15 de enero de 2022, de https://eur-lex.europa.eu/summary/glossary/specialised_court.html?locale=es.

González, B. A., (s. f.). ¿Qué es Machine Learning? *Cleverdata.* Recuperado el 24 de marzo de 2022, de https://cleverdata.io/que-es-machine-learning-big-data/.

González, M., (2016). Este algoritmo sugiere a los jueces de EEUU qué condenas imponer, pero su código es un secreto. *Xataka.* Recuperado el 16/12/2021, de https://www.xataka.com/legislacion-y-derechos/este-algoritmo-sugiere-a-los-jueces-de-eeuu-que-condenas-imponer-pero-su-codigo-es-un-secreto.

González, B., (2021). *Luces y sombras de la nueva ley europea sobre inteligencia artificial.* UOC (Universitat Oberta de Catalunya). Recuperado 1 de enero de 2022, de https://www.uoc.edu/portal/es/news/actualitat/2021/192-ley-europea-inteligencia-artificial.html.

Google, (s. f.). *Política de Privacidad de Google*. Privacy & Terms" Google. Recuperado 9 de enero de 2022, de https://policies.google.com/privacy?hl=es.

Grupo de prensa de la Comisión Europea, (2021). Nuevas normas sobre la inteligencia artificial: preguntas y respuestas. *European Commission*. Recuperado 25 de marzo de 2022, de https://ec.europa.eu/commission/presscorner/detail/es/QANDA_21_1683.

Grupo de prensa de la Comisión Europea, (s. f.). El ABC del Derecho de la Unión Europea. *Comisión Europea*. Recuperado 25 de marzo de 2022, de https://op.europa.eu/webpub/com/abc-of-eu-law/es/.

Grupo de prensa del Parlamento Europeo, (2021). La protección de los valores del Artículo 2 del Tratado de la Unión Europea. Fichas temáticas sobre la Unión Europea. *Parlamento Europeo.* Recuperado 25 de marzo de 2022, de https://www.europarl.europa.eu/factsheets/es/sheet/146/la-proteccion-de-los-valoresdel-articulo-2-del-tratado-de-la-union-europea.

Hernández J. C.; Polanco Medina J., (2020). *Problemas ético-jurídicos de las decisiones algorítmicas y el Big data.* Revista de Humanidades Cuadernos del Marqués

de San Adrián, n.º 12, UNED Tudela. Recuperado 8 de diciembre de 2021, de https://qinnova.uned.es/archivos_publicos/qweb_paginas/111117433/articulo4problemaseticojuridicosdelasdecisionesalgoritmicasyelbigdat.pdf

Hernando, A., (2019). *Por qué debería preocuparte la ética de la inteligencia artificial.* Agencia SINC. Recuperado 8 de diciembre de 2021, de https://www.agenciasinc.es/Reportajes/Por-que-deberia-preocuparte-la-etica-de-la-inteligencia-artificial.

Herrero, T., (2018). La irrupción del Internet de las cosas. *KPMG Tendencias*. Recuperado 24 de marzo de 2022, de https://www.tendencias.kpmg.es/2016/04/la-revolucion-de-las-cosas/.

IKUSI, (2021*).* Aumento de ciberataques con la pandemia: ¿Cuál es la situación actual? *IKUSI velatia*. Recuperado 7 de enero de 2022, de https://www.ikusi.com/es/blog/aumento-de-ciberataques/.

ING, (2020). Historia del Big Data: un largo viaje poco conocido. *IGN - Soluciones de gestión para pymes*. Recuperado 5 de enero de 2022, de https://ignsl.es/historia-del-big-data/.

Intxusta A., (2020). ¿Por qué Google predecía la gripe y ahora no puede con el coronavirus? *Naiz.* Obtenido el 16/12/2021, de: https://www.naiz.eus/es/info/noticia/20200322/por-que-google-predecia-la-gripe-y-ahora-no-puede-con-el-coronavirus.

Jardine, J., Fisher, J. y Carrick, B., (2015). ¿Recopilación de datos inteligente para la era de los teléfonos inteligentes? *ResearchKit de Apple*. Recuperado 3 de enero de 2022, de: https://journals.sagepub.com/doi/pdf/10.1177/0141076815600673.

Jiménez, M., (2021*).* Las empresas aplauden que se regule la inteligencia artificial, pero alertan de su coste. *Cinco Días*. Recuperado 3 de enero de 2022, de https://cincodias.elpais.com/cincodias/2021/04/25/companias/1619371227_719934.html

Landi, L., (2022). ¿Qué porcentaje del conocimiento humano tiene una única persona? *Quo.* Recuperado 8 de enero de 2022, de https://quo.eldiario.es/curiosidades/q2201493211/que-porcentaje-del-conocimiento-

humano-tiene-una-unica-persona/#:%7E:text=En%20el%20gr%C3%A1fico%20de%202018,toneladas%20de%20datos%20al%20segundo.

Larson J., Mattu S., Kirchner L. and Angwin J., (2016*)*. How We Analyzed the COMPAS Recidivism Algorithm. *ProPublica*. Recuperado el 30/11/2021 en: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

León, E., (2020). Big Data: Últimas tendencias. *BAOSS*. Recuperado 5 de diciembre de 2021, de https://www.baoss.es/ultimas-tendencias-big-data-2021/.

Ley Orgánica 7/1998, de 13 de abril, sobre condiciones generales de la contratación, BOE núm. 89, del 14 de abril de 1998. Recuperado 5 de diciembre de 2021, de https://www.boe.es/buscar/doc.php?id=BOE-A-1998-8789

Ley orgánica 15/1999 del 13 de diciembre de Protección de datos de Carácter Personal, BOE, núm. 298 ,14 de diciembre de 1999. Recuperado 5 de diciembre de 2021, de https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Ley Orgánica 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y garantía de los derechos digitales, BOE, núm. 294, del 6 de diciembre de 2018. Recuperado 5 de diciembre de 2021, de https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Llamas, M., (2014). El «derecho al olvido» obliga a Google a convertirse en una herramienta de censura. *Libertad Digital*. Recuperado 25 de marzo de 2022, de https://www.libertaddigital.com/ciencia-tecnologia/internet/2014-05-14/el-derecho-al-olvido-obliga-a-google-a-convertirse-en-una-herramienta-de-censura-1276518559/.

López Escudero, M., (2008). Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo. *Fundación BBVA*. Recuperado 25 de marzo de 2022, de https://www.fbbva.es/wp-content/uploads/2017/05/dat/DE_2008_carta_drechos_fundamentales.pdf.

Maciejewski, D. G., (2021). ¿Pueden pensar las máquinas? De Alan Turing al big data. *Especial 21gramos*. Recuperado 14 de enero de 2022, de https://especial.21gramos.net/pueden-pensar-las-maquinas-de-alan-turing-al-big-data/.

Manceñido, Á., (2021). Nuevas obligaciones en camino para los entornos de IA: La Ley de Inteligencia Artificial. *KPMG Tendencias*. Recuperado 9 de enero de 2022, de https://www.tendencias.kpmg.es/2021/07/nuevas-obligaciones-camino-para-entornos-ia-ley-de-inteligencia-artificial/.

Marquez, N., (s. f.). Big Data y su efecto sobre la sociedad. *Tuatara Tech*. Recuperado 1 de marzo de 2022, de https://www.tuataratech.com/2016/09/big-data-y-su-efecto-sobre-la-sociedad.html.

Martín, E., (2021). Cómo ayuda el Big Data a convertir las ciudades en smart cities. *Cibernos*. Recuperado 2 de febrero de 2022, de https://www.grupocibernos.com/blog/como-ayuda-el-big-data-a-convertir-las-ciudades-en-smart-cities.

Martín, I., (2018). Futuro del Big Data – ¿Qué nos espera? *PublicaTIC.* Recuperado 1 de enero de 2022, de https://blogs.deusto.es/master-informatica/futuro-del-big-data-que-nos-espera/.

Masterlegal, (2020). *Multa a WhatsApp y Facebook en España por no cumplir la Ley de Protección de Datos - Protección de Datos.* Protección de Datos Zaragoza - RGPD, LOPD. Recuperado 22 de febrero de 2022, de https://maserlegal.es/redes-sociales/multa-a-whatsapp-y-facebook-por-proteccion-de-datos/.

Méndez, F., (2021). ¿Cómo el Big Data ayudó a Obama a ganar? *Forbes España*. Recuperado 14 de enero de 2022, de https://forbes.es/emprendedores/7560/como-el-big-data-ayudo-a-obama-a-ganar/.

Mitek, (2018). No todo son ciberataques: Los 5 principales riesgos del Big Data. *Mitek.* Recuperado 2 de enero de 2022, de https://www.miteksystems.com/es/blog/5-principales-riesgos-big-data.

Moreno, A., (2016). *El análisis automático de texto con Big Data e Inteligencia Artificial.* Instituto de Ingeniería del Conocimiento. Recuperado 12 de febrero de 2022, de https://www.iic.uam.es/inteligencia/analisis-automatico-de-texto-con-big-data/.

Nieto, A., (2016). Discriminados y marginados por el Big Data. *Xataka*. Recuperado el 16/12/2021, de https://www.xataka.com/otros/discriminados-y-marginados-por-el-big-data.

Niño, M & Illarramendi, A., (2015*). Entendiendo el Big Data: antecedentes, origen y desarrollo posterior*. DYNA New Technologies, 2(1), 8-p. Recuperado 25 de diciembre de 2021: http://www.mikelnino.com/2015/12/articulo-big-data-antecedentes-origen-desarrollo.html

Noain Sánchez, A., (2016). *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014).* AEPD. Recuperado 25 de diciembre de 2021, de https://www.aepd.es/sites/default/files/2019-10/la-proteccion-de-la-intimidad.pdf.

Parlamento Europeo, (s. f.). *Procedimiento legislativo ordinario.* Parlamento Europeo. Recuperado 14 de enero de 2022, de https://www.europarl.europa.eu/infographic/legislative-procedure/index_es.html.

Pastor. J., (2018). El escándalo de Cambridge Analytica resume todo lo que está terriblemente mal con Facebook. *XATAKA*. Recuperado el 28/11/2021 de https://www.xataka.com/privacidad/el-escandalo-de-cambridge-analytica-resume-todo-lo-que-esta-terriblemente-mal-con-facebook.

Patiño L., (2019). Las claves para entender el escándalo por el que multaron a Facebook. *El Tiempo.* Recuperado el 01/12/2021 de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/que-fue-y-por-que-es-importante-el-escandalo-de-cambrige-analytica-392368.

Pérez, E., (2019). Nos monitorizan y supervisan robots»: Amazon despide a miles de trabajadores por no cumplir con las cuotas. *Xataka.* Recuperado 11 de enero de 2022, de https://www.xataka.com/legislacion-y-derechos/nos-monitorizan-supervisan-robots-amazon-despide-a-miles-trabajadores-no-cumplir-cuotas-productividad.

PowerData, (s. f.). Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad. *PowerData.* Recuperado 13 de marzo de 2022, de https://www.powerdata.es/big-data.

Real Decreto 1720/2007, de 21 de diciembre, de protección de datos de carácter personal, BOE, núm. 17, de 19 de enero de 2008, Recuperado 24 de marzo de 2022 de https://www.boe.es/buscar/act.php?id=BOE-A-2008-979.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. BOE núm. 287 del 30 de noviembre de 2007. Recuperado 24 de marzo de 2022 de https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555.

Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. BOE núm.183, de 30 de julio de 2018. Recuperado 24 de marzo de 2022 de https://www.boe.es/buscar/doc.php?id=BOE-A-2018-10751.

Redacción España, (2019). ¿Qué es Dark Data o datos oscuros? *Blog de B12 admark.* Recuperado 24 de marzo de 2022, de https://agenciab12.com/noticia/que-es-dark-data-datos-oscuros.

Reglamento 2016/679. Del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE, núm.119, del 4 de mayo de 2016. Recuperado 24 de marzo de 2022 de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Renter Barcelona, A. M., (2020). La primera ley de privacidad en línea de EE.UU. entra en vigor en California. *La Vanguardia.* Recuperado 1 de marzo de 2022, de https://www.lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html.

Sánchez, A., (2020). ¿Por qué es importante Big Data? *Data IQ.* Recuperado 1 de enero de 2022, de https://dataiq.com.ar/blog/por-que-es-importante-big-data/.

Serrano, A., (2020). El gran auge del Big Data: repaso desde los inicios hasta hoy. *Infografía, Ideas para tu Empresa.* Recuperado 26 de noviembre de 2021, de https://ideasparatuempresa.vodafone.es/big-data-desde-los-inicios-hoy/.

Sierra, Y., (2019). Análisis big data: su futuro será mejor de que lo que imaginas. *MEDIACLOUD*. Recuperado 17 de diciembre de 2021, de https://blog.mdcloud.es/analisis-big-data-nuevas-corrientes/.

State vs Loomis (2016) 881 NW2d 749. Recuperado el 17 de diciembre de 2021 de: https://harvardlawreview.org/2017/03/state-v-loomis/

Stranieri, S., (2021). Leyes globales de privacidad de datos: USA, UE, China y más. *Progress*. Recuperado 1 de marzo de 2022, de https://www.ipswitch.com/es/blog/leyes-globales-de-privacidad-de-datos-usa-ue-china-y-mas.

Suarez, M., (2020). Big data y ética: ¿Qué condicionantes tiene la privacidad de las personas? *Clase Ejecutiva UC.* Recuperado 5 de enero de 2022, de https://www.claseejecutiva.uc.cl/blog/articulos/big-data-y-etica-que-condicionantes-tiene-la-privacidad-de-las-personas/.

Tablado, F., (2021). Guía sobre la privacidad digital. *Grupo Atico34.* Recuperado 5 de enero de 2022, de https://protecciondatos-lopd.com/empresas/privacidad-digital/.

Tratado de la Unión Europea, firmado en Maastricht el 7 de febrero de 1992. Diario Oficial de la Unión Europea L 191, 29 de julio de 1992. Recuperado 5 de enero de 2022, de https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002.

Tribunal Constitucional. Sentencia núm 292/2000, del 30 de noviembre. Recuperado el 15/12/2021 de http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276.

Tribunal de Justicia de la Unión Europea, asunto C-131/12, del 13 de mayo de 2014, Recuperado el 15/12/2021 de https://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf.

Triguero, I., García-Gil, D., Maillo, J., Luengo, J., García, S., & Herrera, F., (2019). *Transforming big data into smart data: An insight on the use of the k-nearest neighbors algorithm to obtain quality data.* Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(2), e1289. file:///C:/Users/josej/Downloads/Triguero_et_al-2018-

Wiley_Interdisciplinary_Reviews_3A_Data_Mining_and_Knowledge_Discovery(1)%20(1).pdf .

ANEXOS

Cuestionario nº1

Para empezar el cuestionario, querría que me contase cuál es su profesión, qué labores desempeña y en cuáles de sus tareas diarias está implicado el uso del Big Data. (Es importante que diga los años que lleva en este campo, y qué relación tiene su trabajo con el Big Data).

Abogado, Economista y Formador Business Intelligence. Licenciado en Administración y Dirección de Empresas, Abogado ejerciente y Controller CCA Certificate, formador de Busines Intelligence. Más de 20 años de experiencia en el sector de servicios profesionales. En la actualidad trabajo en proyectos de Analítica Avanzada de Negocio, con Microsoft Power BI, Power Automate y Power Apps, Machine Learning con Python así como Azure Machine Learning Studio. Ponente en el Festival Internacional de Microsoft sobre Inteligencia Artificial (FIAN).

1. **¿Usted cree que los ciudadanos leen y entienden las condiciones que aceptan, sobre la recolección y uso de datos personales, que se les pide en los contratos y términos de uso, tanto digitales como físicos?**

No. Se trata de una materia de no fácil comprensión para los no juristas.

2. **¿Cree que los datos que se recopilan diario son destinados solamente para los fines que contemplan en las cláusulas de términos de uso?**

No podemos saber si eso es cierto, sin embargo, la cantidad de llamadas, mails y otro tipo de comunicaciones que se reciben a diario de empresas desconocidas por el usuario, hace pensar que deberían mejorarse los protocolos de seguridad del dato.

3. **¿Le parece que la información que se usa a diario, es supervisada adecuadamente? ¿Se garantiza que la información que usan los algoritmos está libre de sesgos que puedan producir situaciones discriminatorias?**

En mi opinión, la información que usa un algoritmo nunca podrá estar libre de sesgos. En Machine Learning el Error está formado por tres partes:

- Error irreductible. El porcentaje de error que jamás podrás reducir
- Sesgo, que tiene que ver con los datos de muestra que se le pasan al algoritmo.
- Varianza, que sería la dispersión de las predicciones sobre el dato real que finalmente se ha dado.

No existe el dataset perfecto, con lo cual siempre existirá algún sesgo en el algoritmo, si bien es cierto, que es nuestra obligación tener controlado el sesgo existente e intentar reducirlo con el tiempo.

4. **¿Cómo puede defenderse el ciudadano ante las situaciones discriminatorias que producen los sesgos en la información que usan las herramientas de Big Data?**

El concepto Big Data, en mi opinión se refiere, entre otras características, al almacenamiento de gran cantidad de datos, y esto no puede más que ayudar a reducir el sesgo en los algoritmos. A mayor cantidad de variables podremos encontrar mayor cantidad de patrones distintos.

El problema de discriminación, sobre el que entiendo que preguntas, se da más ante la utilización de algoritmos Deep Learning, que suelen tener gran capacidad predictora, pero de difícil demostración, se les suele llamar algoritmos de caja negra precisamente por eso.

5. **¿Qué opinión general le merece la legislación vigente en materia de protección de datos?**

Creo que existe una buena regulación sobre la protección de datos, el problema es que es de difícil y costoso cumplimiento.

6. **¿Usted cree que dicha legislación afecta a la competitividad de las empresas europeas frente a las asiáticas y las americanas?**

Con respecto a la inteligencia artificial, los mercados asiáticos y americanos están más preocupados por la productividad que por la regulación, en contraposición con la legislación europea, y en concreto la española, que es excesivamente burocrática y eso por supuesto que afecta a la competitividad.

7. **¿En su compañía existe algún tipo de código deontológico (o manual de conducta) para los encargados de recolección y gestión de datos y los especialistas en Big Data?**

Solo la pertinente a LOPD, que, de forma transversal, aunque no específica afecta a la materia.

8. **¿Cree usted que sería útil que el Gobierno obligase a tener uno a todas las empresas?**

La PYME española necesita reducir costes para hacerse más competitiva. No creo que fuera eficiente cargar este tipo de obligaciones, donde si regularía está obligación sería para Grandes Empresas.

9. **¿En qué puntos deberían hacer hincapié dichos códigos y manuales?**

No respondió.

10. **¿Cuáles son los peligros más serios que ve en el uso del Big Data y la Inteligencia Artificial? ¿Cree usted que estamos preparados para afrontarlos?**

No sabemos que nos deparará el futuro en cuento a la Inteligencia Artificial, por supuesto, que traerá grandes cambios, muchos para mejor y algunos a peor. Esto no es distinto que cuando aparecieron otros inventos de gran calado en la humanidad.

11. **Y de cara al futuro, ¿Qué nuevos retos deberemos afrontar? ¿Y qué deberían hacer las autoridades al respecto, para prepararnos ante estos nuevos peligros?**

Me remito a la respuesta anterior.

12. **¿Conoce la nueva propuesta de la Comisión Europea sobre la nueva ley de Inteligencia Artificial? Si es así, ¿qué opina sobre ella?**

Si, mi opinión personal, la regulación europea viene como respuesta al retraso tecnológico que llevamos en Europa, que deja ver que somos los últimos en cuanto a desarrollos en Inteligencia Artificial y que por lo tanto se han centrado en ver los problemas que pueden surgir de tecnologías que están dominando otros mercados.

Esto no quiere decir que no vea bien, que la UE sea la primera que esté poniendo coto y regulando estos peligrosos algoritmos de caja negra, si bien, me gustaría que no solo fuéramos buenos regulando sino también creando tecnología.

13. **Si usted pudiera participar en la formulación de dicha ley, ¿qué debería incluir?**

No respondió.

Cuestionario nº2

Para empezar el cuestionario, querría que me contase cuál es su profesión, qué labores desempeña y en cuáles de sus tareas diarias está implicado el uso del Big Data. (Es importante que diga los años que lleva en este campo, y qué relación tiene su trabajo con el Big Data).

Yo soy director del área de data analytics, en una empresa de consultoría, para hacer productos de tecnología y desarrollo de sistemas. Tengo dos responsabilidades principales, una en oferta de servicios de valor, en plataformas de datos, para las grandes compañías, relacionada con las plataformas de datos. Estas plataformas de datos son la base tecnológica sobre la que luego se desarrollan diferentes soluciones de datos. Esta tecnología es el fundamento del software base que se utiliza para desarrollar después todas las bases de datos. La otra parte de mis responsabilidades son en operaciones, que son proyectos propiamente dicho en clientes. Yo llevo proyectos de clientes en el sector de industria, y me encargo principalmente de la oferta de valor.

1. **¿Usted cree que los ciudadanos leen y entienden las condiciones que aceptan, sobre la recolección y uso de datos personales, que se les pide en los contratos y términos de uso, tanto digitales como físicos?**

Un amplio porcentaje de la gente es consciente de que las empresas se están aprovechando de sus datos de alguna manera. No son conscientes de lo que están cediendo al aceptar las cookies o términos y condiciones. No saben cómo se usan sus datos, pero sí que presuponen que se están aprovechando de esos datos.

Europa está lanzando legislaciones muy estrictas y garantistas para el uso del dato y la IA. En cambio, EEUU es justo lo contrario, y ha dado muchísima libertad a las empresas de su país. Y por último el resto de grandes potencias, en donde el uso de datos de sus ciudadanos está más dirigido al control. En EEUU y España los datos principalmente se orientan a monetizar al usuario en términos monetarios.

2. **¿Cree que los datos que se recopilan diario son destinados solamente para los fines que contemplan en las cláusulas de términos de uso?**

Cuando los reguladores dan a este tipo de legislación, las compañías acaban descubriendo como conseguir que esto no afecte a sus fines e intenciones. En Europa, en donde hay una legislación muy estricta, las compañías siguen aprendiendo como conseguir sus fines comerciales. Hay ciertas líneas rojas que en general se respetan, porque de lo contrario podrían encontrarse una serie de conflictos innecesarios, ya que pueden monetizar los datos de los usuarios sin tener que romper la ley. A pesar de ello los usuarios, en vías generales, no son capaces de llegar a desentrañar todo lo que ponen en este tipo de contratos.

3. **¿Le parece que la información que se usa a diario, es supervisada adecuadamente? ¿Se garantiza que la información que usan los algoritmos está libre de sesgos que puedan producir situaciones discriminatorias?**

No sabría decir si el regulador tiene los mecanismos adecuados para garantizar un control adecuado, pero diría que no, en mi opinión.

Y respecto al segundo punto, en el tema de la analítica y los algoritmos, sobre todo en España, en donde el nivel es muy bajo. En España todavía no se ha afrontado el problema, y estamos en un nivel de madurez anterior. Estamos afrontando problemas anteriores, sobre todo de ingeniería del software, que está solucionando problemas previos a poder enfrentar los sesgos.

4. **¿Cómo puede defenderse el ciudadano ante las situaciones discriminatorias que producen los sesgos en la información que usan las herramientas de Big Data?**

No he llegado a afrontar este problema en el mercado, pero la única vía que encuentro es que las personas voten opciones políticas que aboguen por esta causa. En mi opinión, las opciones políticas que más pueden solucionar esta situación, y garanticen un uso adecuado de los datos, serían aquellos partidos que no antepongan la economía a las personas. De lo contrario encontramos situaciones como el EEUU, en donde rige una regulación mucho más laxa, algo que se debe a que es un país neoliberal.

5. **¿Qué opinión general le merece la legislación vigente en materia de protección de datos?**

Yo creo que en España tenemos un histórico en protección de datos bastante bueno, siguiendo el ejemplo de las regulaciones europeas, las cuales han sido siempre muy rigurosas. Ahora mismo en España estamos ante un pequeño colapso legislativo, debido a un sector público hipertrofiado, pero en mi opinión personal prefiero estos modelos, a cualquier otro que no respete los derechos fundamentales.

6. **¿Usted cree que dicha legislación afecta a la competitividad de las empresas europeas frente a las asiáticas y las americanas?**

Totalmente, pues como ya hemos comentado, cuanto más atas las manos a las empresas, más dañas a la competitividad. En el dilema de anteponer los ciudadanos a la economía, ya que, al fin y al cabo, los ciudadanos viven de la economía, y por lo tanto no debemos centrarnos en atar en exceso a las empresas, pues los ciudadanos serían los primeros en resentirse. La clave está en encontrar un balance.

7. **¿En su compañía existe algún tipo de código deontológico (o manual de conducta) para los encargados de recolección y gestión de datos y los especialistas en Big Data?**

No tenemos un código deontológico propiamente dicho, pero nosotros no violamos las leyes existentes. Nosotros trabajamos para grandes empresas, y a mí nunca me han pedido que viole una ley. En ocasiones hemos podido afrontar situaciones poco éticas, pero jamás violar la ley. Trabajamos con toda una oferta de servicios que ofrecemos a nuestros clientes, y que cumplen por completo con la ley.

8. **¿Cree usted que sería útil que el Gobierno obligase a tener uno a todas las empresas?**

No creo que sea cuestión de un código deontológico. Yo creo que la legislación es la clave para solucionar este problema, y en general creo que vamos en un buen camino, y las empresas van a respetar la ley. El conflicto entra en el momento en que cuando hay un ánimo de lucro, que acabará produciendo una falta de ética. Y a pesar de que no incumplamos la ley, sí que podemos romper con el fin de la ley, pero en mi opinión personal creo que eso es inevitable cuando hay una situación en donde hay intereses lucrativos de por medio.

9. **¿En qué puntos deberían hacer hincapié dichos códigos y manuales?**

Volvemos a la pregunta anterior.

10. **¿Cuáles son los peligros más serios que ve en el uso del Big Data y la Inteligencia Artificial? ¿Cree usted que estamos preparados para afrontarlos?**

Dos grandes peligros. El primero es el control social, debido a que ahora mismo, las compañías tecnológicas saben muchísimo de nosotros, lo que se puede utilizar para monetizarnos, pero en algunos países se usa para el control social. Esto mismo nos muestra que si en Europa o EEUU la situación política fuera a peor, nadie nos garantiza de que esos datos no se puedan utilizar para controlarnos. No sería la primera vez, como pasó en Holanda en los años 40, con el registro de religiones, que acabó siendo utilizado por los nazis para los campos de exterminio.

Hay otro riesgo, que es el uso de la tecnología pueda llegar a ser un problema de salud pública, en la sociedad en general y en la juventud e infancia en especial. Está empezando a producir comportamientos adictivos, y difíciles de controlar.

11. **Y de cara al futuro, ¿Qué nuevos retos deberemos afrontar? ¿Y qué deberían hacer las autoridades al respecto, para prepararnos ante estos nuevos peligros?**

Que toda esta información obtenida de los individuos no se dirija a controlar a las personas, y controlar los nuevos comportamientos aditivos de los usuarios, en especial en los menores.

12. **¿Conoce la nueva propuesta de la Comisión Europea sobre la nueva ley de Inteligencia Artificial? Si es así, ¿qué opina sobre ella?**

En todo el texto, cuando hacía hincapié en la regulación actual, en especial me refería a esta.

13. **Si usted pudiera participar en la formulación de dicha ley, ¿qué debería incluir?**

No la conozco lo suficiente.

Cuestionario nº3

Para empezar el cuestionario, querría que me contase cuál es su profesión, qué labores desempeña y en cuáles de sus tareas diarias está implicado el uso del Big Data. (Es importante que diga los años que lleva en este campo, y qué relación tiene su trabajo con el Big Data).

En mi vida profesional, antes del cargo que ostento a día de hoy, tuve otro trabajo relacionado con este campo:

Trabajo 1. En mi primer trabajo, como becaria, me dediqué a tareas relacionadas con la protección de datos y la propiedad intelectual del sector audiovisual.

Trabajo 2. Mi labor actual consiste en el uso de los datos internos de una compañía para construir bases de datos y algoritmos de automatización para uso interno que supone matchear necesidades de clientes o intereses de potenciales clientes con recursos internos de la empresa. Además, también se genera documentación varia, que se automatizada en la medida de lo posible. Todo esto en el ámbito legal.

Para encontrar posibles clientes y datos de los mismos se emplea webscraping para obtener bases de datos masivos que luego se limpiarían.

1. **¿Usted cree que los ciudadanos leen y entienden las condiciones que aceptan, sobre la recolección y uso de datos personales, que se les pide en los contratos y términos de uso, tanto digitales como físicos?**

No, sin duda las personas aceptan únicamente porque consideran que la cesión de sus datos es un mal menor que hay que sufrir para acceder a cosas que quieren. Especialmente, cuando son contratos online no se leen, ya que la velocidad del mundo virtual es tal que pararse a leer tantas condiciones, cuando estamos acostumbrados a obtener en un clic a lo que queremos supone un porcentaje de tiempo muy elevando de nuestro tiempo en la página de que se trate. O porque nos hemos convencido de que no podemos no tener ciertas cuentas en redes sociales porque eso empeoraría nuestra calidad de vida.

En contratos físicos tampoco se leen mucho, pero sí que se observan más. Cuando pasábamos las nuevas cláusulas de PPDD a los empleados que no trabajaban presencialmente en la empresa en mis prácticas respondían afirmativamente de forma instantánea, sin embargo, aquellos que firmaban en papel lo pensaban más, porque la poca costumbre de tener contratos físicos en nuestras manos y el respeto que generan en los firmantes hacía que se sintieran "mal" si no leían, aunque fuera por encima y sin entender realmente el contenido.

2. ¿Cree que los datos que se recopilan diario son destinados solamente para los fines que contemplan en las cláusulas de términos de uso?

En muchas ocasiones no, pero estos casos, creo que cada vez son los menores. No obstante, sí que a veces las empresas estudian y ponen en la balanza: las posibilidades de que les multen porque alguien denuncie, la posible multa y los posibles beneficios que obtendría, y si lo último supera lo anterior, se lanzan.

Las empresas, para evitar las multas de PPDD incluyen un clausulado muy extenso, a propósito, en ocasiones que no se pueda comprender bien por los ciudadanos de a pie, e incluyen clausulas genéricas con las que prácticamente pueden justificar cualquier uso que le den posteriormente.

En mi primera experiencia profesional, cuando teníamos que incluir cláusulas de PPDD subcontrataban una empresa especialista que garantizase el cumplimiento, y se responsabilizase del incumplimiento. Por lo tanto, están surgiendo agentes especializados en que las empresas cumplan. Cuando empiezan a surgir esta clase de agentes en cualquier ámbito acaba suponiendo que algunas empresas, que quieren maximizar beneficios, ofrezcan prácticas más baratas al límite de lo legal.

3. **¿Le parece que la información que se usa a diario, es supervisada adecuadamente? ¿Se garantiza que la información que usan los algoritmos está libre de sesgos que puedan producir situaciones discriminatorias?**

Las grandes empresas sí que están tratando de eliminar los sesgos en el uso de sus algoritmos por Compliance. Sin embargo, todo el mundo prueba el mejor algoritmo posible, y luego le elimina el sesgo entonces, aunque el algoritmo ya no esté sesgado, sí que la persona que lo controla lo esté.

Además, las empresas, al personalizar mucho los algoritmos, pueden no sesgar de forma directa el algoritmo pero que el mismo se acabe sesgando sin repercusiones, y, a mi juicio, tampoco es malo que los algoritmos se personalicen mucho, si generan beneficios para la empresa y para el usuario, aunque esto suponga un sesgo indirecto, que es fruto de que realmente cada persona sigue unos patrones de comportamiento.

4. ¿**Cómo puede defenderse el ciudadano ante las situaciones discriminatorias que producen los sesgos en la información que usan las herramientas de Big Data?**

Los ciudadanos pueden:

1. No aceptar indiscriminadamente las condiciones de uso, leerlas si es posible, y sino rechazarlas o marcar las mínimas.

2. Usar navegación privada.

3. Cuidar las páginas en las que entran y valorar la necesidad que tienen de acceder, al final se pueden obtener los mismos servicios de muchas formas, no tenemos que usar necesariamente las mismas páginas que se suelen usar.

4. Ser cuidadoso cuando proporciona datos personales.

5. Cancelar la suscripción cuando tema por el uso de sus datos, o cuando ya simplemente ya no le interese que una página tenga sus datos y solicitar por escrito la eliminación de sus datos personales.

5. **¿Qué opinión general le merece la legislación vigente en materia de protección de datos?**

Considero que es bastante exhaustiva y prevé unas sanciones muy elevadas, creo que en ocasiones es demasiado proteccionista con los usuarios, de forma que lo que genera es que las empresas acaben generando las interminables cláusulas que generan y que se aceptan sin pensar. Además, realizar una legislación para usuarios y redactarla como está redactada en lugar de leyes de fácil comprensión, es poco útil. Creo que deberían hacer una legislación más sencilla, más corta, más directa, y que sea realmente beneficiosa para las personas no obligando a las empresas a generar enormes clausulados, que a la empresa le supone una simple mañana de trabajo, y provocan que el ciudadano no lo lea realmente.

6. **¿Usted cree que dicha legislación afecta a la competitividad de las empresas europeas frente a las asiáticas y las americanas?**

Probablemente si, ya que se exige afrontar los costes de adaptarse y mantener correctamente los datos a las empresas que operan con los datos en Europa. Sin embargo, como la legislación afecta a quien opera en Europa y no a quien es europeo, y con las nuevas tecnologías cada vez es más complejo saber dónde se generan las operaciones realmente, así que para competir en Europa las empresas tendrán que cumplir los mismos estándares. Así que afecta, pero no tanto como parece a priori.

7. **¿En su compañía existe algún tipo de código deontológico (o manual de conducta) para los encargados de recolección y gestión de datos y los especialistas en Big Data?**

No había dicho Código, se subcontrataba todo en el primer trabajo. En mi actual trabajo sí que hay dicho código y se forma al personal en la materia.

8. **¿Cree usted que sería útil que el Gobierno obligase a tener uno a todas las empresas?**

No, creo que sería una intromisión de la Administración muy grande. La ética no debe ser objeto de la ley. Si la ética de la compañía es buena o mala según el mercado, este debe manifestarlo demandando más o menos sus productos, pero no es algo en lo que deba meterse el Estado.

Sin embargo, si se manejan datos personales sensibles, si creo que es necesario que se exija por ley un profesional, porque el coste para las personas de un mal uso es excesivo.

9. **¿En qué puntos deberían hacer hincapié dichos códigos y manuales?**

Si se hicieran los manuales deberían incidir en la transparencia y facilidad de información para los usuarios, y en la formación del personal de la empresa, ya que son quienes manejan los datos.

10. **¿Cuáles son los peligros más serios que ve en el uso del Big Data y la Inteligencia Artificial? ¿Cree usted que estamos preparados para afrontarlos?**

El excesivo control de las personas por parte de las empresas y Estados, y los problemas psicológicos que cada vez más vemos que generan. Estos problemas son tanto el miedo de estar en constante vigilancia, así como los problemas de autoestima y soledad que provocan los dispositivos electrónicos y la información constante que nos hace creer que siempre necesitamos más para ser felices, o que nuestra vida siempre podía ser mejor con algo nuevo, en lugar de fomentar aprovechar lo que tenemos. La sociedad no está aún preparada.

11. **Y de cara al futuro, ¿Qué nuevos retos deberemos afrontar? ¿Y qué deberían hacer las autoridades al respecto, para prepararnos ante estos nuevos peligros?**

El estado tiene que facilitar el acceso psicológico gratuito, y educación desde la infancia en el correcto uso de la tecnología y enseñar a los niños a hablar de sus problemas y sus dudas, sin que vean la psicología como un tema tabú. Además, creo que más que castigar a empresas, deberían ayudar a las empresas que proporcionan beneficios reales a la sociedad en este ámbito.

12. **¿Conoce la nueva propuesta de la Comisión Europea sobre la nueva ley de Inteligencia Artificial? Si es así, ¿qué opina sobre ella?**

No la conozco.

13. **Si usted pudiera participar en la formulación de dicha ley, ¿qué debería incluir?**

Como mencionaba creo que cada ley tiene que centrarse mucho en la educación social, y laboral.

Cuestionario nº4[1]

Para empezar el cuestionario, querría que me contase cuál es su profesión, qué labores desempeña y en cuáles de sus tareas diarias está implicado el uso del Big Data. (Es importante que diga los años que lleva en este campo, y qué relación tiene su trabajo con el Big Data).

Mi trabajo está vinculado al dato desde hace más de 25 años, en este momento pertenezco a YY y a UU España (https://www.damaspain.org/), en esta última estoy como coordinador del equipo de Modelado y BI y perteneciente a la Junta Directiva de YY España. En este instante estoy desempeñando labores de Product Owner en un cliente para la empresa en la que desempeño mi actividad profesional y coordinando acciones orientadas al dato, proponiendo y abordando soluciones de analítica, big data y en estadíos primigenios, modelización y BI.

1. **¿Usted cree que los ciudadanos leen y entienden las condiciones que aceptan, sobre la recolección y uso de datos personales, que se les pide en los contratos y términos de uso, tanto digitales como físicos?**

En mi humilde opinión, diría que un 10% de los usuarios puede llegar a entender y comprender las múltiples páginas de literatura extensa en la que se dice de forma para nada entendible que es lo que van a hacer con los datos personales.

2. **¿Cree que los datos que se recopilan diario son destinados solamente para los fines que contemplan en las cláusulas de términos de uso?**

Aunque se le supone que el uso real no debiera extrapolarse a lo indicado en los términos de uso, creo que existe la mala praxis en utilizar los datos en base a las necesidades del momento, ya que no hay ningún organismo que realmente vele por ello. Los datos al estar ya en los sistemas de información de quien provee el servicio, pueden operar de forma libre con la información en base a sus propios intereses.

[1] El entrevistado se olvidó de que el cuestionario debería ser anónimo, y por ello se nombra YY a la compañía en donde trabaja, y UU al proyecto en el que está trabajando.

3. **¿Le parece que la información que se usa a diario, es supervisada adecuadamente? ¿Se garantiza que la información que usan los algoritmos está libre de sesgos que puedan producir situaciones discriminatorias?**

Creo que nadie hace una supervisión de la información.

Estoy convencido que no existe esa garantía. Pongo un ejemplo que muchas personas que tienen más de 45 años viven día a día en portales de empleo como infojobs, en el que personas con la edad indicada o superior, son descartados en menos de 1 minuto desde que se realiza el postulado, con independencia a la hora que hagas la inscripción a la oferta.

4. **¿Cómo puede defenderse el ciudadano ante las situaciones discriminatorias que producen los sesgos en la información que usan las herramientas de Big Data?**

Muchas personas desconocen los trámites para poder proceder a denunciar a quienes están utilizando las herramientas de Big Data de forma inadecuada, por lo que no hay una defensa posible, además que tampoco existe una correcta legislación en la actualidad que permita este tipo de defensa. Deberá existir un cambio legislativo tanto a nivel nacional, europeo y mundial para conseguir que estas situaciones sigan produciéndose.

5. **¿Qué opinión general le merece la legislación vigente en materia de protección de datos?**

Ha mejorado mucho, pero le falta todavía dar mayores pasos de gigante, no es normal que los términos de uso ininteligibles sean un argumento para que quienes manejan los datos puedan hacer lo que les de la real gana con esa información. Creo que debiera haber unos mínimos que debieran estar preestablecidos y que fueran de obligado cumplimiento y que existieran herramientas al alcance de quienes legislan para poder realizar seguimiento y valoración del cumplimiento de la legislación, realmente utilizar IA por los legisladores para validar que realmente se cumplen las “reglas”.

6. **¿Usted cree que dicha legislación afecta a la competitividad de las empresas europeas frente a las asiáticas y las americanas?**

Creo que no, y de hecho que ellos tengan leyes más permisivas conlleva a que los derechos de las personas puedan verse afectados por ello, no quiero leyes permisivas que permitan que determinadas informaciones de las personas puedan ser manejadas al antojo de cualquiera.

7. **¿En su compañía existe algún tipo de código deontológico (o manual de conducta) para los encargados de recolección y gestión de datos y los especialistas en Big Data?**

Sí y se exige su cumplimiento al 100% se revisa su cumplimiento y se realizan auditorías.

8. **¿Cree usted que sería útil que el Gobierno obligase a tener uno a todas las empresas?**

No solamente el Gobierno de España, creo que debiera ser obligatorio como mínimo a nivel de Europa y exigir que quién quiera trabajar con Europa, lo cumpla.

9. **¿En qué puntos deberían hacer hincapié dichos códigos y manuales?**

No hay una reglamentación adecuada ni global para la utilización, deberían establecerse limitaciones en el uso para evitar sesgos y discriminaciones, así como el evitar la violación de aquellos datos que realmente corresponden a la intimidad y privacidad del ciudadano, y que la mala praxis tuviera penalizaciones extremas, pero no a nivel español, sino que también europeo y global. Pero los grandes lobbys impedirán esto, véase META de Mark Zuckerberg que quiere marcharse de Europa porque se le indica que no está utilizando de forma adecuada la información recopilada y que esta no puede llevársela dónde él quiera. Establecería un organismo independiente que hiciera la gestión y el almacenamiento de la información y que quien quisiera utilizar los datos existentes en dicho organismo, rellenar un formulario en el que indicara que información quiere procesar y el objetivo de dicho procesamiento. Al igual que sucede con el uso de

Internet y la gestión de la WWW (por ejemplo, el ICANN), entidades sin ánimo de lucro que hacen la correcta gestión y administración de los nombres de dominio y direcciones IP, para IA debiera existir un organismo encargado de gestionar la información y sus consumidores, responsabilizando a éstos de la utilización fraudulenta y/o incorrecta de la información.

10. **¿Cuáles son los peligros más serios que ve en el uso del Big Data y la Inteligencia Artificial? ¿Cree usted que estamos preparados para afrontarlos?**

Sesgos, por ejemplo, la utilización de IA en procesos de selección, en los que se discrimine por edad, raza, sexo o cualquier otro criterio que implica discriminaciones a las personas. No hay una reglamentación adecuada ni global para la utilización, deberían establecerse limitaciones en el uso para evitar sesgos y discriminaciones.

Espiar comportamientos de los usuarios que violen la intimidad, que accedan a derechos

Se está preparado pero los intereses económicos impedirán una correcta legislación y primarán los intereses de los lobbys sobre el de las personas.

11. **Y de cara al futuro, ¿Qué nuevos retos deberemos afrontar? ¿Y qué deberían hacer las autoridades al respecto, para prepararnos ante estos nuevos peligros?**

La creación de un organismo regulador que haga de controlador el uso de los datos y que gestione todo lo relativo a IA.

Formar a los usuarios en proteger la información que les concierne.

Utilizar el nuevo organismo regulador para que se controle la utilización de la información.

12. **¿Conoce la nueva propuesta de la Comisión Europea sobre la nueva ley de Inteligencia Artificial? Si es así, ¿qué opina sobre ella?**

Está ley como propuesta, le faltan muchos aspectos por reglar, y encima tal cual se describe, los términos existentes hacen que puedan existir agujeros legales en los que se podrían hacer acciones que permitieran hacer acciones en contra de los derechos personales e individuales de cada ciudadano.

13. **Si usted pudiera participar en la formulación de dicha ley, ¿qué debería incluir?**

Reglar incluso para personas con necesidades especiales, ayudar a personas a que puedan acceder a temas relacionados con sus datos e impedir que sus datos puedan pertenecer a esas bases de datos de IA.

Cuestionario nº5[2]

Para empezar el cuestionario, querría que me contase cuál es su profesión, qué labores desempeña y en cuáles de sus tareas diarias está implicado el uso del Big Data. (Es importante que diga los años que lleva en este campo, y qué relación tiene su trabajo con el Big Data).

Hace ya un año que me gradué del doble grado en derecho y análisis de datos. Estos últimos dos años, he podido trabajar en el sector del big data en dos empresas: El JJ y MM, medio año de prácticas en la primera, y otro medio año de prácticas y un año trabajando en la segunda.

En la primera, formaba parte del equipo de Gestión Regional y Estrategia de Cliente, siendo el soporte principal de los distintos centros comerciales que hay en España. Durante los 6 meses de prácticas tuve acceso a la base de datos de los clientes de la empresa en la que se veía toda la información relevante a su persona y a sus compras.

En la actual, mi labor consiste en la creación de un cuadro de mandos con Power BI teniendo acceso a la base de datos financiera de la empresa, con la idea de crear un panel en el que el director ejecutivo y el Equipo Financiero pudieran moverse con mayor facilidad que usan Excel y así mejorar las tomas de decisiones internas de la empresa.

1. ¿Usted cree que los ciudadanos leen y entienden las condiciones que aceptan, sobre la recolección y uso de datos personales, que se les pide en los contratos y términos de uso, tanto digitales como físicos?

Por supuesto que no, son textos muy largos y enrevesados cuya función principal es que no se lean y se acepten una vez salga la notificación

[2] El entrevistado se olvidó de que el cuestionario debería ser anónimo, y por ello se nombra MM a la compañía en donde trabaja actualmente, y JJ a la empresa donde realizó sus prácticas.

2. ¿Cree que los datos que se recopilan diario son destinados solamente para los fines que contemplan en las cláusulas de términos de uso?

En gran parte sí. Los datos recopilados por las empresas tienen dos funciones muy marcadas: uso interno de la compañía para futuras estrategias y su venta a otros entes.

3. ¿Le parece que la información que se usa a diario, es supervisada adecuadamente? ¿Se garantiza que la información que usan los algoritmos está libre de sesgos que puedan producir situaciones discriminatorias?

Actualmente toda información pasa unos mínimos de supervisión, ya sea por una máquina o por una persona ya que su uso es tan importante que si una empresa quiere tener resultados satisfactorios necesitan de esa supervisión.

Por otro lado, es inevitable que existan sesgos en el uso de los datos, pero ya no tanto que lleguen a situaciones discriminatorias (que no quiere decir que a veces ocurra), sino que hay sesgos necesarios que hacen que la predicción y el análisis de datos sea lo más correcto posible, como por ejemplo filtrar por la edad, el género, la ubicación…

4. ¿Cómo puede defenderse el ciudadano ante las situaciones discriminatorias que producen los sesgos en la información que usan las herramientas de Big Data?

Como ciudadano particular es muy difícil que pueda luchar contra este problema ya que no tiene poder suficiente para ello. Estos problemas deberían resolverse por medio de leyes y reglamentos que hagan del uso de datos un mundo más igualitario y sin discriminaciones absurdas por el simple hecho de que un ordenador lo decida, o incluso una persona.

5. ¿Qué opinión general le merece la legislación vigente en materia de protección de datos?

Debido a que el uso de datos ha sufrido una explotación masiva estos últimos años creo que todavía queda mucho por mejorar. Creo que lo que hay actualmente está muy logrado para los avances que hay día tras día en materia de datos.

Además, creo que también es importante, no solo la existencia de la ley de protección de datos, si no que sean los usuarios quienes mejoren su forma de utilizar las nuevas tecnologías y que no lo tomen como un simple aparato en el que buscan por internet y suben fotos si no que sea capaces de entender lo importante que es un simple *click* en una página web o una aplicación.

6. ¿Usted cree que dicha legislación afecta a la competitividad de las empresas europeas frente a las asiáticas y las americanas?

En el mundo tan globalizado y conectado en el que vivimos no creo que afecte. Muchas empresas que manejan esos datos aquí en Europa son empresas americanas. (Apple, Facebook, Microsoft) y viceversa (Inditex, Santander), por lo que es imposible pensar que hay situaciones muy claras de competitividad en ese sentido.

7. ¿En su compañía existe algún tipo de código deontológico (o manual de conducta) para los encargados de recolección y gestión de datos y los especialistas en Big Data?

Cuando estuve trabajando en JJ desde el primer día nos dejaron como usar los datos que usábamos, ya que era información personal del cliente tal como su nombre, dirección, género, edad, que ha comprado, cuando, donde …

Son datos muy sensibles que hay que tener cuidado a quien se le manda y como se le manda ya que teníamos la obligación de mandar los ficheros con contraseña y que su uso solo podía ser de un máximo de 3 semanas.

8. ¿Cree usted que sería útil que el Gobierno obligase a tener uno a todas las empresas?

Por supuesto, es la manera más fácil de evitar tener problemas legales y que, de alguna manera, ayuda a que su uso dentro de la empresa sea tan correcto que beneficie incluso a la misma a la hora de analizar y trabajar con ellos.

9. ¿En qué puntos deberían hacer hincapié dichos códigos y manuales?

Principalmente en el envío de los datos. El análisis de los datos en las empresas nunca es igual, si no que cada entidad decidirá trabajar con ellos como les convenga. Por otro lado, si una empresa decide enviar/vender esos datos es importante que pasen un filtro teniendo en cuenta a quien se le va a mandar y que uso le dará.

De esta manera conseguimos que el análisis de datos en las empresas sea limpio y correcto.

10. ¿Cuáles son los peligros más serios que ve en el uso del Big Data y la Inteligencia Artificial? ¿Cree usted que estamos preparados para afrontarlos?

Los únicos problemas que le puedo llegar a ver a todo este mundo es que se haga un mal uso y se llegue a traspasar la legalidad. Creo firmemente que son herramientas muy necesarias y que ayudan mucho al día a día de todo el mundo, pero son muy poderosas y es necesario que haya un control de que se hace y como se hace.

11.Y de cara al futuro, ¿Qué nuevos retos deberemos afrontar? ¿Y qué deberían hacer las autoridades al respecto, para prepararnos ante estos nuevos peligros?

La mejor forma de prepararnos ante esto (cosa que también es un reto) es la educación. Actualmente cualquier niño de 8 años sabe cómo funciona un móvil o una tablet pero no sabe que hay detrás de eso.

Veo necesario que se implementen asignaturas que te enseñen a entender y usar y conocer todo este mundo que cada vez va siendo más grande. Esto hace que sea necesario que existan expertos en la materia para poder regular y "usar" el Big Data.

12 ¿Conoce la nueva propuesta de la Comisión Europea sobre la nueva ley de Inteligencia Artificial? Si es así, ¿qué opina sobre ella?

Pienso que es un buen comienzo de regulación dentro del desconocimiento que hay detrás de la Inteligencia Artificial, pero pienso que intentan crear una ley al uso, cuando no puede ser así ya que de alguna manera lo que están intentando regular es el funcionamiento y uso de las máquinas mientras que las leyes clásicas afectan a las personas.

Por otro lado, pienso que hay un miedo excesivo a la Inteligencia Artifical por el exceso de series y películas de ciencia ficción que hablan de ellos y las usan como robots que acabarán dominando el mundo.

Es muy complicado conseguir una regulación perfecta teniendo en cuenta que se conoce muy poco al respecto ya que cada vez salen cosas nuevas y se van desarrollando nuevos algoritmos con nuevos usos.

13. Si usted pudiera participar en la formulación de dicha ley, ¿qué debería incluir?

Como dije antes, veo necesario un control en la entrega y venta de datos entre empresas, que no se vendan como si estuviésemos haciendo la compra si no con conciencia de que datos va a utilizar esa empresa y con qué fin.

Cuestionario nº6[3]

Para empezar el cuestionario, querría que me contase cuál es su profesión, qué labores desempeña y en cuáles de sus tareas diarias está implicado el uso del Big Data. (Es importante que diga los años que lleva en este campo, y qué relación tiene su trabajo con el Big Data).

Soy "Software Development Engineer III" en AA. Actualmente trabajo en el equipo del servicio "X".

X, para el usuario es como una base de datos, recibe SQL del usuario, genera un plan de ejecución para la consulta, y distribuye el trabajo entre muchos nodos que trabajan de forma coordinada para acceder a los datos que generalmente están almacenados en AA y responder a la consulta lo más rápido y eficientemente posible.

X es usado por miles de empresas alrededor del mundo para tratar y extraer información de grandes cantidades de datos. Esta información seria prácticamente imposible de extraer en un tiempo y coste razonable con una base de datos transaccional tradicional.

Actualmente trabajo implementando mejoras en el núcleo de X para que las consultas se ejecuten usando menos recursos y más rápido.

En el equipo de X usamos técnicas de Big Data nosotros mismos para entender mejor cómo los usuarios usan nuestro producto. Podemos extraer información como qué tipo de consultas son las más comunes, cuales las más lentas que debemos mejorar, etc…

[3] El entrevistado se olvidó de que el cuestionario debería ser anónimo, y por ello se nombra AA a la compañía en donde trabaja, FF la competencia y X al proyecto en el que está trabajando.

1. **¿Usted cree que los ciudadanos leen y entienden las condiciones que aceptan, sobre la recolección y uso de datos personales, que se les pide en los contratos y términos de uso, tanto digitales como físicos?**

Dudo mucho que los ciudadanos particulares en general lean y entiendan las condiciones de uso y privacidad.

Pese a esto, la mayoría de nuestros usuarios son grandes empresas, con requisitos de privacidad súper estrictos, y ellos, sí que obviamente revisan las condiciones de uso y privacidad.

Ningún ingeniero en AA es capaz de acceder a datos relativos a clientes de ninguna manera. Solo el cliente puede acceder a sus datos. Esto muchas veces dificulta nuestro trabajo a la hora de replicar problemas internamente. Pero realmente la privacidad es algo extremadamente crítico para nuestros clientes corporativos y para nosotros.

2. **¿Cree que los datos que se recopilan diario son destinados solamente para los fines que contemplan en las cláusulas de términos de uso?**

Pues esto dependerá altamente de la ética de la empresa que estes hablando. En AA somos super estrictos con los datos que recopilamos y solo recopilaremos lo mínimo e imprescindible para dar el mejor servicio al cliente. Esto es, ya que como plataforma de cloud usada por las más grandes empresas del mundo no nos podemos permitir filtrados de información, y escándalos que dañarían altamente la confianza que los clientes tienen hacia nosotros.

En cambio, si hablamos de una empresa como FF, estaríamos diciendo cosas muy distintas.

3. **¿Le parece que la información que se usa a diario, es supervisada adecuadamente? ¿Se garantiza que la información que usan los algoritmos está libre de sesgos que puedan producir situaciones discriminatorias?**

De nuevo, esto dependerá altamente de qué empresa estemos hablando. La mayor parte de grandes empresas que usan Big Data tienen actualmente una presión social muy grande para evitar situaciones discriminatorias que podrían dañar la imagen de la empresa.

Sin embargo, los startups más pequeños que están luchando por sacar un producto lo más rápido posible quizás cometan estos errores más habitualmente.

4. **¿Cómo puede defenderse el ciudadano ante las situaciones discriminatorias que producen los sesgos en la información que usan las herramientas de Big Data?**

No creo que el ciudadano tenga demasiadas opciones. Lo primero es que es muy difícil para el ciudadano saber si se está produciendo una situación discriminatoria. Podría hacer una investigación en internet preliminar, para ver opiniones de otra gente acerca de la empresa o servicio, tratar de hablar con algún empleado de ella. En general lo veo muy difícil.

5. **¿Qué opinión general le merece la legislación vigente en materia de protección de datos?**

La legislación depende altamente del país del cual estemos hablando. Personalmente me parece un tema relativamente complicado dependiendo del sector. En EEUU la legislación es quizás más sencilla, pero protege menos los intereses y la privacidad de las personas que en la UE.

6. **¿Usted cree que dicha legislación afecta a la competitividad de las empresas europeas frente a las asiáticas y las americanas?**

Definitivamente, la regulación es siempre un obstáculo para startups y empresas pequeñas. Tener una regulación más sencilla facilitaría la creación de nuevos proyectos.

7. **¿En su compañía existe algún tipo de código deontológico (o manual de conducta) para los encargados de recolección y gestión de datos y los especialistas en Big Data?**

Por supuesto, en AA cada empleado solo tiene acceso solo y únicamente a los datos que estrictamente necesita para realizar su función. Aún con acceso a la información, solo se puede usar para lo que se necesite hacer en el momento. Está terminantemente prohibido el acceso a la información por “curiosidad” personal.

8. **¿Cree usted que sería útil que el Gobierno obligase a tener uno a todas las empresas?**

Tendría cosas positivas y negativas. Lo positivo, más protección de la información y un uso más ético.

Lo negativo, más burocracia, más fricción a la hora de empezar un negocio. Personalmente leyes como esa solo me incitarían a fundar mi startup en un país menos burocrático.

9. **¿En qué puntos deberían hacer hincapié dichos códigos y manuales?**

Cómo tratar los datos, donde almacenarlos, a que empleados dar acceso a los datos, etc..

10. **¿Cuáles son los peligros más serios que ve en el uso del Big Data y la Inteligencia Artificial? ¿Cree usted que estamos preparados para afrontarlos?**

Realmente no veo peligros, solo mejores productos, mejores servicios, mejor adaptación al usuario y al público en general, más eficiencia en las empresas, reducción de puestos de trabajo innecesarios que forzara a la población a desarrollar trabajos más creativos, etc…

11. **Y de cara al futuro, ¿Qué nuevos retos deberemos afrontar? ¿Y qué deberían hacer las autoridades al respecto, para prepararnos ante estos nuevos peligros?**

Pienso que lo más difícil será limitar y/o controlar como las empresas usan los datos de una forma que no limite o entorpezca el crecimiento de las empresas y de los productos.

Las autoridades deberían crear un marco regulatorio claro que establezca claramente como se pueden usar los datos y que datos, como se debe informar al usuario, etc.

12. ¿Conoce la nueva propuesta de la Comisión Europea sobre la nueva ley de Inteligencia Artificial? Si es así, ¿qué opina sobre ella?

No, la desconozco.

13. Si usted pudiera participar en la formulación de dicha ley, ¿qué debería incluir?

Me remito a la respuesta anterior.

Cuestionario nº7

Para empezar el cuestionario, querría que me contase cuál es su profesión, qué labores desempeña y en cuáles de sus tareas diarias está implicado el uso del Big Data. (Es importante que diga los años que lleva en este campo, y qué relación tiene su trabajo con el Big Data).

Soy Abogado y consejero delegado de una compañía dedicada a los servicios sanitarios.

En ambas actividades, el Big Data es absolutamente esencial. La incorporación del Big Data a la metodología de trabajo de los despachos de abogados está suponiendo una auténtica revolución en el sector jurídico**.** La transformación digital es la oportunidad de las empresas del sector para aumentar su eficacia y productividad. En la actualidad no se concibe el ejercicio de la profesión de abogado si no se tienen conocimientos en Big Data.

Por otro lado, en el mundo sanitario se hace innecesario confirmar la evidencia de la necesidad del tratamiento de datos como una de las labores críticas para la prestación del servicio.

1. **¿Usted cree que los ciudadanos leen y entienden las condiciones que aceptan, sobre la recolección y uso de datos personales, que se les pide en los contratos y términos de uso, tanto digitales como físicos?**

Bajo mi punto de vista, es claro que no solo no las entienden, sino que habitualmente ni las leen.

Es tal la cantidad de contratos que en la actualidad firma un individuo, y todos ellos con una referencia a su protección de datos, que se hace necesaria una regulación más proteccionista, no dependiente en su totalidad de los pactos entre las partes.

2. **¿Cree que los datos que se recopilan diario son destinados solamente para los fines que contemplan en las cláusulas de términos de uso?**

No puedo afirmar lo contrario, pero por lo que se lee en este mundo, parece muy razonable mantener dudas de que las empresas "recolectoras" de datos destinan exclusivamente a los fines que declaran.

3. **¿Le parece que la información que se usa a diario, es supervisada adecuadamente? ¿Se garantiza que la información que usan los algoritmos está libre de sesgos que puedan producir situaciones discriminatorias?**

No respondió.

4. **¿Cómo puede defenderse el ciudadano ante las situaciones discriminatorias que producen los sesgos en la información que usan las herramientas de Big Data?**

Frente a la resolución de la ONU (2016) en defensa de los derechos humanos en Internet, en la que se insiste en la necesidad de igualdad, el desarrollo de los algoritmos perpetúa una situación discriminatoria para las mujeres y las minorías.

Los algoritmos se reprograman con la información que obtienen y producen reglas externas, es decir, que ya no son una garantía del pretendido orden y control que sugiere la automatización.

Es evidente que es necesario un análisis crítico y humano de los algoritmos con métodos como la transparencia de su funcionamiento y condiciones de verdad, la conexión al software social, el enriquecimiento de conexiones para la mejora, y el impulso a su uso.

Hay que reducir los riesgos de la Inteligencia Artificial con la elaboración de principios éticos que definan, en conjunto, las necesidades del desarrollo de instrumentos e información de acuerdo con la seguridad, la transparencia, la responsabilidad, el alineamiento con valores humanos, la privacidad, la libertad, el control humano y el beneficio y la prosperidad comunes.

5. **¿Qué opinión general le merece la legislación vigente en materia de protección de datos?**

El nuevo Reglamento General de Protección de Datos (RGPD, por sus siglas en castellano y GDPR, por sus siglas en inglés) aprobado en abril de 2016 por la Unión Europea, constituye un nuevo marco jurídico sobre la protección de los datos personales y sobre sobre su libre circulación.

El RGPD está diseñado para otorgar mayor seguridad y control a las personas sobre su información personal, así como para establecer unas reglas comunes en toda Europa de protección de dicha información.

En España rige la Ley Orgánica de Protección de Datos (LOPD), una de las normativas más estrictas de la Unión Europea en materia de protección de datos. Hasta la entrada en vigor del RGPD, tanto la Directiva 95/46/CE como las normas internas de los diferentes países de la UE seguirán siendo aplicables, incluida la LOPD en España

Sin embargo, entiendo que falta un desarrollo mayor y más claro, así como más flexible a los cambios de la propia sociedad. En la actualidad, nuestra legislación tiene un retraso real sobre los datos de más de 20 años.

6. **¿Usted cree que dicha legislación afecta a la competitividad de las empresas europeas frente a las asiáticas y las americanas?**

Seguramente sí, por ser más estricta. Pero también es cierto que los clientes valoran cada vez más el respeto a los datos y el tener una legislación más restrictiva puede dar lugar a una diferencia competitiva en positivo.

7. **¿En su compañía existe algún tipo de código deontológico (o manual de conducta) para los encargados de recolección y gestión de datos y los especialistas en Big Data?**

Si. Tanto en la vertiente jurídica como en el trato de los datos sanitarios, los códigos deontológicos, y los protocolos respetuosos con las normas y los derechos fundamentales son absolutamente necesario.

8. **¿Cree usted que sería útil que el Gobierno obligase a tener uno a todas las empresas?**

No sé si a todas las empresas, pero seguro que sí a algunas por razón de su actividad e, incluso, por el volumen de los datos que traten.

9. **¿En qué puntos deberían hacer hincapié dichos códigos y manuales?**

Desde hace más de tres décadas, el mundo comenzó a tomar conciencia sobre la importancia de proteger los datos personales. Fue así como en 1980, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), con la colaboración del Consejo de Europa, publicó una guía para resguardar la privacidad y los flujos transfronterizos de datos personales a partir de los siguientes principios (OECD, 2013):

I Establecer límites claros para la obtención de los datos.

II Determinar la relevancia de los datos para el uso previsto.

III Definir con claridad el uso que se dará a los datos antes de solicitarlos.

IV Abstenerse de utilizar los datos para usos distintos al determinado originalmente sin el consentimiento de las personas afectadas.

V Asegurarse de proteger los datos contra el acceso ilícito o piratería.

VI Asegurar que los avances, prácticas y políticas sobre el uso de los datos sean abiertos y transparentes.

VII Garantizar que las personas cuyos datos se han recolectado tengan acceso a los mismos y puedan solicitar bien sea modificaciones o su eliminación definitiva

10. **¿Cuáles son los peligros más serios que ve en el uso del Big Data y la Inteligencia Artificial? ¿Cree usted que estamos preparados para afrontarlos?**

Hay que distinguir primero entre asistentes inteligentes e inteligencia artificial. En este momento, la mayoría de las aplicaciones que calificamos de inteligencia artificial son sólo asistentes inteligentes que aumentan y sirven a los humanos, como Google Maps, Google Lens, Alexa...

Puede que tengan un lenguaje avanzado y capacidad para el reconocimiento de imágenes, basados en aprendizajes profundos, pero claramente no son inteligentes. El coche autónomo tiene una inteligencia bastante menor, pero es poderoso en sus dominios, aunque no pueda comprender a un niño de dos años o jugar al ajedrez. Cuando las máquinas tengan añadidas otras piezas inteligentes y se expandan, cuando sean socialmente inteligentes, entiendan las emociones y se conecten unas con otras, entonces, rápidamente serán infinitamente inteligentes, lo que supone un riesgo para los seres humanos. La inteligencia artificial es asombrosa y bastante disruptiva ya, sobre todo en el entorno laboral, pero a medida que nos acerquemos a la inteligencia artificial general (IAG), mayor necesidad tendremos de guías éticas y de seguridad, y de regulaciones similares a los tratados de proliferación nuclear.

11. **Y de cara al futuro, ¿Qué nuevos retos deberemos afrontar? ¿Y qué deberían hacer las autoridades al respecto, para prepararnos ante estos nuevos peligros?**

Es evidente que nos encontramos en un momento que los legisladores tienen que hacer su trabajo, y no esperar a problemas futuros, sino a los que ya tenemos en la actualidad, y proceder a realizar una legislación moderna, potente y flexible.

12. **¿Conoce la nueva propuesta de la Comisión Europea sobre la nueva ley de Inteligencia Artificial? Si es así, ¿qué opina sobre ella?**

La propuesta de la Comisión Europa para regular la inteligencia artificial establece cuatro niveles de riesgo e informa que las normas deberán ser implementadas por todos los Estados Miembros por igual, quedando excluidos de la normativa los usos de la IA a nivel militar.

En el máximo nivel se encuentra el "riesgo inaceptable". Se trata de aquellos sistemas de IA considerados una "amenaza para la seguridad, los medios de vida y los derechos de las personas". Aquellos sistemas de IA que se engloben aquí serán prohibidos.

Entre los ejemplos que la Comisión expone está por ejemplo un sistema de IA que manipule el comportamiento humano e incite a la violencia, por ejemplo, un juguete con asistencia de voz que fomente el comportamiento peligroso de los menores. También se incluye aquí un sistema de "puntuación social" por parte de los gobiernos para diferenciar a los ciudadanos.

En un segundo punto de "alto riesgo" se incluyen usos de la IA en infraestructuras críticas que puedan afectar a la salud de los ciudadanos, IA para afectar a la educación y por ejemplo permita hacer trampas en exámenes, componentes en cirugía, sistemas de reclutamiento de personal, servicios públicos, legislación, inmigración o IA para la administración o justicia.

13. Si usted pudiera participar en la formulación de dicha ley, ¿qué debería incluir?

Sería magnífico poder participar en dicha legislación, pero ciertamente no estoy formado para ello.

No sé claramente qué es lo que debería incluir, pero sí creo que, en todos los ámbitos, la IA debería estar sujeta a obligaciones estrictas, entre las que se incluye un análisis de riesgos, trazabilidad de resultados, documentación detallada, supervisión humana y un alto nivel de robustez.