Máster en Negocio y Derecho de las Telecomunicaciones, Internet y Audiovisual.

Curso Académico 2019-2020

Trabajo de Fin de Máster

"Big Data y Protección de Datos en Tiempos del Covid-19"

Gerardo Antonio Steta Perea

Tutor: Teodora Toma

Madrid, junio 2020.

Agradecimientos

Este trabajo representa la culminación de una parte importante de mi carrera profesional como abogado, en la que pude ampliar mis conocimientos por medio del Máster en Negocio y Derecho de las Telecomunicaciones, Internet y Audiovisual. Por ello, quisiera dedicar unas breves líneas de este trabajo para mostrar mi agradecimiento a todas aquellas personas que de alguna u otra forma me han acompañado a lo largo de este proceso. De forma muy especial a mi familia y amigos.

Resumen

Derivado de la pandemia por el Sars-CoV-2 (Covid-19) que afectó prácticamente a todo el mundo, los gobiernos, empresas y particulares se vieron en la necesidad de tomar diferentes medidas para evitar los contagios y la consecuente propagación del virus. Estas medidas incluyeron, entre otras, el uso de mecanismos de Big Data (como son los relativos a la geo localización) para medir niveles de contagio y comportamientos, y así poder establecer un mayor control e información sobre las posibles maneras de transmisión del virus. El Big Data es una herramienta que sin duda permite monitorear lo anterior, sobre todo en una situación tan singular como lo ha sido la pandemia que aun estamos viviendo. Sin embargo, al implicar el uso de datos, algunos de ellos de carácter personal, nos enfrentamos a importantes retos en materia de privacidad y protección de datos que se deben tomar en cuenta con el fin de evitar violentar el derecho a la intimidad y a la privacidad de las personas.

Palabras Clave: *privacidad, protección de datos, RGPD, Big Data, Covid-19.*

Abstract

As a result of the Sars-CoV-2 (Covid-19) pandemic, that has affected the entire world, governments, companies and individuals had been forced to take measures to prevent infection and the consequent spread of the virus. These measures include, among other things, the use of Big Data mechanisms (such as geo localization systems) to measure infections and behaviors, and be able to establish better control and information in the matter, in order to prevent the spread of the virus. Big Data is a tool that undoubtedly allows the above described. However, since it involves the use of data, and in some cases personal data, we face significant challenges in terms of privacy and data protection that must be taken into account in order to avoid violating people's right to privacy and intimacy.

Key Words: *privacy, data protection, GDPR, Big Data, Covid-19****.***

Índice

Índice de Abreviaturas

AEPD: Agencia Española de Protección de Datos. La Agencia Española de Protección de Datos (AEPD) es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos. La Agencia es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.

BOE: Boletín Oficial del Estado. Es el diario oficial nacional español dedicado a la publicación de determinadas leyes, disposiciones y actos de inserción obligatoria. Su edición, impresión, publicación y difusión está encomendada, en régimen de descentralización funcional, a la Agencia Estatal Boletín Oficial del Estado.

CE: Consejo de Europa. Es un órgano de la Unión Europea de ámbito regional destinada a promover, mediante la cooperación de los estados de Europa, la configuración de un espacio político y jurídico común en el continente que se encarga de legislar conjuntamente con el Parlamento Europeo.

CEPD: El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE.

CNIL: La *Commission Nationale de L'informatique et des Libertés* es un organismo regulador administrativo francés independiente cuya misión es garantizar que la ley de privacidad de datos se aplique a la recopilación, almacenamiento y uso de datos personales.

COVID-19: La COVID-19 es la enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente. Tanto el nuevo virus como la enfermedad eran desconocidos antes de que estallara el brote en Wuhan (China) en diciembre de 2019.

Datos Personales: toda información sobre una persona física identificada o identificable como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

EDPS: El Supervisor Europeo de Protección de Datos es una autoridad supervisora independiente que tiene como objetivo principal garantizar que las instituciones y órganos de la Unión Europea respeten el derecho a la intimidad y la protección de datos.

OCDE: Organización para la Cooperación y el Desarrollo Económico. Es un organismo de cooperación internacional, compuesto por 35 estados miembros cuyo objetivo es coordinar sus políticas económicas y sociales.

OMS: Organización Mundial de la Salud. Es un organismo especializado de las Naciones Unidas fundado en 1948, cuyo objetivo es alcanzar para todos los pueblos el máximo grado de salud, definida en su Constitución como un estado de completo bienestar físico, mental y social, y no solamente como la ausencia de afecciones o enfermedades.

RGPD: Reglamento General de Protección de Datos. Es el Reglamento (UE) 2016/679 Del Parlamento Europeo y Del Consejo del 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.

UE: Unión Europea. Es una entidad geopolítica que cubre gran parte del continente europeo. Es una asociación económica y política única en el mundo, formada por 27[1] países que mantienen entre sí especiales relaciones económicas y políticas de cooperación e integración.

[1] El 31 de enero de 2020 el Reino Unido dejó de formar parte de la Unión Europea por lo que la UE pasó de 28 estados miembro a 27.

Introducción

Stefan Gross-Selbeck, presidente de Xing[2], una de las plataformas para profesionales más importante, afirmó que: los *datos personales son el petróleo del siglo XXI*. Esta frase es una afirmación que quizá refleja, en buena medida, la realidad que estamos viviendo desde el plano tecnológico. Las diferentes tecnologías han irrumpido de una forma incontrolable en nuestras vidas y hoy, no podemos imaginar nuestra vida diaria sin el uso de *smartphones*, internet, redes sociales, datos móviles, aplicaciones, y otras. Estos son ejemplos más que claros de lo que conocemos como "Tecnologías Disruptivas". Denominadas así porque han venido a transformar de una manera crucial nuestra vida diaria.

Con el surgimiento de estas tecnologías disruptivas, los datos se vuelven el valor más preciado de las empresas que hacen de éstos su principal modelo de negocio. Hasta 2003, de acuerdo con Google[3], la humanidad había generado cinco exabytes de información a lo largo de toda su historia. En 2007 se generaron 281 exabytes, según las investigadoras Hardy y Williams, y apenas cuatro años más tarde alcanzamos los 1.800 exabytes[4]. Vivimos en un mundo hiperconectado, en el cual se crean más datos que nunca en la historia de la humanidad y, por tanto, obtenerlos, almacenarlos y tratarlos es posible de formas cada vez más automatizadas y eficientes.

Las empresas tecnológicas, (no solo las gigantes tecnológicas como Facebook, Amazon o Google) ofrecen acceso gratuito a sus aplicaciones o plataformas, a cambio de poder acceder de forma casi ilimitada a nuestros datos, y, en muchos casos, transferirlos para propósitos comerciales; muchas veces sin nuestro consentimiento. Esto implica, por tanto, que el producto somos nosotros (o más bien, nuestros datos), no la aplicación o el servicio como tal[5]. Según Robert Kirkpatrick el *Big Data es el nuevo plutonio. En su estado natural tiene fugas, contamina y hace daño. Contenido y aprovechado de manera segura puede iluminar una ciudad*. Esto refleja el papel que juegan los datos en el modelo de negocio de las empresas de referencia de esta época. El ejemplo más claro es Facebook. El modelo de negocio de la red social más importante

2 XING es la red social para profesionales líder en Europa y en el mercado español, destacando su utilidad en la búsqueda y oferta de trabajo

3 López, Daniel. ¿Cuánta información se genera al año en el mundo? By Orange. 30 de abril de 2019. Fecha de consulta: 10 de abril de 2020, recuperado de: http://blog.orange.es/red/datos-mundo/

4 Un exabyte es una unidad de medida de almacenamiento de datos cuyo símbolo es el EB. Equivale a 10^{18} bytes.

5 Peirano, M. (2019). *El enemigo conoce el sistema: manipulación de ideas, personas e influencias después de la economía de la atención*. Barcelona: Debate.

del mundo, mezcla la publicidad con la inteligencia de datos para generar una rentabilidad que no se había visto antes. Esto se logra mediante el uso de cookies[6] pero con niveles de sofisticación muy elevadas y, también con el uso de APIs que sirven de puerta y de muralla; ofrecen acceso a ciertas bases de datos, procesos, funciones y bloquea el acceso a otros. *Los anuncios en estos modelos de negocios son la tapadera. El negocio no es vender productos a los usuarios sino vender los usuarios como productos a una industria que "trafica" con los datos. Para que el negocio funcione hay que mantener a los usuarios entretenidos mirando la página el mayor tiempo posible (Peirano, 2019)*[7]. Mientras más datos obtenga el algoritmo de Facebook, se consigue personalizar de forma mucho más eficiente la publicidad y los anuncios en la plataforma. La necesidad de Facebook por obtener más información y datos es tal que ha sabido adquirir plataformas de forma estratégica (Instagram[8] y WhatsApp[9]) para así poder recabar mas datos y generar un nivel de sofisticación de sus anuncios todavía mayor, a través de la inteligencia de datos. Además de esto, cada vez es más frecuente encontrar entidades o personas dedicadas a la compra de bases de datos para fines de especulación comercial (*data brokers*)[10].

Actualmente, uno de los aspectos más relevantes en la era de las sociedades de la información es el Big Data. *El Big Data es el conjunto de tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, con el objetivo de poder otorgarles una utilidad que proporcione valor. Éste puede ser descubrir patrones de comportamiento de los clientes de una organización para crear publicidad dirigida mucho más efectiva, predecir tendencias económicas*[11] o enlazar distintos tipos de datos médicos o de salud con el fin de evitar contagios o disminuir la propagación de estas, como sucedió con el surgimiento del Coronavirus en varios países.

6 Pequeños archivos de texto en el navegador que registran los datos sin molestar al usuario. Trozos de código que se pegan en el navegador cuando se pasa por un sitio web y que le dice al servidor de esta página web, quien eres.

7 Peirano, M. (2019). El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención. Barcelona: Debate.

8 El Mundo. (abril 9, 2012). Facebook compra Instagram por 1.000 millones de dólares. Recuperado el 12 de junio de 2020, de https://www.elmundo.es/elmundo/2012/04/09/navegante/1333991473.html

9 Europa Press, R. (octubre 21, 2016). Facebook compra WhatsApp por cerca de 22.000 millones de dólares. Recuperado el 21 de junio de 2020 de https://www.europapress.es/internacional/noticia-facebook-compra-whatsapp-cerca-22000-millones-dolares-20141007004852.html

10 Los Data Brokers o vendedores de datos son empresas que se dedican a recoger información de los consumidores, ya sea con o sin su permiso, y que venden a un tercero que esté interesado en obtener dicha información.

11 González Elena Gil. (2016). *Big data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos.

Es sabido que la tecnología va siempre a mayor velocidad que el derecho, por lo que la capacidad de los estados para regular distintos aspectos vinculados con el desarrollo tecnológico es cada vez mas complicada. Sin embargo, esto hace necesario tener en cuenta que la tecnología genera también riesgos y estos riesgos se transforman, a su vez, en grandes retos sobretodo para los juristas del siglo XXI.

Por otro lado, derivado del surgimiento de la pandemia de la COVID-19, se ha intensificado el uso, tratamiento y almacenamiento de datos de distinto ámbito. Destacando, sobretodo, el uso de datos médicos y de salud para los diagnósticos rápidos de la enfermedad por medio de herramientas tecnológicas como aplicaciones o bien, en algunos países, por medio de tecnologías de reconocimiento facial.

En esta investigación analizaremos de forma muy particular el papel que está jugando el Big Data con el surgimiento de la pandemia por coronavirus que ha afectado a miles de personas en todo el mundo. Además, matizaremos algunos aspectos relevantes que deben ser tomados en cuenta desde el punto de vista de la protección de datos, la privacidad y la seguridad de la información.

El trabajo está dividido en seis capítulos. Así, en el Capítulo I daremos una breve descripción sobre la COVID-19, en qué consiste la enfermedad y qué efectos ha tenido sobre la sociedad este padecimiento. En el Capítulo II dedicaremos algunas páginas para hablar sobre el concepto de Big Data, sus características y elementos esenciales. Siguiendo con el Capítulo III donde nos enfocaremos en algunos aspectos relevantes sobre la normativa de protección de datos en el ámbito europeo.

En el Capítulo IV, la parte medular de la investigación, revisaremos algunos casos relevantes sobre monitorización de datos de salud aplicados a la enfermedad de la COVID19, centrándonos en lo que han hecho Estados como Israel y España en relación al tratamiento de los datos para el control de la enfermedad. Continuaremos, en el Capítulo V, haciendo una aproximación de los criterios normativos que se pueden aplicar al Big Data, así como algunos puntos a tomar en cuenta desde la normativa cuando se trabaja con Big Data.

Finalmente, en el Capítulo VI, cerraremos el trabajo con algunas consideraciones finales y conclusiones sobre el Big Data y su relación con la protección de datos.

I. Capítulo Primero. Un Breve Panorama sobre la Covid-19

Cada vez, de forma mucho más frecuente, surge una nueva enfermedad, en la que los inicios resultan complicados por la falta de información y la falta conocimiento por parte de médicos, infectólogos y especialistas de la salud para el tratamiento de dichas patologías. La COVID19 es un claro ejemplo de este desconocimiento. A pesar de que países como China han logrado frenar, casi en su totalidad, los contagios de ésta, la posibilidad de desarrollar una vacuna es todavía lejana, pues aun existe una falta de información importante que nos pueda permitir determinar las causas que dieron origen a esta pandemia.

No obstante lo anterior, investigadores de distintas partes del mundo han podido generar cada vez mas información que posibilita a la sociedad a aclarar cada vez más las dudas en torno a esta enfermedad. ¿Qué es realmente la COVID19? Para poder entender a qué nos referimos cuando hablamos de COVID-19 es necesario hacer referencia a la enfermedad del Coronavirus. De acuerdo con la OMS (que es el organismo que dispone de mayor información hasta el momento) los coronavirus (CoV) son una amplia familia de virus que pueden causar diversas afecciones, desde el resfriado común hasta enfermedades más graves, como ocurre con el coronavirus causante del síndrome respiratorio de Oriente Medio (MERS-CoV) y el que ocasiona el síndrome respiratorio agudo severo (SARS-CoV). Un nuevo coronavirus es una nueva cepa que no se había encontrado antes en el ser humano[12].

Como se puede ver, el nuevo coronavirus es una nueva fase o capa de coronavirus de la cual no se tenia registro hasta hace algunos meses. En esta misma línea y, de acuerdo con la información que ha hecho pública la OMS derivada de sus recientes investigaciones, l*os coronavirus se pueden contagiar de los animales a las personas (transmisión zoonótica)[13].*

De acuerdo con estudios exhaustivos al respecto, el SARS-CoV se transmitió de la civeta al ser humano y que se ha producido transmisión del MERS-CoV del

[12] Organización Mundial de la Salud. Coronavirus. Consultado el 9 de abril de 2020. Recuperado de: https://www.who.int/es/health-topics/coronavirus/coronavirus
[13] Ibídem

dromedario al ser humano. Además, se sabe que hay otros coronavirus circulando entre animales, que todavía no han infectado al ser humano[14].

Así, teniendo claro en qué consiste la enfermedad del Coronavirus podemos destacar, entonces, que la COVID-19 es la enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente. Tanto el nuevo virus como la enfermedad eran desconocidos antes de que estallara el brote en Wuhan (China) en diciembre de 2019.

A. El Antecedente

Como se ha referido líneas arriba, las causas del surgimiento de esta enfermedad, son todavía desconocidas. Sin embargo, hay algunas teorías que hacen suponer que el surgimiento de esta "nueva versión" del virus tienen que ver con el consumo de animales silvestres en los mercados asiáticos, particularmente en China[15].

Pero vayamos al origen. Los primeros síntomas de los que se tiene registro se dieron por primera vez en la región de Wuhan, (que es una localidad ubicada en la provincia de Hubei en China), el 8 de diciembre de 2019[16]. La enfermedad se manifestaba como una especie de neumonía que afectaba gravemente el sistema respiratorio de los pacientes en los casos más graves. El sistema sanitario en China notó que la capacidad de contagio de la enfermedad era exponencial, pues el 20 de diciembre la enfermedad ya afectaba, al menos, a 60 personas[17]. Un número importante de los pacientes ingresados habían frecuentado un mercado público mayorista que comercializaba pollos, gatos, faisanes, murciélagos, marmotas, culebras venenosas, ciervos, órganos de conejos y otros animales salvajes, por lo que surgió la teoría de que el origen de esta pandemia estaba estrechamente asociado con el consumo de animales silvestres[18]. Es decir, un nuevo tipo de coronavirus de fuente animal.

[14] Ídem
[15] BBC News Mundo. Coronavirus: el riesgo que aún generan para la salud en China la cría y el consumo de animales silvestres. 7 de abril de 2020. Fecha de consulta: 11 de abril de 2020, recuperado de: https://www.bbc.com/mundo/noticias-52209095
[16] World Health Organization. *Pneumonia of unknown cause – China (en inglés)*, 5 de enero de 2020. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.who.int/csr/don/05-january-2020-pneumonia-of-unkown-cause-china/en/
[17] BLANCO R.P. (24 de marzo de 2020) Reporteros Sin Fronteras rastrea cómo la censura china contribuyó a expandir el coronavirus. El País. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://elpais.com/elpais/2020/03/24/hechos/1585063368_490254.html
[18] Shih, G. (9 de enero de 2020) *Specter of possible new virus emerging from central China raises alarms across Asia.* The Washington Post. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.washingtonpost.com/world/asia_pacific/specter-of-possible-new-virus-emerging-from-central-china-raises-alarms-across-asia/2020/01/08/3d33046c-312f-11ea-971b-43bec3ff9860_story.html

Esta teoría sobre el surgimiento de la enfermedad se empezó a expandir de forma importante y, a pesar de que no hay evidencia suficiente para afirmar que la enfermedad haya surgido en dicho mercado, el mercado chino fue cerrado el 1 de enero de 2020 por el gobierno para evitar una expansión aún mayor.

El virus continuó expandiéndose en varias partes del territorio de China y tras el desarrollo de un diagnostico específico se confirmó, finalmente, la existencia de la COVID19 en al menos 41 personas de un conjunto de casos sospechosos en Wuhan[19]. Con el avance y evolución de la enfermedad se empezó a divulgar información en relación a que la enfermedad solamente afectaba a personas mayores. En China, las primeras muertes se registraron entre el 9 y 16 de enero de 2020[20]. Las personas afectadas eran personas cuyas edades superaban los 60 años[21].

La Comisión Nacional de Salud de China hizo público de manera oficial el 20 de enero de 2020 que era factible que esta nueva epidemia se trasmitiera entre los mismos seres humanos[22]. Tras dicho anuncio, se empezaron a registrar casos de la enfermedad entre personal sanitario y el virus se empezó a expandir a otras regiones del continente como Corea del Sur y Japón.

El virus empezó a expandirse de forma muy acelerada. Por lo que el 30 de enero de 2020 la OMS declaró a esta epidemia como una "emergencia sanitaria de preocupación internacional, basándose en el impacto que el virus podría tener en países subdesarrollados con menos infraestructuras sanitarias[23]."

El 11 de marzo la enfermedad se encontraba ya presente en cerca de 100 territorios[24] a nivel mundial y fue en ese momento cuando finalmente la OMS declaró dicha enfermedad como pandemia[25]. El número de casos confirmados continuó

[19] Hui, David S, et al. (14 de enero de 2020) The continuing 2019-nCoV epidemic threat of novel coronaviruses to global health — The latest 2019 novel coronavirus outbreak in Wuhan, China. International Journal of Infectious Diseases. Recuperado de: https://www.ijidonline.com/article/S1201-9712(20)30011-4/pdf

[20] QIN, A. y HERNÁNDEZ, J. (21 de enero de 2020) *China Reports First Death From New Virus*. The New York Times (En Inglés). Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.nytimes.com/2020/01/10/world/asia/china-virus-wuhan-death.html

[21] Comisión de Salud de Wuhan. (16 de enero de 2020). *Comisión Municipal de Salud de Wuhan sobre neumonía infectada por nuevo coronavirus*. Fecha de consulta: 11 de abril de 2020. Recuperado de: http://wjw.wuhan.gov.cn/front/web/showDetail/2020011609057

[22] GAN, N; XIONG, Y; et al. *China confirms new coronavirus can spread between humans*. CNN (En inglés). Fecha de consulta: 11 de abril de 2020. Recuperado de: https://edition.cnn.com/2020/01/19/asia/china-coronavirus-spike-intl-hnk/index.html

[23] Cinco Días. (30 de enero de 2020). La OMS declara emergencia sanitaria internacional. El País. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://cincodias.elpais.com/cincodias/2020/01/30/economia/1580413773_537607.html

[24] Organización Mundial de la Salud. (11 de marzo de 2020). *Alocución de apertura del Director General de la OMS en la rueda de prensa sobre la COVID-19 celebrada el 11 de marzo de 2020*. Fecha de consulta: 11 de abril de 2020. Recuperado de https://www.who.int/es/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[25] *Ibídem*

creciendo. El 9 de abril de 2020 el mundo ya registraba cerca de 1.6 millones de casos confirmados.

Para evitar una propagación masiva de la enfermedad y evitar el consecuente colapso de los sistemas sanitarios en distintos países, los gobiernos de los mismos se vieron en la necesidad de imponer restricciones de viajes, cuarentenas, confinamiento, toques de queda, asilamientos sociales, cancelación de eventos, entre otras medidas. En España, el 14 de marzo, el gobierno encabezado por Pedro Sánchez decretó el estado de alarma para hacer frente a la expansión de la COVID19[26].

Al momento de la redacción del presente apartado, España sigue en estado de alarma toda vez que ha iniciado ya la fase de desescalada anunciada por el propio gobierno. No obstante, el Congreso ha aprobado una última prorroga del estado de alarma hasta el 21 de junio[27].

B. Algunos números: la evolución de la enfermedad en algunos países

Para entender la magnitud del problema de la enfermedad, es necesario acudir a la estadística para entender de qué forma ha ido evolucionando la enfermedad y sobre todo el número de contagios a escala global. Al día de la redacción del presente capítulo (13 de junio de 2020), se han registrado a nivel mundial alrededor de 1,4 millones de casos de coronavirus (SARS-CoV-2)[28]. En cuanto al número de personas fallecidas, a la fecha de redacción de esta investigación, Estados Unidos encabeza la clasificación al superar los 116.035 decesos, seguido de Reino Unido con alrededor de 41.279. España ha registrado un total de 27.136 fallecidos. En el continente americano, Brasil encabeza la lista con un total de 41.058 personas fallecidas[29].

Veamos ahora algunos gráficos para comprender de mejor forma la evolución y situación actual de la enfermedad. El gráfico que se muestra a continuación muestra,

[26] Presidencia de Gobierno (14 de marzo de 2020). El Gobierno decreta el estado de alarma para hacer frente a la expansión de coronavirus COVID-19. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2020/14032020_alarma.aspx

[27] Presidencia de Gobierno (3 de junio de 2020). Sánchez defiende una última prórroga del estado de alarma para "acompañar a los territorios hasta la nueva normalidad". Fecha de consulta: 12 de junio de 2020. Recuperado de: https://www.lamoncloa.gob.es/presidente/actividades/Paginas/2020/030620-sanchezprorroga.aspx

[28] Statista. Evolución del número acumulado de casos de coronavirus en el mundo desde el 22 de enero hasta el 8 de abril de 2020. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://es.statista.com/estadisticas/1104227/numero-acumulado-de-casos-de-coronavirus-covid-19-en-el-mundo-enero-marzo/

[29] Ibídem

de forma clara, la evolución que ha tenido la pandemia en distintos países. Al 9 de abril de 2020 el número de casos en China se ha mantenido relativamente constante mientras que en el resto de los territorios ha habido aumentos significativos:

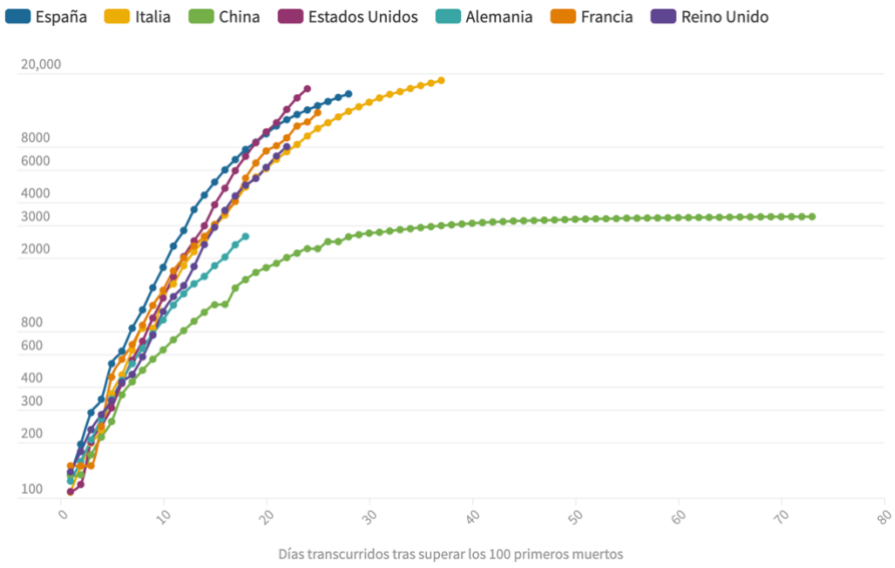


Gráfico 1[30]

Vemos, finalmente, la curva de casos de coronavirus en cada país. Estados Unidos es el que ha tenido mayores aumentos en comparación con el resto de los países. España e Italia, epicentros de la enfermedad, siguen con aumentos de casos, pero no de forma tan drástica.

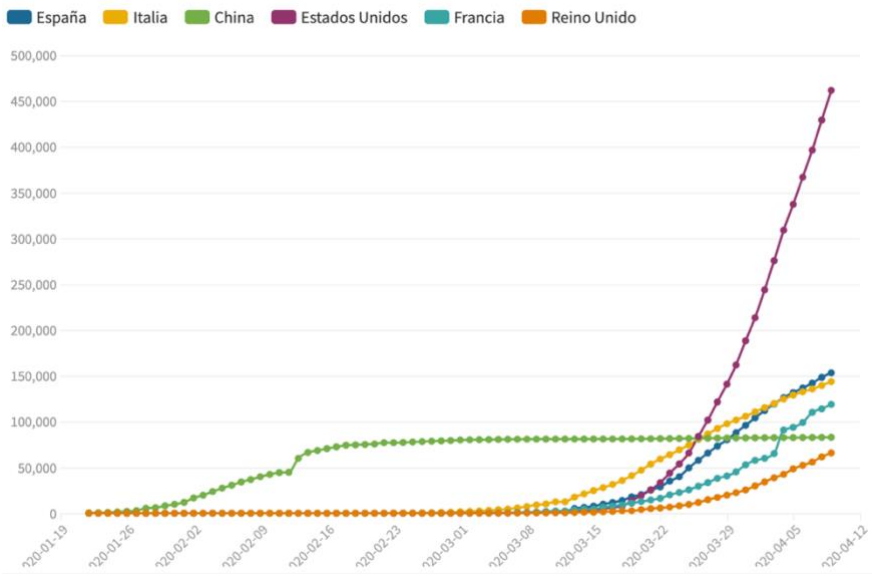


Gráfico 1.1[31]

30 EP Data. (10 de abril de 2020) La evolución del coronavirus en España y en el mundo, en gráficos. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.epdata.es/datos/coronavirus-china-datos-graficos/498

31 Ibídem

II. Capítulo Segundo: Big Data y Algunos Conceptos Preliminares

Cuando surgió el internet por primera vez en los años 60, muy pocos creyeron que llegaría a tener el impacto e importancia que tiene hoy en día y que se convertiría en parte fundamental de nuestra vida diaria. Como sabemos, el internet no es solo las redes y su infraestructura (no se limita solo al servicio per se) sino que es también una serie de datos e información que viajan por medio de dichas infraestructuras. Hoy, así como en su día internet fue un fenómeno completamente transformador, nos encontramos ante un nuevo fenómeno paradigmático quizá con un menor impacto desde el punto de vista tecnológico pero que esta revolucionando el mundo de la sociedad de la información: el Big Data.

El Big Data se refiere a los sistemas informáticos basados en la acumulación de grandes cantidades de datos y de los procedimientos usados para identificar patrones recurrentes dentro de estos datos. El Big Data, pues, se refiere a las grandes cantidades de datos e información controlados por distintos entes (públicos o privados) y que se basan, en su mayoría, en el uso de algoritmos o mecanismos de automatización[32]. Si bien muchos describen al Big Data como una "nueva tecnología" es importante destacar que cuando nos referimos al Big Data no hablamos en sí de una nueva tecnología sino de un nuevo mecanismo que nos permite obtener valor y beneficio como consecuencia del tratamiento y procesamiento de grandes cantidades de información y, desde luego, datos. Como una primera definición de Big Data podemos entender este fenómeno como la gestión de enormes volúmenes de datos que no pueden ser tratados de manera convencional, ya que superan los límites y capacidades de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos. Big Data es pues una tendencia de tratamiento de datos que busca aprovechar y darle valor a la información.

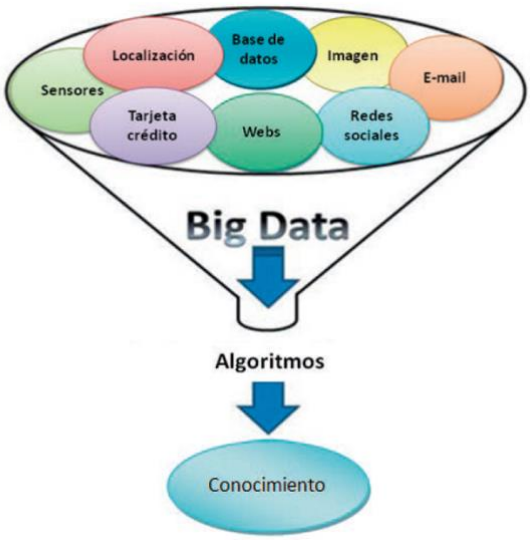
Como mencionamos en la parte introductoria de esta investigación, los datos y la información son el nuevo petróleo del siglo XXI. Pero, veamos algunas estadísticas interesantes en este sentido. En el año 2000 solamente un cuarto de toda la información mundial estaba almacenada en formato digital; el resto se almacenaba en medios análogos. Es decir, valores continuos para representar a la información. En la

[32] IBM Institute for Business Value, en colaboración con la Escuela de Negocios Säid de la Universidad de Oxford. «Analytics: el uso del big data en el mundo real». IBM Global Business Services (2012).

actualidad, esta realidad se ha visto transformada de forma tal, que hoy en día el 28% de toda nuestra información es digital. Es decir, usan valores discretos o discontinuos para representar la información.[33]

Como hemos dicho, el Big Data genera un cambio de paradigma en la forma en la que tratamos y procesamos grandes cantidades de información. Esto quiere decir que los datos como tal no generan valor por lo que el gran desafío que tiene el Big Data es justo darle ese valor a dicha información y ahí las nuevas tecnologías son el principal aliado del Big Data.

Así, el Big Data permite, de cierta forma, traducir en datos concretos gran cantidad de información que anteriormente no podía ser descifrada por carecer de una estructura sistemática como es el caso de las imágenes, vídeos, sonidos, etc. y, más recientemente, el caso de los datos de geolocalización de los usuarios. Lo anterior refiere al concepto que los anglosajones han bautizado como "datafiction"[34]. Asimismo, los datos que como usuarios vamos generando a través de internet (como a través de Facebook, Instagram o Twitter) es información que va adquiriendo cada vez un mayor valor. Las redes sociales son un excelente ejemplo de como se le da valor a esos datos, pues la información que proporcionamos en redes sociales es el modelo de negocios por excelencia de estas plataformas. Visto de una forma gráfica el Big Data se traduce de la siguiente manera:



[33] González, E. G. (2016). Big data, privacidad y protección de datos. Madrid: Agencia Española de Protección de Datos.
[34] Ibídem

Lo anterior implica una aproximación general sobre este "nuevo concepto" del Big Data. Sin embargo, para poder comprender de mejor manera este concepto, es necesario acudir a las características básicas de este fenómeno. La doctrina ha determinado que estamos ante Big Data cuando identificamos siguientes 3 dimensiones conocidas como las 3 uves[35] (o 4 uves dependiendo del autor)[36]. En este caso compartimos la visión de los autores que establecen la visión de las 4 uves:

Las cuatro dimensiones conceptualizadas en el gráfico anterior se pueden entender como atributos que se complementan entre sí para hacer posible este nuevo procesamiento y tratamiento de datos y se explica de la siguiente manera:

- **Volumen**: al hablar de este concepto nos referimos a los datos masivos. Esto es que el Big Data sea capaz de gestionar un gran volumen o número de datos que se generen diariamente por las empresas y organizaciones a nivel global[37]. Por ejemplo, la red social más grande del mundo, Facebook, almacena cerca de 4 petabytes de datos por día. Este volumen da datos es tan elevado (y se espera que crezca aún más) que las aplicaciones tradicionales de estructuración de

[35] Ibídem
[36] Bes, F. P., & Mexía, P. G. (2016). *El Derecho de Internet*. Barcelona: Atelier.
[37] Ibídem

datos como Excel o Access han quedado obsoletas, siendo necesario el desarrollo de sistemas mucho mas sofisticados[38].

- **Variedad**: los datos masivos deben ser capaces de poder combinar todos los formatos de información que circulan a través de las redes ya sea por medio de textos, imágenes, video, audios o cualquier otro formato[39]. Cada vez, se hace más frecuente la interacción de los distintos dispositivos conectados a la red por medio de, por ejemplo, IoT, lo que requiere de la posibilidad de combinar todos estos datos haciendo necesaria la interacción de diferentes dispositivos como laptops y dispositivos móviles. En la actualidad, solo el 20% de nuestros datos provienen de fuentes estructuradas, mientras que el 80% restante son datos no estructurados. Las tecnologías que se han desarrollado para el *Big Data* permiten, entre otras soluciones, combinar datos a pesar de que no se encuentren almacenados en ficheros con la misma estructura. Algunos expertos, así como no destacan la veracidad como una característica esencial, consideran que la variedad es el elemento más importante del Big Data.

- **Velocidad**: uno de los retos más importantes en cuanto al rendimiento de las redes que operan actualmente, es el de la velocidad. Big Data debe ser capaz de poder almacenar y funcionar en tiempo real con las fuentes generadores de información como sitios web, cámaras IP, redes sociales, servicios de mensajería instantánea, sensores de reconocimiento facial, sistemas de recolección de datos biométricos, entre otros. En virtud de esto, es indispensable que estas redes cuenten con un rendimiento tal que permitan reducir los tiempos de procesamiento de dichos datos. La velocidad permite, por ejemplo, detectar a un ritmo acelerado la velocidad de propagación de una pandemia en los sistemas sanitarios de una región determinada, para poder calcular la expansión que puede tener a nivel global[40].

- **Veracidad**: el Big Data debe tener la capacidad de tratar y analizar de manera inteligente los grandes volúmenes de información con el objeto de obtener de manera casi instantánea información útil y necesaria que nos permita tomar mejores decisiones en nuestro día a día. La veracidad de los datos se refiere pues, al sesgo, el ruido o alteración de datos. Esta característica puede ser otro

38 Steta, G. (2019). *Aspectos Regulatorios De Derecho De Las Tecnologías De La Información: Retos Para Una Regulación Efectiva De Cara A Una Disciplina Jurídica Autónoma Ante La Realidad De Los Fenómenos Tecnológicos Actuales* (Tesis de Grado). Universidad Panamericana, México.
39 Ibídem
40 Ibídem

de los grandes retos cuando se comparan con otras, como el volumen o la velocidad, debido a la dificultad de poder cerciorarnos de que un dato es 100% fiable. Garantizar este principio permitiría resolver el problema de la propagación de información o datos falsos o poco precisos a través de la red.[41]

A. Beneficios del Big Data

Como hemos podido apreciar a lo largo del presente apartado, Big Data es un cambio de paradigma en la forma en la que tratamos, procesamos y almacenamos información a gran escala. Debido a ello, el Big Data trae importantes beneficios encaminados a facilitarnos la vida en muchos sentidos y además permite resolver una serie de problemas. En este contexto, el sector tecnológico es una de las áreas de mayor crecimiento a escala global. De acuerdo con la organización GSMA, la tecnología y servicios móviles generarán el 5% del PIB mundial en 2022.[42] Por lo que es innegable que el sector de la economía digital seguirá creciendo de una forma considerable. En este sentido, el Big Data genera beneficios importantes no sólo para la industria sino también para la sociedad.

Uno de los grandes beneficios que trae consigo el Big Data es la capacidad de poder ofrecer una visión cada vez más precisa de las fluctuaciones y rendimientos de todo tipo de recursos, permitir realizar adaptaciones experimentales a cualquier escala de un proceso y conocer su impacto en tiempo casi real, ayudar a conocer mejor la demanda y así realizar una segmentación mucho más ajustada de la oferta para cada bien o servicio, o acelerar la innovación y la prestación de servicios cada vez más innovadores y más eficientes.[43]

El sector salud es otro de los sectores que pueden resultar beneficiados por el uso del Big Data ya que es un sector que trata grandes cantidades de información mucha de ella sensible, lo que permitiría generar mejores diagnósticos que puedan ayudar a la comunidad científica a desarrollar tratamientos a un ritmo mucho mayor y con un grado de efectividad mucho mejor. También permite medir a gran escala una enfermedad contagiosa como cuando se llega a dar el caso de una pandemia. A pesar

[41] Ibidem
[42] Bilbao, N. (febrero 27, 2018). La tecnología y servicios móviles generarán el 5% del PIB mundial en 2022. Recuperado el 13 de junio de 2020 de https://www.computerworld.es/tendencias/la-tecnologia-y-servicios-moviles-generaran-el-5-del-pib-mundial-en-2022
[43] Ídem.

de los beneficioso que representa el Big Data para este sector, al tratarse de datos con un grado de sensibilidad muy alta, el tema de protección de los mismos y la seguridad de la información juega un papel fundamental.

Otro de los grandes sectores que se pueden ver beneficiados por el desarrollo de este fenómeno son los gobiernos y las administraciones públicas, ya que implicaría una toma de decisiones más rápida y eficaz. Con el Big Data se podrían realizar análisis predictivos o una mejora continua de los sistemas de trabajo, además de mejorar la eficiencia en cuestiones tan sensibles como la protección ciudadana o la asistencia sanitaria.

Por ejemplo, la Ciudad de Nueva York ha utilizado la analítica de datos masivos para fines tan dispares como prevenir atascos, pues la regulación del tráfico en las grandes ciudades es una causa de problemas conexos como la dificultad de atender a víctimas de incendios o la ineficiencia de los servicios en la ciudad[44]. El Big Data podría, por ejemplo, medir en que hora del día hay mayor circulación de coches y a través de semáforos inteligentes generar que la luz roja dure mas o menos tiempo dependiendo de la hora.

Como vemos, el Big Data genera innumerables beneficios para distintos sectores. Sin embargo, esto también se traduce en importantes retos desde un punto de vista legal o jurídico del que hemos sido testigo todos: la privacidad y la seguridad de la información, que es, quizá, el principal riesgo que trae consigo la evolución y desarrollo del Big Data. Grandes empresas como Google, Facebook, AOL o Microsoft se encuentran entre las peor percibidas por los usuarios en términos de privacidad[45]. Y es que, como veremos en el siguiente apartado, la defensa de la privacidad y la protección de datos es uno de los retos más importantes a los que se enfrenta el *Big Data* en la actualidad.

B. Riesgos del Big Data

Aunque es cierto que este fenómeno puede traer consigo innumerables riesgos, para efectos de la presente investigación nos centraremos en analizar los riesgos desde la óptica de la protección de los datos de carácter personal, la privacidad y la seguridad de la información.

[44] Ibídem
[45] Ibídem

Como hemos visto en el apartado anterior, la falta de seguridad de la información representa uno de los principales riesgos sobre el uso masivo de datos. Los ciberataques a las empresas se han multiplicado de forma exponencial en los últimos años y esto obedece a dos factores principales: Por un lado, la sofisticación por parte de los atacantes con el uso de herramientas que son mucho mas potentes para penetrar sistemas informáticos y, por la otra, una falta de concienciación por parte de las empresas y usuarios en materia de ciberseguridad. De acuerdo con Bruce Schenir, *Chief Technology Officer* de IBM, *Cualquier tipo de dispositivo, como altavoces, objetos domésticos, juguetes, bombillas o coches estará conectado a Internet* (…) *Buena parte de estas redes y sistemas instalados en los dispositivos no cuentan con el apoyo de buenos equipos de ciberseguridad. Muchas incluso carecen de la posibilidad de ser actualizadas después de un ciberataque.*[46]

El segundo aspecto de mayor riesgo de cara al Big Data es la protección de los usuarios. Sin adentrarnos en demasiados detalles en este apartado (pues será objeto de análisis en capítulos posteriores) podemos decir que el Big Data debe asegurar anonimización que dichos datos permanezcan anónimos, para evitar que la información de los usuarios se vea vulnerada. En particular cuando las empresas tratan datos que impliquen una especial sensibilidad como son los casos de datos de salud, orientación sexual, preferencias políticas, entre otros. De acuerdo con Taylor Armending, especialista en seguridad de la información, *a medida que más y más dispositivos personales contribuyan al torrente de datos se hará más difícil mantener el anonimato y la privacidad. Una cosa es que las empresas, de forma intencionada, rechacen acceder a la información personal que también forma parte del Big Data, pero eso no significa que estos datos no se acumulen y que, llegado el caso, alguien los pueda utilizar*. [47]

En este sentido, es importante destacar un aspecto importante que será analizado a mayor detalle en el apartado siguiente, que tiene que ver con la aplicabilidad de la normativa europea de protección de datos. La normativa de protección de datos se aplica cuando la información de las personas físicas hace que estas sean identificadas o identificables.[48] Sensu contrario, cuando los datos no hacen identificable a una persona, no se aplica esta regulación. Es decir, cuando los datos se hacen anónimos a

[46] Samaniego, J. (mayo 18, 2018). ¿Cuáles son los riesgos del Big Data? Recuperado el 13 de junio de 2020, de https://hablemosdeempresas.com/empresa/riesgos-del-big-data/
[47] Ibídem
[48] Artículo 2 del Reglamento General de Protección de Datos.

través de técnicas de anonimización, se convierten en datos no personales, y la privacidad de los individuos queda protegida, de modo que no es necesario aplicar ninguna norma sobre protección de datos.

No obstante, el Big Data supone un tratamiento masivo de cantidades ingentes de información obtenida, en su gran mayoría, de forma absolutamente legal, es decir, basada en un consentimiento debidamente informado, así como dando cumplimiento al principio de calidad, en tanto las finalidades con las que son obtenidos dichos datos incluyen incluso el tratamiento mediante técnicas de Big Data. Es decir, son los propios usuarios los que facilitan la información sin ningún tipo de problema, normalmente a cambio de poder utilizar gratuitamente servicios de la sociedad de la información, juegos sociales, etc.

III. Capítulo Tercero. La Aplicación de la Normativa Europea de Protección de Datos.

Antes de adentrarnos en el estudio completo y el análisis del Big Data en relación a determinados casos concretos (que se expondrán en los capítulos posteriores) y la consecuente aplicación de la normativa europea para el tratamiento de dichos datos, es importante mencionar algunas cuestiones previas establecidas en el RGPD y en la LOPDYGDD. Al aludir al tratamiento masivo de datos para cuestiones relacionada con la salud de las personas, en el presente capítulo, se hará referencia a 5 cuestiones que considero importante tomar en cuenta en relación con el posible tratamiento de este tipo de datos, a saber: (*i*) base legal del tratamiento; (*ii*) el tratamiento de categorías especiales de datos personales; (*iii*) plazo de conservación de los datos; (*iv*) medidas de seguridad; y (*v*) evaluación de impacto.[49]

Base Legal del Tratamiento. El RGPD establece determinados aspectos de gran relevancia para el tratamiento de determinados datos como es el caso de los datos de salud. El RGPD establece ahora dentro de sus novedades, aquellas situaciones en las que el tratamiento de los datos será considerado como lícito. En este sentido, el artículo 6 de la propia normativa de protección de datos establece que, por ejemplo, *tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: (…) d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física*. Esto implica que para que un Responsable[50] pueda llevar a cabo el tratamiento de datos de carácter personal, debe justificar su tratamiento en algunas de las bases de legitimación que se establece en este precepto.

Tratamiento de Categorías Especiales de Datos Personales. Por otro lado, el RGPD establece algunos matices para el tratamiento de algunos tipos de datos que el reglamento define como "categorías especiales de datos personales. Por regla general el RGPD prohíbe el tratamiento de datos personales que *revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física*.[51]

[49] Recordemos que el RGPD al tratarse de un Reglamento comunitario es de aplicación directa para los 27 Estados Miembros sin necesidad de un acto de transposición (como sucede con las Directivas)
[50] Persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento (…).
[51] Artículo 9.1 del Reglamento General de Protección de Datos.

Sin embargo, el RGPD establece una serie de excepciones en la cuales no se aplicarán las prohibiciones establecidas en el apartado anterior. En este sentido, se estará exceptuado de dichas prohibiciones cuando, entre otros aspectos, (*a*) el interesado haya dado su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados; (…); (*c*) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; (…); (*g*) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; (*h*) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social,

Plazo de Conservación de los Datos. Otro punto fundamental a tomar en cuenta es el tiempo que podemos conservar los datos personales que recabemos. Por esta razón, los datos personales no pueden tratarse y almacenarse por un periodo indefinido y los plazos de conservación deben estar expresamente delimitados en la correspondiente política de privacidad. En este sentido, toda vez que el RGPD no establece plazos concretos de conservación de los datos, los datos deben conservarse por un plazo de tiempo no superior al necesario para cumplir con los fines del tratamiento. La conservación de datos debe limitarse a las finalidades para las cuales se han recabado dichos datos. Una vez cumplidas estas finalidades, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados. A manera de ejemplo, se proporcionan algunos criterios orientadores sobre los plazos de conservación:

Evaluación de Impacto. Otra cuestión a tomar en cuenta de cara al tratamiento de datos es la evaluación de impacto. Hay situaciones en el que, en función del mecanismo a través del cual recabemos y tratemos determinados datos, existe una mayor exposición a riesgo de dichos datos. Por ello, el RGPD establece que *cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la*

protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.[52]Dentro de la evaluación de impacto se deben considerar una serie de elementos previo al tratamiento de los datos personales. Así, la AEPD ha publicado una Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD. En este sentido, dicha Guía determina que el análisis de impacto debe incorporar (conforme a las propias disposiciones del RGPD) (i) una descripción sistemática de la actividad de tratamiento previstas; (ii) una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad; (iii) una evaluación de los riesgos; y (iv) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Medidas de Seguridad. Para terminar, el último punto a tomar en cuenta en relación con el tratamiento de determinados datos, sobretodo como los que hemos referido a lo largo de la presente investigación (datos de salud por ejemplo), son las medidas de seguridad que se deben de implementar al momento de llevar a cabo un determinado tratamiento de datos en función del tipo de riesgo al que están expuestos determinados datos. En este sentido, el RGPD determina que los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: (i) la seudonimización y el cifrado de datos personales; (ii) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (iii) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y (iv) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

A. Algunas Directrices de la AEPD sobre el tratamiento de datos de salud

El 12 de marzo de 2020 la AEPD publicó un informe[53] en el que analiza el tratamiento de datos de salud en relación con la crisis provocada por la epidemia de la

[52] Artículo 35 del Reglamento General de Protección de Datos.
[53] Agencia Española de Protección de Datos (2020). Informe 0017/2020

COVID-19. En dicho informe, establece que *el tratamiento de datos de salud en distintos ámbitos puede considerarse lícito, sometido al cumplimiento de los principios y obligaciones establecidos en el Reglamento General de Protección de Datos.*

En este sentido, la AEPD establece en el referido informe que para que el tratamiento de datos de salud sea lícito, el tratamiento debe realizarse en virtud de algunas de las bases que legitiman su tratamiento conforme al artículo 6 del RGPD. Asimismo, al ser los datos de salud datos especialmente protegidos, los responsables del tratamiento de los datos deben tutelar el tratamiento de los datos en algunas de las siguientes bases:

- → Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social.[54]

- → Que el tratamiento sea necesario por razones de interés público esencial o por razones de interés público en el ámbito de la salud pública.[55]

- → Que el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.[56]

- → Que el tratamiento de los datos de salud sea necesario para proteger el interés vital del interesado o de otra persona física cuando el interesado se encuentre física o jurídicamente incapacitado.[57]

Finalmente, la AEPD en dicho informe determina que el tratamiento de los datos referidos debe respetar el resto de los principios establecidos en el RGPD. En este sentido, determina la AEPD que se aplican todos sus principios, contenidos en el artículo 5 RGPD, y entre ellos el de tratamiento de los datos personales con licitud, lealtad y transparencia, de limitación de la finalidad (en este caso, salvaguardar los intereses vitales/esenciales de las personas físicas), principio de exactitud, y por supuesto, y hay que hacer hincapié en ello, el principio de minimización de datos.

[54] Artículo 9.2 b) del Reglamento General de Protección de Datos.
[55] Artículo 9.2 g) e i) del Reglamento General de Protección de Datos.
[56] Artículo 9.2 h) del Reglamento General de Protección de Datos.
[57] Artículo 9.2 c) del Reglamento General de Protección de Datos.

A priori se podría pensar que todo tratamiento de datos implica la sujeción automática al RGPD. Sin embargo, la aplicabilidad del RGPD no siempre es tan fácil de determinar. Hay casos en los cuales, por ejemplo, se trata de datos anonimizados en los cuales no es posible identificar o hacer identificable a una persona física por lo que no resultaría de aplicación las disposiciones del propio RGPD. Así, por ejemplo, algunas autoridades en materia de protección de datos como es el caso de la CNIL, en Francia, ha determinado que, en el caso de la toma de temperatura, en caso de que no implique un registro de dicha información que lo vincule de forma directa con el empleado, no sería de aplicación el RGPD[58].

Así cuando una autoridad pública (como es el caso) o una entidad privada, llevan a cabo el tratamiento de datos de salud, es indispensable realizar la evaluación de impacto para determinar, en primer lugar, las finalidades de dichos datos, la exposición al riesgo y las medidas de seguridad que, en su caso, se deben implementar. Por otro lado, es importante tomar en cuenta el criterio de proporcionalidad, esto es, obtener solo aquellos datos que sean indispensables para cumplir con la finalidad especifica y que impliquen la menor intrusión para el interesado, cumpliendo con el criterio de minimización de datos. Finalmente, es importante tomar en cuenta los plazos de conservación, en caso de tratar datos de salud, como es la temperatura de un interesado, pues los datos que se obtengan como medida para hacer frente a la COVID-19, deben ser utilizados únicamente por plazos estrictamente delimitados y no más. Al limitarse en cierta forma, el derecho a la privacidad y la intimidad con ese tipo de medidas, los plazos tanto de tratamiento como de conservación deben ser muy estrictos. Lo que podría implicar que una vez que se descubra una vacuna (o incluso antes), los datos de los ciudadanos deben dejar de usarse para esos fines, pues se trata de medidas extraordinarias y temporales.

En los siguientes apartados se analizarán de forma particular algunas de las medidas implementadas por algunos Estados, (como España e Israel) que implican el tratamiento masivo de determinados datos (como la geolocalización) a través de aplicaciones móviles, para luchar contra la expansión de la pandemia de la COVID-19.

[58] Portera, A. (marzo 18, 2020). La inoportuna doctrina de las autoridades europeas de protección de datos frente al Covid-19. Recuperado el 13 de junio de 2020 de https://hayderecho.expansion.com/2020/03/18/la-inoportuna-doctrina-de-las-autoridades-europeas-de-proteccion-de-datos-frente-al-covid-19/

IV. Capítulo Cuarto. Aplicaciones de Monitorización de Datos de Salud sobre la Covid19: el Caso de España e Israel.

Parte esencial de la presente investigación, es lo que se explicará en el presente capítulo y en el capítulo siguiente en relación a los proyectos desarrollados por los Estados para hacer frente a la Covid-19. Importante volver a mencionar, que hablamos, del desarrollo de herramientas tecnológicas que permitan luchar contra la transmisión de los contagios. Para efectos de la presente investigación se ha decidido la misma en dos proyectos esenciales que serán analizados desde la óptica de la protección de datos. Por un lado, el proyecto desarrollado por el Gobierno de Israel denominado "*HaMaguen*", y por el otro lado, el proyecto desarrollado por el Gobierno de España denominado "Asistencia Covid-19 y, de forma complementaria, el proyecto desarrollado por la Comunidad de Madrid, denominado "Coronamadrid". Todos estos proyectos tienen algunos rasgos en común: se trata de aplicaciones móviles que tienen por objeto prevenir los contagios entre sus ciudadanos mediante el monitoreo de los propios habitantes de una determinada localidad. Cada aplicación tiene particularidades propias y el tipo de datos e información que recaba varía de una a otra. Algunas acceden, por ejemplo, a la localización del usuario a través de las frecuencias de Bluetooth[59], otras lo hacen a través de la geolocalización GPS, algunas solicitan datos como la temperatura, teléfono móvil, entre otros.

A continuación, presentamos un análisis pormenorizado de cada una de ellas, haciendo especial énfasis en los datos que se solicitan, así como aquellas cuestiones que llaman particularmente la atención tras la consulta de su respectiva política de privacidad.

A. HaMaguen

Se trata de una aplicación móvil desarrollada por el Ministerio de Sanidad[60] de Israel disponible en hebreo, árabe, inglés, ruso y amhárico. El propósito fundamental de

[59] La tecnología Bluetooth trabaja en la banda mundial sin licencia ISM *(Industrial Scientific and Medical*) de 2.4 GHz, perteneciente a la banda de ultra altas frecuencias (UHF por sus siglas en inglés) la cual abarca los 300 MHz a los 3 GHz.

[60] Fernández, M. (marzo 24, 2020). Esta app detecta si estás junto a un contagiado por coronavirus: Israel ya la está usando. Recuperado el 13 de junio de 2020, de

dicha aplicación es determinar si una persona ha estado en presencia de otra que haya sido diagnosticada con Covid-19. La aplicación cruza el historial de GPS de tu teléfono móvil con los datos geográficos históricos de los pacientes del Ministerio de Salud. Si confirma, se le remitirá al sitio web del Ministerio de Salud para obtener información sobre lo que debe hacer a continuación, y podrá informar al Ministerio sobre la exposición[61].

¿Cómo sabe el Ministerio de Sanidad dónde han estado los enfermos si no tienen la App instalada? De acuerdo con las investigaciones y reportes de diversos medios de comunicación, las autoridades usan los servicios de Inteligencia del país para rastrear móviles de personas infectadas, registrando todos sus movimientos desde 2 semanas antes de dar positivos. También se rastrean personas sospechosas de estar infectadas[62].

Tras la revisión de su Política de Privacidad[63], estos son los aspectos más relevantes que se detectaron tras el análisis de la misma:

→ Cada hora, la aplicación descarga de la nube del Ministerio de Salud un archivo con una lista anónima de las ubicaciones en las que han visitado los pacientes diagnosticados con COVID-19 (pacientes que fueron examinados por el Ministerio de Salud y sometidos a una investigación epidemiológica mediante las diversas herramientas de que dispone el Ministerio) (incluyendo fechas y horas) y luego la aplicación hará una referencia cruzada de estas ubicaciones con las ubicaciones (incluyendo fechas y horas) que están almacenadas en su dispositivo. Si el usuario otorga el consentimiento, las ubicaciones se envían al Ministerio de Salud con el fin de ayudar a identificar a las personas que han estado expuestas y que deben entrar en aislamiento domiciliario lo antes posible. Si la solicitud descubre que existe la posibilidad de que el interesado haya estado en el mismo lugar y al mismo tiempo que un paciente

https://www.elespanol.com/omicrono/20200324/app-detecta-junto-contagiado-coronavirus-israel-usando/477202924_0.html

61 Ministerio de Sanidad de Israel (2020). HaMagen - The Ministry of Health App for Fighting the Spread of Coronavirus [Traducción Propia]. Recuperado el 13 de junio de 2020, de https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/.

62 Fernández, M. (marzo 24,). Esta app detecta si estás junto a un contagiado por coronavirus: Israel ya la está usando. Recuperado el 13 de junio de 2020, de https://www.elespanol.com/omicrono/20200324/app-detecta-junto-contagiado-coronavirus-israel-usando/477202924_0.html.

63 Ministerio de Sanidad de Israel (2020). Privacy Policy and Information Security. Recuperado el 13 de junio de 2020, de https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/.

diagnosticado, recibirá una notificación de la solicitud con los detalles del lugar y las horas en que ha estado expuesto a un paciente.

→ La aplicación accede a información como (*i*) los datos de geolocalización de las últimas dos semanas (fecha, hora y lugares concretos); (*ii*) historial de las redes inalámbricas a las que el usuario se ha conectado (Wi-Fi); (*iii*) referencias cruzadas de lugares con pacientes diagnosticados (si los hay) - sólo en las últimas dos semanas.

→ El cruce de información de personas infectadas en proporcionado directamente por el sistema de epidemiología del Ministerio de Sanidad. Dicha información la recibe el Ministerio de Sanidad de forma directa por los laboratorios.

→ En cuanto a las finalidades, si el usuario consiente en compartir el historial de ubicaciones almacenados en el dispositivo con el Ministerio de Sanidad, éste utiliza la información (i) para ayudar a llevar a cabo investigaciones epidemiológicas para localizar a personas que fueron expuestos a él o ella y corren el riesgo de enfermarse; (ii) a información en bruto que el usuario comparte con el Ministerio de Salud se examinará junto con el usuario en el marco de la investigación epidemiológica. La información sobre las ubicaciones que fueron confirmadas por el usuario se almacenará como parte de la investigación epidemiológica y se publicará sin ningún detalle de identificación, a fin de notificar y alertar al público y a los usuarios de la aplicación que se encontraban en los mismos lugares.

→ En cuanto al plazo de conservación, la propia Política de Privacidad establece un plazo de conservación de 7 años en el caso de la información sobre las ubicaciones confirmadas por el usuario y de 30 días en el caso de la información que no se utilice para investigaciones epidemiológicas.

→ La información que el usuario comparte con el Ministerio de Sanidad no se comparte con terceros (encargados).

→ En cuanto a las medidas de seguridad, la Política de Privacidad determina que, *aunque no escatimamos esfuerzos, experiencia*

profesional y controles, no existe un sistema completamente seguro. Por lo tanto, nos comprometemos a informar al público usuario de los incidentes de seguridad de la información que le afecten, para que pueda tomar las precauciones necesarias.

1. Algunas valoraciones personales sobre HaMaguen

Sin duda el Gobierno de Israel busca hacer frente, a través del uso de la tecnología, a los graves índices de contagio que se presentan en dicho país. Sin embargo, su política de privacidad establece algunas cuestiones que consideramos desproporcionadas (Israel es conocido por su gran capacidad para el desarrollo de actividades de inteligencia lo que implica comprometer la privacidad de los usuarios). Dentro de estos criterios desproporcionados vemos el plazo de conservación, se establece un plazo general de 7 años[64]. Por otro lado, hay nulas medidas de seguridad tendientes a evitar que se produzcan vulneraciones de seguridad al interior de la aplicación y, finalmente, no existe ningún tipo de derecho que los usuarios de dicha aplicación puedan ejercer para limitar el tratamiento. Sin embargo, vemos que a través de dicha aplicación el Gobierno puede monitorear casi de forma perfecta el comportamiento de sus ciudadanos a través del Big Data (datos de localización y ubicación) incluso de aquellos que no tengan instalada la aplicación.

B. Coronamadrid

Esta fue la primera aplicación que se desarrolló en España para tratar de hacer frente al alto número de contagios que se produjeron principalmente en Madrid. La Comunidad de Madrid lanzó esta aplicación, primero en versión de escritorio y luego en versión móvil, para luchar contra la saturación que en esos momentos existía en el sistema sanitario tanto de la capital como de la Comunidad Autónoma. En el proyecto de desarrollo de la aplicación participaron básicamente tres empresas: (i) *Mendesaltaren*, encargada fundamentalmente del diseño y programación de la aplicación; (ii) *Carto*, una empresa especializada en Big Data y análisis de datos; y (iii) *Force Manager*, una empresa de CRM[65] dedicada a unificar información concreta. A continuación, se exponen algunas consideraciones sobre dicha aplicación:

64 Ibídem

65 *Customer Relationship Management*. Es una aplicación que permite centralizar en una única Base de Datos todas las interacciones entre una empresa y sus clientes.

→ Se trata de una aplicación desarrollada a petición de la Comunidad de Madrid que permite hacer una prueba de autodiagnóstico de la Covid-19 que tiene por objeto primordial reducir la saturación tanto de las líneas de atención de Covid-19 habilitadas, como del mismo sistema sanitario de Madrid.

→ En cuanto al funcionamiento, la aplicación solicita varios datos personales, entre ellos (a) el nombre, la edad, el género, el correo electrónico, nuestra calle y código postal. Así como el número de teléfono y el DNI. Además, debemos aceptar que la aplicación acceda a nuestros datos de ubicación a través de geolocalización[66].

→ En relación con el tratamiento de los datos, los que se solicitan son para "*ofrecer información sobre el Covid-19, incluyendo el envío de notificaciones*", "*realizar tu autoevaluación" y "si es necesario, selección de cita para posible prueba". De la propia Política Privacidad de la aplicación se desprende que la app trata los datos para las finalidades siguiente: (a) Estadísticas; (b) Para investigación biomédica, científica o histórica; (c) Para archivo en interés público*[67].

→ En cuanto a los datos de ubicación de los usuarios a los que nos referimos anteriormente, la aplicación utiliza dichos datos para que las autoridades puedan visualizar infecciones en un mapa interactivo y realizar análisis geoespaciales para determinar áreas de alto riesgo. También se utilizan dichos datos para "*rastrear la evolución de los casos con más detalle, asesorando sobre las áreas de cuarentena para determinar si se están cumpliendo*".

→ En cuanto al plazo de conservación de los datos personales, la Política de Privacidad establece que los datos solo se conservarán y tratarán mientras sean necesarios para las finalidades indicadas en el punto 4 anterior, y durante el período que dure la situación de emergencia sanitaria[68].

Es innegable que la tecnología resulta una herramienta de gran ayuda para los Gobiernos en su lucha contra la Covid-19. Madrid ha hecho uso de las aplicaciones para llevar a cabo diagnósticos rápidos en esta lucha, en una Comunidad Autónoma gravemente afectada por la pandemia. Sin embargo, la gran interrogante está en si los datos que se solicitan resultan proporcionales con las finalidades que busca alcanzar el

66 Comunidad de Madrid. Política de Privacidad Corona Madrid. Recuperado el 13 de junio de 2020 de https://coronavirus.comunidad.madrid/politica-de-privacidad
67 Ibídem
68 Ibídem

propio Ayuntamiento. La propia aplicación argumenta que “son estrictamente necesarios por razones de interés público ante la actual situación de emergencia sanitaria decretada por las Autoridades como consecuencia de la pandemia de la Covid-19 y la necesidad de su control y propagación[69]. Aquí los gobiernos deben evitar caer en el abuso de querer argumentar todo tratamiento en el interés público. Pues también en estos casos debe respetarse el criterio de minimización de los datos.

1. Algunas valoraciones personales sobre Coronamadrid

A la hora de analizar tanto el funcionamiento de la aplicación como la Política de Privacidad en su conjunto, hay ciertas cuestiones que llaman mi atención que invitan a pensar que la Política de Privacidad tiene ciertos vacíos. Por un lado, considero que no está justificado el uso de datos como el DNI o el teléfono móvil si consideramos que estos datos no son necesarios para cumplir con las finalidades que se establecen en la propia Política de Privacidad. Otro punto importante a tomar en cuenta es lo relativo a la transferencia de datos a terceros, pues la aplicación no deja claro con qué terceros comparte dicha aplicación. Al inicio de este apartado se mencionó que participaron tres empresas en el proyecto, dos de ellas utilizan los datos que arroja la propia aplicación, una para el Big Data y otra para monitorizar determinados tipos de datos. Es por ello, que la Política de Privacidad debería aclarar dicha situación. Si bien es cierto que la aplicación dice “garantizar el máximo nivel de protección en el acceso que estos terceros tengan a los datos e información facilitada”, en ciertos apartados es ambigua. Es fundamental tomar en cuenta que la aplicación trata datos relativos a la salud de las personas, considerados como datos especialmente sensibles por la propia normativa de protección de datos, por lo que se espera primero un tratamiento proporcionado y segundo, medidas de seguridad tendientes a garantizar la seguridad de dichos datos.

C. Asistencia Covid-19

El 8 de mayo de 2020, el Gobierno de España, lanzó su propia aplicación bajo el nombre arriba referido. Básicamente lo que hace esta aplicación es reproducir tanto el funcionamiento como la recolección de datos que hace la aplicación de la Comunidad de Madrid. Incluso, la Política de Privacidad de esta aplicación del Gobierno es casi una reproducción de la de la aplicación de la Comunidad de Madrid. La aplicación está limitada para determinadas Comunidades Autónomas en las cuales no hay desarrollada

[69] Ibídem

una aplicación propia[70]. Por lo anterior, no se analizarán las particularidades de esta aplicación pues se aplican las mismas disposiciones que hemos indicado en el apartado anterior, por lo que es innecesario para efectos de la presente investigación. Este apartado sirve para advertir al lector que tanto en las comunidades autónomas como a nivel gobierno, existen aplicaciones tendentes a un mismo fin.

[70] Gobierno de España. Autoevaluación oficial del COVID-19. Recuperado el 13 de junio de 2020 de https://asistencia.covid19.gob.es/autoevaluacion-oficial/

V. Capítulo Quinto. Criterios normativos para el tratamiento del Big Data en el ámbito de la Salud.

Todas las aplicaciones que hemos analizado en el capítulo anterior implican una recolección y tratamiento masivo de datos de distinta naturaleza para propósitos específicos. Esto implica que los distintos gobiernos, a través de dichas aplicaciones, están haciendo uso del Big Data para hacer frente a una situación extraordinaria. Esto es, luchar contra una pandemia que ha afectado de forma particular a España.

Es innegable que el Big Data es una herramienta muy poderosa. Por ello, es importante tomar en cuenta todos los aspectos normativos que, según la escala de la Unión Europea, se deben tomar en cuenta para el tratamiento de datos de forma masiva. El Big Data por tratarse de una herramienta que maneja datos (en ocasiones de carácter personal), debe considerar la aplicación de algunos criterios para garantizar la seguridad de los mismos.

Así pues, en el presente capítulo se abordarán algunas cuestiones que los Responsables y Encargados del tratamiento de datos personales deben tomar en cuenta. Se analizarán también algunos instrumentos emitidos por la Unión Europea que, aunque no son vinculantes, si representan un punto de partida sobre determinados criterios que deben ser aplicados para el tratamiento de datos personales.

En 2014, la extinta autoridad europea de protección de datos Articulo 29 Emitió una Declaración del Grupo de Trabajo Artículo 29 (el "Grupo de Trabajo") sobre el impacto del desarrollo de Big Data sobre la protección de las personas en lo que respecta al tratamiento de sus datos personales en la UE[71]. Dicha declaración estaba encaminada a establecer aspectos clave sobre el desarrollo del Big Data en la UE. En este sentido, dentro de los aspectos esenciales de dicha declaración destacamos las siguientes directrices:

→ Los grandes usos de Big Data se basan en un amplio tratamiento de datos personales en la UE. Por ello, se plantean importantes cuestiones sociales, jurídicas y éticas, entre las que se encuentran las preocupaciones relativas

[71] Article 29. Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU. September 16, 2014.

a la privacidad y los derechos de protección de datos de estas personas. Por consiguiente, los beneficios que se derivan del análisis de Big Data sólo pueden alcanzarse a condición de que se satisfagan adecuadamente las correspondientes expectativas de privacidad de los usuarios y se respeten sus derechos de protección de datos.

→ Algunos interesados afirman que la aplicación de algunos principios y obligaciones de protección de datos en virtud de la legislación de la Unión Europea debería revisarse sustancialmente para permitir que se produzcan futuros y prometedores avances en las grandes operaciones de datos. La aplicación de los principios de limitación de los fines y minimización de los datos se presentan como preocupaciones fundamentales a este respecto, ya que exigen que los responsables del tratamiento de datos recopilen datos personales únicamente para fines específicos, explícitos y legítimos, y que no sigan procesando esos datos de manera incompatible con dichos fines.

→ El Grupo de Trabajo cree firmemente que el cumplimiento de este marco es un elemento clave para crear y mantener la confianza que toda parte interesada necesita para desarrollar un modelo comercial estable, basado en el procesamiento de esos datos. También considera que el cumplimiento de este marco y la inversión en soluciones respetuosas de la intimidad, son esenciales para garantizar una competencia leal y efectiva entre los agentes económicos de los mercados pertinentes.

→ Big Data es un término amplio que abarca un gran número de operaciones de procesamiento de datos, algunas de las cuales ya están bien identificadas, mientras que otras todavía no están claras y se espera que se desarrollen muchas más en un futuro próximo.

→ Además, las grandes operaciones de tratamiento de datos no siempre entrañan datos personales. No obstante, la retención y el análisis de enormes cantidades de datos personales en grandes entornos de datos requieren especial atención y cuidado. Pueden identificarse patrones relativos a personas concretas, también mediante la mayor disponibilidad de potencia de procesamiento informático y capacidades de extracción de datos.

→ El Grupo de Trabajo es consciente además de que la competencia internacional en materia de Big Data significa que pueden aplicarse

simultáneamente a nivel mundial diferentes marcos reglamentarios nacionales, regionales e internacionales de protección de datos y de la intimidad, lo que puede entrañar importantes problemas de cumplimiento. En vista de ello, el Grupo de Trabajo considera que es necesario aumentar la cooperación entre las autoridades de protección de datos y otras autoridades competentes de todo el mundo en relación con estas cuestiones.

Por otro lado, el Supervisor Europeo de Protección de Datos ("EDPS") emitió en 2015 una opinión[72] en la cual establece una seria de parámetros para enfrentar el fenómeno del Big Data que implican: (*i*) las oportunidades, riesgos y desafíos; (*ii*) el principio de transparencia; (*iii*) el control del usuario y compartir los beneficios de los grandes datos con los individuos; (*iv*) la protección de datos desde el diseño; (*v*) principio de "*Accountability*"[73]; y (*vi*) la puesta en práctica de los principios de protección de datos. A continuación, se destacan los aspectos más relevantes de dicha opinión:

→ Se establecen como principales desafíos del Big Data, (*a*) organizaciones que son mucho más transparentes en cuanto a la forma en que procesan los datos personales; (*b*) individuos que pueden beneficiarse de un mayor grado de control sobre cómo se utilizan sus datos; (*c*) protección de datos diseñada en productos y servicios; y (*d*) más controladores responsables;

→ En cuanto al principio de transparencia, para asegurar la protección de la elaboración de perfiles, se recomienda reforzar la aplicación del principio de transparencia y que se incluya específicamente la divulgación de la "lógica de la toma de decisiones", los datos propiamente dichos, así como su fuente. Se establece también la incorporación de mejores herramientas que permiten cumplir con la obligación (y el derecho) de información previa;

→ La privacidad y la protección de datos por diseño tiene por objeto incorporar la privacidad y la protección de datos en las especificaciones de diseño y la arquitectura de los sistemas y tecnologías de la información y las

[72] European Data Protection Supervisor. (noviembre 19, 2015). *Opinion 7/2015: Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability.*
[73] *Aconutability* es un principio común para las organizaciones en muchas disciplinas; el principio encarna el hecho de que las organizaciones cumplen con las expectativas, por ejemplo, en la entrega de sus productos y su comportamiento hacia aquellos con los que interactúan. El Reglamento General de Protección de Datos (RGPD) integra la rendición de cuentas como un principio que exige que las organizaciones establezcan medidas técnicas y organizativas adecuadas y puedan demostrar lo que hicieron y su eficacia cuando se les solicite.

comunicaciones. No se limita a los aspectos técnicos, las medidas organizativas son igual de importantes. Es necesario ofrecer a los individuos formas nuevas e innovadoras de estar informados sobre lo que sucede con sus datos, y de ejercer control sobre sus datos;

→ Finalmente, el principio de "*Accountability*". Los responsables deben establecer mecanismos internos y sistemas de control que aseguran el cumplimiento y proporcionan pruebas -incluidas las políticas internas y los informes de auditoría- para demostrar el cumplimiento a los interesados externos, incluidas las autoridades de supervisión. La rendición de cuentas no es un ejercicio aislado: la verificación periódica de que estos sistemas de control interno siguen siendo adecuados y que todo procesamiento de datos sigue cumpliendo la ley es un elemento esencial de la rendición de cuentas.

No obstante lo anterior, es importante tomar en cuenta que la declaración efectuada por Grupo de Trabajo y por la EDPS[74] es previa a la entrada en vigor del RGPD en la cual se establecen y amplían algunos criterios generales sobre el tratamiento de datos personales de las personas físicas. Sin embargo, guarda gran relevancia por la relación que dichos criterios tienen sobre el desarrollo del Big Data a nivel comunitario. En el apartado siguiente, analizaremos de forma concreta, todos aquellos elementos que conforme a la normativa europea deben tomarse en cuenta a la hora de utilizar herramientas de Big Data, que, en determinados casos, pueden implicar el tratamiento de datos de carácter personal.

A. ¿Qué se debe tomar en cuenta a la hora de trabajar con Big Data?

Como hemos visto a lo largo del presente documento, el tratamiento de datos de carácter personal es un tema complejo y que debe analizarse a la luz de cada caso concreto, y más aún cuando se utilizan herramientas del Big Data. En este apartado se pretende establecer algunos aspectos que se deben tomar en cuenta por los responsables a la hora de llevar a cabo un tratamiento de datos, sobretodo cuando nos referimos a datos pertenecientes a categorías especiales de datos como es el caso de los datos de salud.

74 Ibídem

El primer punto a considerar, es el tipo de datos que estamos tratando. Hay casos en que los datos que se procesan mediante herramientas de Big Data, son datos que no identifican ni hacen identificable a una persona, situación en la cual no será necesaria la aplicación de las disposiciones del RGPD. Si los datos que se están recabando se obtienen a través de mecanismos tecnológicos, es altamente recomendable llevar a cabo una evaluación de impacto para determinar lo anterior, así como las medidas que, en su caso, se deban implementar.

Si, por el contrario, se tratan datos que identifican o hacen identificable a una persona, es indispensable cumplir con determinadas medidas tanto de forma previa al tratamiento, como una vez que se esté llevando el tratamiento de datos propiamente dicho. A continuación, enlisto los principales criterios que, se estima, deben ser consideradas para tal efecto:

1. Evaluación de impacto. La evaluación de impacto permitirá valorar la exposición del riesgo de determinados datos personales, cuando éstos estén expuestos a un alto riesgo para los derechos y libertades de las personas. Esto permitirá determinar aquellas medidas de seguridad que se deban implementar para disminuir los riesgos.

2. Establecer las finalidades. Las finalidades son los motivos para los cuales se van a utilizar los datos personales. Las finalidades deben estar justificadas por una base legítima conforme al artículo 6 del Reglamento. Sin embargo, cuando se traten, por ejemplo, de datos de salud, estos solo se podrán tratar cuando se amparen en alguna de las finalidades que establece el artículo 9 del RGPD.

3. Determinar los datos que se van a recabar. En este punto es imprescindible tomar en cuenta el criterio de minimización de datos. Esto implica que solo podremos usar los datos personales que sean indispensables para cumplir con la finalidad establecida. No más. Esto implica que los datos recabados deben ser proporcionales a las finalidades perseguidas.

4. Establecer las medidas de seguridad aplicables a dichos datos. La evaluación de impacto nos indicará la exposición de riesgo que tienen dichos datos para lo cual se deberán aplicar determinadas medidas de seguridad. Los datos de salud son datos altamente sensibles por lo que se deben implementar medidas de seguridad reforzadas, tanto desde un punto de vista

técnico como organizativo. Algunas posibles medidas de seguridad son, por ejemplo, limitar el acceso a personas que no requieran acceder a determinados datos, utilizar mecanismos de seudonimización de datos, utilizar herramientas de cifrado como pueden ser certificados de seguridad o bien mecanismos criptográficos como contraseñas o firmas electrónicas para así garantizar la seguridad de la información.

5. Determinar los plazos de conservación de los datos. Este punto, resulta, igualmente, fundamental. Los datos solo podrán conservarse para cumplir con la finalidad prevista. Una vez que dicha finalidad se agota, se deberán bloquear dichos datos y se mantendrán solo para hacer frente a las posibles obligaciones que puedan surgir. Por ejemplo, en materia mercantil se establece un plazo de conservación de 6 años (depende de cada materia en particular).

6. Notificar en caso de cualquier violación de seguridad. Como bien sabemos, todo sistema es, en cierta medida, vulnerable; sobretodo los que utilizan las infraestructuras de Internet. Por ello, los responsables de los datos personales deben de tener muy presentes sus obligaciones en caso de presentarse brechas de seguridad en sus sistemas que comprometan la integridad de los datos que posean. Así, el RGPD establece que, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente a más tardar 72 horas después de que haya tenido constancia de ella (…)[75].

[75] Artículo 33 del Reglamento General de Protección de Datos.

VI. Capítulo Sexto. Conclusiones.

Para finalizar la presente investigación, a lo largo del presente apartado se aportan algunas conclusiones y consideraciones finales a las que se han llego en virtud de lo que se ha expuesto a lo largo del presente documento, considerando la relevancia del tema para la sociedad actual.

En primer lugar, se ha expuesto de forma importante, al inicio de la presente investigación, el impacto que ha tenido la Covid-19 en toda la sociedad, destacando el alto índice de contagios de la misma y las extraordinarias medidas que han tenido que tomar los gobiernos para hacer frente a la enfermedad.

En segundo lugar, se han establecido algunas cuestiones generales sobre le Big Data, que implica la posibilidad de procesar y acumular grandes cantidades de datos utilizando, en la mayoría de los casos, algoritmos para procesar información. Asimismo, se han establecidos algunos de los principales beneficios y riesgos de esta herramienta.

En el tercer apartado del presente documento se ha hecho referencia a la normativa europea de protección de datos, el RGPD como una normativa que representa uno de los mecanismos legislativos mas importantes de los últimos años. Así, se han expuesto algunos de los aspectos más relevantes a tomar en cuenta por parte de las entidades que hacen uso de datos de carácter personal sobretodo relacionados con lo que el reglamento denomina “categorías especiales de datos”.

En el quinto capítulo de la investigación se han analizado algunos de los proyectos de monitorización de datos llevados a cabo por Israel y España por medio del lanzamiento de las aplicaciones como HaMaguen y Coronamadrid. En dicho análisis se ha revisado el impacto que tiene para los usuarios este tipo de aplicaciones desde el punto de vista de la protección de datos.

En el último capítulo, se han establecido algunas directrices y criterios normativos aplicables a la gestión de datos masivos enfocados al tratamiento de datos en el ámbito de la salud, destacando algunos de los criterios emitidos tanto por el Grupo de Trabajo Artículo 29 como por el Supervisor Europeo de Protección de Datos. Concluye dicho apartado con algunos de los aspectos más relevantes que desde la óptica de la protección de datos se deben tomar en cuenta cuando se trabaja con Big Data.

El tratamiento de datos de salud representa, conforme al RGPD, una categoría de datos especiales que implica que los responsables deben tomar medidas mucho más reforzadas para su tratamiento. En este sentido, es importante que los responsables de este tratamiento delimiten muy bien las finalidades para recabar este tipo de datos, pues tienen una consideración de alta sensibilidad. Así, los gobiernos deben evidenciar de forma muy precisa la necesidad de obtener determinados tipos de datos de forma que se justifique su tratamiento. Es importante tomar en cuenta, que las medidas que implican una importante intromisión y cierta vulneración a los derechos a la privacidad y a la intimidad (basado en el interés público) debe realizarse de forma completamente excepcional y por plazos perfectamente delimitados.

Finalmente, del análisis que se ha llevado a cabo tanto de la aplicación HaMaguen en el caso de Israel y Coronamadrid en el caso de España, si bien es cierto dichas aplicaciones tienen por objetivo disminuir los contagios entre los ciudadanos, los gobiernos deben tomar en cuenta la proporcionalidad de los datos que se recaban. Desde luego es importante hacer frente a esta pandemia con los mecanismos que estén el alcance, pero hay datos que se solicitan en dichas aplicaciones que no guardan ningún tipo de relación con las finalidades establecidas en las propias políticas de privacidad de las aplicaciones referidas. Los gobiernos, en todos los casos, deben de tener muy presente el criterio de minimización de los datos personales al cual se ha hecho referencia a lo largo de la presente investigación.

Para concluir, es innegable que la pandemia de la Covid-19 ha hecho necesario que los Gobiernos de distintos niveles opten por tratar datos de diversas índoles, muchos de ellos relacionados con la salud de las personas. Este tipo de medidas, que han implicado una limitación del derecho a la privacidad e intimidad, deben ser completamente excepcionales, proporcionales y deben mantenerse por el menor tiempo posible para garantizar los derechos plenos de todas las personas. Los Gobiernos no pueden pretender justificar la obtención y la intromisión de éstos en la privacidad de las personas con el argumento del interés público. La normativa actual de protección de datos genera un marco adecuado que permite establecer las limitaciones y obligaciones a las que deben someterse los responsables del tratamiento de datos. Por ello, las autoridades nacionales deben velar por su cumplimiento y más aún ante el evidente crecimiento del uso de herramientas como el Big Data que implican un uso masivo de datos, muchos de ellos de carácter personal.

Referencias

Bibliográficas

Agencia Española de Protección de Datos. *Guía práctica para Las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD*. Recuperado el 13 de junio de 2020 de https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

Agencia Española de Protección de Datos. *Informe N/REF: 0017/2020*. Recuperado el 13 de junio de 2020, de https://www.aepd.es/es/documento/2020-0017.pdf

Bes, F. P., & Mexía, P. G. (2016). *El Derecho de Internet*. Barcelona: Atelier.

González Elena Gil. (2016). *Big data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos.

IBM Institute for Business Value, en colaboración con la Escuela de Negocios Säid de la Universidad de Oxford. «Analytics: el uso del big data en el mundo real». IBM Global Business Services (2012).

Peirano, M. (2019). *El enemigo conoce el sistema: manipulación de ideas, personas e influencias después de la economía de la atención*. Barcelona: Debate.

Steta, G. (2019). *Aspectos Regulatorios De Derecho De Las Tecnologías De La Información: Retos Para Una Regulación Efectiva De Cara A Una Disciplina Jurídica Autónoma Ante La Realidad De Los Fenómenos Tecnológicos Actuales* (Tesis de Grado). Universidad Panamericana, México

Electrónicas

BBC News Mundo. Coronavirus: el riesgo que aún generan para la salud en China la cría y el consumo de animales silvestres. 7 de abril de 2020. Fecha de consulta: 11 de abril de 2020, recuperado de: https://www.bbc.com/mundo/noticias-52209095

Bilbao, N. (febrero 27, 2018). La tecnología y servicios móviles generarán el 5% del PIB mundial en 2022. Recuperado el 13 de junio de 2020, de https://www.computerworld.es/tendencias/la-tecnologia-y-servicios-moviles-generaran-el-5-del-pib-mundial-en-2022

BLANCO R.P. (24 de marzo de 2020) Reporteros Sin Fronteras rastrea cómo la censura china contribuyó a expandir el coronavirus. El País. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://elpais.com/elpais/2020/03/24/hechos/1585063368_490254.html

Cinco Días. (30 de enero de 2020). La OMS declara emergencia sanitaria internacional. El País. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://cincodias.elpais.com/cincodias/2020/01/30/economia/1580413773_537607.html

Comisión de Salud de Wuhan. (16 de enero de 2020). *Comisión Municipal de Salud de Wuhan sobre neumonía infectada por nuevo coronavirus*. Fecha de consulta: 11 de abril de 2020. Recuperado de: http://wjw.wuhan.gov.cn/front/web/showDetail/2020011609057

Comunidad de Madrid. Política de Privacidad Corona Madrid. Recuperado el 13 de junio de 2020 de https://coronavirus.comunidad.madrid/politica-de-privacidad

El Mundo. (abril 9, 2012). Facebook compra Instagram por 1.000 millones de dólares. Recuperado el 12 de junio de 2020, de https://www.elmundo.es/elmundo/2012/04/09/navegante/1333991473.html

EP Data. (10 de abril de 2020) La evolución del coronavirus en España y en el mundo, en gráficos. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.epdata.es/datos/coronavirus-china-datos-graficos/498

Europa Press, R. (octubre 21, 2016). Facebook compra WhatsApp por cerca de 22.000 millones de dólares. Recuperado el 21 de junio de 2020 de https://www.europapress.es/internacional/noticia-facebook-compra-whatsapp-cerca-22000-millones-dolares-20141007004852.html

Fernández, M. (marzo 24, 2020). Esta app detecta si estás junto a un contagiado por coronavirus: Israel ya la está usando. Recuperado el 13 de junio de 2020, de https://www.elespanol.com/omicrono/20200324/app-detecta-junto-contagiado-coronavirus-israel-usando/477202924_0.html.

GAN, N; XIONG, Y; et al. *China confirms new coronavirus can spread between humans*. CNN (En inglés). Fecha de consulta: 11 de abril de 2020. Recuperado de: https://edition.cnn.com/2020/01/19/asia/china-coronavirus-spike-intl-hnk/index.html

Gobierno de España. Autoevaluación oficial del COVID-19. Recuperado el 13 de junio de 2020 de https://asistencia.covid19.gob.es/autoevaluacion-oficial/
Presidencia de Gobierno (14 de marzo de 2020). El Gobierno decreta el estado de alarma para hacer frente a la expansión de coronavirus COVID-19. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2020/14032020_alarma.aspx

Hui, David S, et al. (14 de enero de 2020) The continuing 2019-nCoV epidemic threat of novel coronaviruses to global health — The latest 2019 novel coronavirus outbreak in Wuhan, China. International Journal of Infectious Diseases. Recuperado de: https://www.ijidonline.com/article/S1201-9712(20)30011-4/pdf

López, Daniel. ¿Cuánta información se genera al año en el mundo? By Orange. 30 de abril de 2019. Fecha de consulta: 10 de abril de 2020, recuperado de: http://blog.orange.es/red/datos-mundo/

Ministerio de Sanidad de Israel (2020). HaMagen - The Ministry of Health App for Fighting the Spread of Coronavirus [Traducción Propia]. Recuperado el 13 de junio de 2020, de https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/.

Ministerio de Sanidad de Israel (2020). Privacy Policy and Information Security. Recuperado el 13 de junio de 2020, de https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/.

Organización Mundial de la Salud. (11 de marzo de 2020). *Alocución de apertura del Director General de la OMS en la rueda de prensa sobre la COVID-19 celebrada el 11 de marzo de 2020*. Fecha de consulta: 11 de abril de 2020. Recuperado de https://www.who.int/es/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

Organización Mundial de la Salud. Coronavirus. Consultado el 9 de abril de 2020. Recuperado de: https://www.who.int/es/health-topics/coronavirus/coronavirus

Portera, A. (marzo 18, 2020). La inoportuna doctrina de las autoridades europeas de protección de datos frente al Covid-19. Recuperado el 13 de junio de 2020 de https://hayderecho.expansion.com/2020/03/18/la-inoportuna-doctrina-de-las-autoridades-europeas-de-proteccion-de-datos-frente-al-covid-19/

Presidencia de Gobierno (3 de junio de 2020). Sánchez defiende una última prórroga del estado de alarma para "acompañar a los territorios hasta la nueva normalidad". Fecha de consulta: 12 de junio de 2020. Recuperado de: https://www.lamoncloa.gob.es/presidente/actividades/Paginas/2020/030620-sanchezprorroga.aspx

QIN, A. y HERNÁNDEZ, J. (21 de enero de 2020) *China Reports First Death From New Virus*. The New York Times (En Inglés). Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.nytimes.com/2020/01/10/world/asia/china-virus-wuhan-death.html

Samaniego, J. (18 de mayo 2018). ¿Cuáles son los riesgos del Big Data? Recuperado el 13 de junio de 2020 de https://hablemosdeempresas.com/empresa/riesgos-del-big-data/

Shih, G. (9 de enero de 2020) *Specter of possible new virus emerging from central China raises alarms across Asia.* The Washington Post. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.washingtonpost.com/world/asia_pacific/specter-of-possible-new-virus-emerging-from-central-china-raises-alarms-across-asia/2020/01/08/3d33046c-312f-11ea-971b-43bec3ff9860_story.html

Statista. Evolución del número acumulado de casos de coronavirus en el mundo desde el 22 de enero hasta el 8 de abril de 2020. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://es.statista.com/estadisticas/1104227/numero-acumulado-de-casos-de-coronavirus-covid-19-en-el-mundo-enero-marzo/

World Health Organization. *Pneumonia of unknown cause – China (en inglés)*, 5 de enero de 2020. Fecha de consulta: 11 de abril de 2020. Recuperado de: https://www.who.int/csr/don/05-january-2020-pneumonia-of-unkown-cause-china/en/

Legales

Article 29. Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU. September 16, 2014.

European Data Protection Supervisor. (noviembre 19, 2015). *Opinion 7/2015: Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability.*

Unión Europea. *Reglamento (UE) 679/2017 del Parlamento Europeo y del Consejo, de 27de 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).* Diario Oficial de la Unión Europea L 119/1, 4 de mayo de 2016.