Reglamento General de Protección de Datos de la Unión Europea: nuevos derechos y alcances normativos

General Data Protection Regulation of the European Union: new rights and regulatory scope

Juan Esteban Durango[1]

Resumen

La economía digital y el *Big Data* han puesto de manifiesto la importancia del tratamiento de datos personales como insumo primordial para la generación de ventaja competitiva y riqueza. A través de poderosos y complejos algoritmos las empresas que ofrecen bienes y servicios en Internet procesan gran cantidad de datos, lo que les permite conocer a profundidad los gustos, preferencias y otros aspectos más íntimos de sus usuarios o clientes. Este modelo económico basado en los datos conlleva riesgos a la privacidad y a los datos personales que identifican o hacen identificable a los consumidores, además plantea nuevos retos jurídicos en un entorno complejo y dinámico como lo es el mundo digital. El siguiente artículo aborda el estudio del Reglamento General de Protección de Datos de la Unión Europea (RGDP) y su impacto en la economía digital. Para este propósito, se realiza un análisis de los antecedentes de dicho marco legal y de los aspectos más relevantes incluidos en esta nueva normativa, como por ejemplo, el doble objeto del Reglamento, su ámbito de aplicación y su ámbito territorial. Se expondrá además la definición de sus principios jurídicos rectores (Responsabilidad Proactiva y Privacidad desde el Diseño), así como los nuevos derechos que protegen al ciudadano en materia de protección de datos. Finalmente se explican las principales obligaciones que impone el Reglamento a los responsables y encargados del tratamiento de datos personales.

Palabras claves

Internet, economía digital, *Big Data*, protección de datos, tratamiento de datos, datos personales, RGPD, Reglamento Protección de Datos, Europa, Unión Europea.

Abstract

The digital economy and Big Data have highlighted the importance of the treatment of personal data as a primary input for the generation of competitive advantage and wealth. By

[1] Estudiante de la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), San José, Costa Rica, quien opta al grado de licenciada en Derecho. Correo electrónico: juandurango@gmail.com

using powerful and complex algorithms, companies that offer goods and services on the Internet, can process a large amount of data, which allows them to know in depth the pleasures, preferences and other more intimate aspects of their users or customers. This economic model based on data entails risks to privacy and personal data that identify or make consumers identifiable, it also raises new legal challenges in a complex and dynamic environment such as the digital world. The following article addresses the study of the General Data Protection Regulation of the European Union (GDPR) and its impact on the digital economy. For this purpose, an analysis is made about its regulatory background and the most relevant aspects included in this new regulation, such as, for example, the double objective of the GDPR, its application scope and territorial scope as well. The definition of its guiding legal principles (Accountability and Privacy by Design) will also be exposed, as well as the new rights that protect citizens in terms of data protection. Finally, the main obligations imposed by the Regulation on those responsible for and handling personal data are explained.

Keywords

Internet, digital economy, Big Data, data Privacy, processing personal data, personal data, GDPR, General Data Protection Regulation, Europe, Europe Union.

Cuestiones preliminares: La Sociedad de la Información

Durante las décadas de los sesenta y setenta el sector de la información y la tecnología comienza a ganar relevancia global, de una manera muy preliminar y tratando de explicar este fenómeno, se fueron construyendo las bases teóricas de lo que hoy conocemos como la Sociedad de la Información. El origen de este término, de acuerdo con Estudillo (2001) se podría ubicar a inicios de los años setenta, primero en los Estados Unidos con un trabajo de Machlup, luego sería Daniel Bell con *El Advenimiento de la Sociedad Postindustrial*, en 1977 Marc Porat publicó *La Economía de la Información en Estados Unidos* y en Japón, Yoneji Masuda, dio a conocer su trabajo *La Sociedad informatizada como sociedad*.

Estos primeros trabajos cimentaron un nuevo paradigma en la sociedad, en este sentido Estudillo (2001) señala que "aparece una nueva sociedad caracterizada por el incremento de la información, como una definición del mundo moderno creándose un nuevo paradigma para interpretar el desarrollo social sobre la base del uso y empleo de tecnologías de información" (p. 78). Acota el mismo Estudillo (2001) que Bell "considera al sector de la información como el motor de cambio que hará posible una sociedad postindustrial, en donde podrá observarse un cambio en la economía de la producción de bienes, a una de servicios basados en la información" (p. 83).

El concepto Sociedad de la Información se posiciona entonces como la expresión dominante, la cual se ha utilizado para resaltar el preponderante rol de las tecnologías digitales en la generación de información y conocimiento. Lo importante a continuación, es definir lo que se entiende por Sociedad de la Información.

Para construir el significado del concepto, diversos autores han destacado el papel protagónico de la información y su tratamiento como generación de conocimiento y riqueza, por ejemplo, Miège (como se citó en Crovi, 2002) quien afirma que Sociedad de la Información es una sociedad caracterizada "por un modo de ser comunicacional que atraviesa todas las actividades (industria, entretenimiento, educación, organización, servicios,

comercio, etc.). En este tipo de organización social la información ocupa un lugar sustantivo y se convierte en fuente de riqueza" (p. 16).

Similar significado ofrece Castells (2000), pero utiliza su propio término al que ha llamado Sociedad Informacional, la cual explica como una organización social "en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de productividad y poder, debido a las nuevas condiciones tecnológicas que surgen en este periodo histórico" (p. 56).

Se aprecia como en las acepciones del término arriba mencionadas, se resalta la importancia de la información como fuente de productividad, riqueza y poder, pero además de esto y bajo la perspectiva de Castells, las tecnologías de la información han sido la causa de la evolución de esta sociedad. De esta forma, el empleo y el avance de las TIC, la información y el conocimiento se convierten en protagonistas, ya que como lo señala Peña-López (2010) "la información se utiliza como insumo para aplicarla en el proceso de mejora de otra información que dará, como resultado, mejor y más información. Así, la información es materia prima, capital y producto" (p. 54).

Este criterio es también seguido por Crovi (2002) quien afirma que

> la digitalización es una de las claves técnicas de la SI, proceso que ha dado lugar a nuevos medios; nuevas formas de producir, almacenar y difundir la información; y ha modificado sustancialmente las relaciones interpersonales y los sistemas de producción, educación y entretenimiento (p. 16).

Desde la perspectiva de lo expuesto por Miège, Castells y Peña-López, se entiende que La Sociedad de la Información ha evolucionado durante las últimas décadas impulsada por tres componentes claves: las TIC, esencial para su desarrollo ofreciendo la infraestructura física (*hardware*) y el medio digital y lógico (*software*); la información y las comunicaciones, como principal materia prima del conocimiento; y el usuario como beneficiario y participante final del intercambio y comunicación de esa información.

Posterior al surgimiento de la Sociedad de le Información, irrumpe Internet[2] durante la década de los noventa, su aparición provoca que la comunicación y las interacciones basadas en la información y el conocimiento se multipliquen de manera acelerada, facilitado todo lo anterior, por el desarrollo veloz de las TIC. Por lo tanto y de acuerdo con Pérez (2011) "no parece lícito dudar que Internet (International Network of Computers) está siendo el fenómeno estelar de las Nuevas Tecnologías de la información y la comunicación a partir de la década de los noventa" (p. 291).

[2] "El 24 de octubre de 1995, la FNC aprobó por unanimidad una resolución que define el término Internet. (...) RESOLUCIÓN: El Consejo Federal de Redes (FNC) acepta que el siguiente lenguaje refleja nuestra definición del término "Internet". "Internet" se refiere al sistema de información global que: (i) está vinculado lógicamente entre sí por un espacio de direcciones único a nivel mundial basado en el Protocolo de Internet (IP) o sus subsiguientes extensiones / complementos; (ii) puede admitir comunicaciones mediante el conjunto de Protocolo de control de transmisión / Protocolo de Internet (TCP / IP) o sus extensiones / complementos posteriores, y / u otros protocolos compatibles con IP; y (iii) proporciona, utiliza o hace accesibles, de manera pública o privada, servicios de alto nivel en las comunicaciones y la infraestructura relacionada descritas en este documento" (Internet Society, S. f.)

Por tanto, se pretende estudiar a continuación algunos aspectos resultantes de la interacción acelerada de los elementos supra mencionados. De manera concreta, lo referido a los riesgos jurídicos que emanan de dichas manifestaciones, es decir, la afectación de derechos y libertades de los usuarios en las interacciones surgidas en el Ciberespacio[3], así como la consecuente respuesta jurídica que algunos ordenamientos están ofreciendo a las diversas problemáticas que han emanado de la evolución de esta Sociedad de la Información, y que han puesto al individuo en posición vulnerable respecto a derechos fundamentales como la privacidad y la protección de datos, así lo afirma Pérez (2011) al destacar que "en las sociedades avanzadas con tecnología de punta ya no se puede juzgar como una amenaza remota las advertencias y experiencias de asalto informático a las libertades" (p. 293).

La economía digital

Desde inicios del Siglo XXI ya se afianzaba la idea de considerar a la persona como centro de esta revolución tecnológica y de la información. Este criterio fue plasmado en la declaración de principios de la primera Cumbre Mundial sobre la Sociedad de la Información celebrada en Ginebra en el 2003 (CMSI, 2004):

> Declaramos nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida (principio 1).

Con el explosivo auge de Internet, comienzan a surgir en la primera década del presente siglo iniciativas privadas cuya actividad comercial y económica está directamente relacionada con bienes y servicios digitales, es decir, que dependen de la tecnología y de Internet para ofrecer sus servicios y productos. En este entorno, aparecen empresas como Google[4] (búsquedas de información por Internet), Facebook[5] (Redes Sociales), Amazon[6] (comercio electrónico) y Apple[7] (dispositivos electrónicos).

Dichas empresas, impulsadas por el auge de la Sociedad de la Información y por Internet, descubren que la ventaja competitiva depende en gran medida, de que tan hábiles puedan ser

---

[3] "El ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada. Su conquista se ha convertido en meta obligada para quién desee sentirse miembro de la sociedad informática y es en la actualidad uno de los puntos de encuentro para el ocio y el negocio, que cuenta con mayores perspectivas de futuro (Castillo, 2003; Lagares, 2000; Rico, 1995; Sánchez Bravo, 2001)." (Pérez Luño, 2011, p. 292).

[4] Google fue fundada en 1998 y surge como el gigante de las búsquedas por Internet en la década siguiente. (Google, s. f.).

[5] Facebook fue fundada en el año 2004. (Facebook, s. f.).

[6] Amazon fue fundada en 1995, pero fue en la década anterior que se consolidó como la mayor empresa de comercio electrónico del mundo (Enciclopedia Britanica, s. f.).

[7] Si bien Apple fue fundada en 1976, fue en el año 2007 que se posicionó como una de las grandes de la tecnología, con el lanzamiento del teléfono inteligente *iPhone* (Enciclopedia Britanica, s. f).

en la recolección y análisis de la información que los propios usuarios suministran, en ese sentido Corredor (2015) explica que

> Las actividades de recolección y almacenamiento de estas informaciones solo comenzaron a evidenciarse a finales de la década anterior, a partir del interés de las grandes empresas del sector de la publicidad y el mercadeo en línea (*advertising networks*) por lograr un acceso consolidado a estos grandes volúmenes de datos. (p. 5).

El usuario como proveedor de información, tiene un papel preponderante en la generación de estos datos como insumo para la actividad económica de las empresas de Internet, tal y como afirma Corredor (2015) al destacar que el usuario "accede a la información y confronta la decisión racional de hacer disponible su propia información personal, como medio de contribuir a la optimización de las funcionalidades de los servicios que le son ofrecidos a través de Internet" (p.8).

En la práctica, "el modelo de negocio de muchos gigantes de internet está basado exclusivamente en la explotación de datos personales" (Gómez-Barroso y Feijóo-González, 2013, p. 292). Ejemplo de lo anterior, fue lo afirmado por la ex-comisaria europea para la protección de los consumidores Kuneva (2009), quien señaló que

> la información personal y de comportamiento también puede revelar cuánto usted está realmente dispuesto a pagar por un servicio. Puede revelar los riesgos en los que es probable que incurra, ya sea en pagos atrasados, enfermedades o incluso en la probabilidad de que devuelva los bienes que compra (párr. 36).

Por su parte, el FMI (2018) afirma que la economía digital no se puede definir de manera restringida con relación a las plataformas en línea, en un sentido amplio, toda actividad que utilice datos digitales es parte de la economía digital.

En otras palabras y visto lo anterior, la expresión economía digital es utilizado para indicar que la digitalización (el uso de Internet) se ha extendido a todos los sectores de la economía.

El vocablo "economía digital" fue acuñado por primera vez en 1995 por Tapscott en su libro de *The Digital Economy: Promise and Peril In The Age of Networked Intelligence* (Gada, 2016). El significado de esta expresión recoge diversos aspectos esenciales que se interrelacionan entre sí, entendiendo entonces por economía digital:

> el resultado de miles de millones de conexiones diarias en línea entre personas, empresas, dispositivos, datos y procesos. La columna vertebral de la economía digital es la hiperconectividad, lo que significa una creciente interconexión de personas, organizaciones y máquinas que resulta de Internet, la tecnología móvil y la Internet de las cosas (IoT). (Deloitte, s. f.).

Por su parte, el *big data* ha sido otro concepto que ha emergido con la Sociedad de la información y en concreto con el flujo de datos generado en la economía digital. En la sentencia del caso Publicis / Omnicom resuelto por la Comisión Europea, ésta desarrollo el concepto de *Big Data* al referir que

esto se relaciona con el proceso de examinar grandes cantidades de datos de una variedad de tipos ("big data") para descubrir patrones, correlaciones y otra información útil. El objetivo principal del análisis de big data es ayudar a las empresas a tomar mejores decisiones comerciales al permitir que los científicos de datos y otros usuarios analicen grandes volúmenes de datos de transacciones (European Commision, 2014).

Visto lo anterior, se observa la relevancia que en la actualidad tiene el alcance del *big data*, ya que otorga a las empresas el poder de realizar análisis de grandes cantidades de datos y de esta forma, no solo llegar a obtener mejores pronósticos, sino también a tomar decisiones que mejoren la productividad en el desarrollo de su actividad económica. Así explicado por la CEPAL (2013)

su aplicación va desde el diseño de un producto hasta la definición de su precio, pasando por la atención al cliente (…) [las empresas] están comenzado a utilizar estas herramientas para modelar los patrones de comportamiento y las preferencias de los consumidores, basándose, más que en muestras estadísticas, en el análisis de universos completos de observación (CEPAL, 2013, p. 11).

Un nuevo modelo económico se ha desarrollado, ya que la implementación del *big data* de acuerdo con Corredor (2015) "pone de presente una de las particularidades de la economía digital que consiste en que su materia prima es la información, la cual fluye a través de la red permitiendo, simultánea o sucesivamente, a múltiples usuarios utilizarla para diversos propósitos" (p. 6). En el mismo sentido Kuneva (2009) dijo que los datos personales son el nuevo combustible de internet y la nueva moneda del mundo digital.

Para poner en contexto la relevancia de las afirmaciones anteriores, los datos personales son el insumo más importante para las empresas de publicidad en línea, las cifras de facturación de compañías como Google y Facebook así lo señalan, de acuerdo con Pardo (2018) durante el año 2017 Google y Facebook acapararon el 63% de la inversión mundial en publicidad, Google facturó por publicidad más que toda la prensa escrita del mundo, mientras que Facebook ingreso por el mismo rubro tanto como todas las radios del planeta, Google además facturó en publicidad 80.800 millones de dólares mientas que Facebook 36.300 millones de dólares.

Con esas cifras, se puede comprender lo sostenido por Kuneva (2009) al afirmar que "Internet es un servicio respaldado por publicidad y el desarrollo de marketing basado en perfiles y datos personales es lo que hace que funcione." (párr. 5). Es propósito entonces de estas empresas de publicidad, ofrecer la gran mayoría de sus servicios gratis para recolectar y

procesar millones de datos y ofrecer publicidad de acuerdo con los gustos y preferencias de cada usuario, de esta forma se cumple lo dicho por Kuneva (2009) quien destacó que "La nueva realidad es que, en Internet, los consumidores están pagando los servicios con sus datos personales y su exposición a los anuncios" (párr. 17).

Protección de datos en la economía digital

El concepto de dato personal de manera restringida debe aplicarse a "toda la información relativa a una persona física identificada o identificable" (El Parlamento Europeo y el Consejo de la Unión Europea, 2016, Considerando 26). De manera amplia, se entiende que datos de carácter personal son

aquellos que pertenecen al individuo -a la persona- o son propios de él y que, por tanto, afectan, en mayor o menor medida, a la vida privada, y, consecuentemente, a la intimidad, que los eleva a la calidad de personalísimos, entrando en la esfera y el ámbito de un único poder de decisión y disposición sobre ellos: el de su titular (Davara, 2008, p. 53).

Los datos personales pueden ser públicos o privados, son públicos cuando "son conocidos por cualquiera, y privados aquellos que de acuerdo con ese valor, solamente serán conocidos o por voluntad del titular o en circunstancias especiales y tasadas por las leyes" (Davara, 2008, p. 54). Respecto al derecho a la protección de los datos personales, Davara (2008) entiende este derecho como

El amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad (p. 49).

Establecidas las definiciones anteriores, es conveniente analizar la manera en que el derecho a la protección de datos fue ganando relevancia en el entorno actual.

Con la llegada de Internet en los años noventa se incrementan las comunicaciones, las transacciones en entornos digitales y consecuentemente el flujo de información personal, así Domínguez (2018) destaca que a través de Internet

se ha generalizado la recogida y tratamiento de enormes cantidades de información sobre personas. Datos que provienen, no sólo de los que nosotros facilitamos directamente a través de la información que voluntariamente subimos a la red, sino también de los rastros que dejamos de forma inconsciente (p. 108).

Agrega este autor además que "la navegación por Internet generara gran cantidad de datos transaccionales de forma que cuando se accede a la red se deja un rastro digital" (Domínguez, 2018, p. 109). Como se mencionó anteriormente, la manera de procesar y tratar el rastro

digital que los usuarios dejan por la red, se realiza a través del *Big Data*, el cual se convierte para las empresas de la economía digital, en un importante instrumento para el tratamiento masivo de los datos personales que los usuarios entregan, explica Allen (2016) que

> los individuos contribuyen invisiblemente al Big Data cuando viven estilos de vida digitales o participan de otra manera en la economía digital, como cuando compran con una tarjeta de crédito, reciben tratamiento en un hospital, solicitan un trabajo en línea, investigan un tema en Google o publican en Facebook (párr. 1).

En ese mismo sentido, el RGPD afirma que

> La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. (El Parlamento Europeo y el Consejo, 2016, Considerando 6).

Lo anterior, implica riesgos y potenciales amenazas para la privacidad de los mismos usuarios, Allen (2016) agrega que "en la actualidad, Big Data puede sentirse como Gran Hermano, un enemigo natural de la privacidad personal y la libre elección" (párr. 6). Bajo este escenario, una de las formas en que se vulneran estos derechos, es a través de la creación de perfiles realizando análisis masivo de datos personales, por tal razón, este tema en específico se ha convertido en una de las principales preocupaciones del Parlamento Europeo y el Consejo (2016), quienes han señalado que

> Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas. (Considerando 30).

Ante estas circunstancias descritas, "las normas relativas al tratamiento de los datos de carácter personal constituyen un instrumento para salvaguardar la vida privada del sujeto" (Vilasau y Vila, 2010, p. 154). Es por esta razón que en las últimas décadas se ha venido promulgando regulación en materia de protección de datos personales, la cual busca "proteger a las personas ante el manejo o manipulación, no autorizada, de sus datos

personales, con especial atención cuando estos datos sean susceptibles de tratamiento automatizado o no" (Davara, 2008, p. 49).

Antecedentes regulatorios de la Protección de Datos

El antecedente del derecho a la protección de datos se remonta a 1983, en la consagración del derecho a la autodeterminación informativa. Dicho derecho nace en la Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983 sobre la Ley del Censo (Vilasau y Vila, 2010). En el texto de la sentencia, el Tribunal defiende la necesaria protección de los individuos frente a la recolección de datos como parte del derecho de la personalidad, así argumenta que "el derecho fundamental garantiza en esta medida la capacidad de los individuos, para determinar, en principio, la divulgación y empleo de sus datos personales (Schwabe, 2009, p. 94).

Así las cosas, el derecho a la autodeterminación informativa establecido en dicha sentencia, "comporta que el individuo pueda decidir básicamente por sí mismo cuándo y dentro de que límites procede revelar situaciones referentes a su propia vida" (Vilasau y Vila, 2010, p. 154).

Por su parte los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconocen el respeto de la vida privada y la protección de los datos de carácter personal como derechos fundamentales estrechamente relacionados, pero independientes[8].

En 1981, se publica el Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[9]. Posteriormente, a nivel comunitario se dictó en 1995 la Directiva 95/46/CE relativa a la protección de datos[10] y la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas[11], más adelante en el año 2006, la Directiva 2006/24/CE sobre la conservación de datos[12].

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD), entró en vigor en mayo de 2018. El RGPD como lo explica Garcerán et al. (2018) "presenta un espíritu armonizador y

[8] Carta de los Derechos Fundamentales de la Unión Europea http://europarl.europa.eu/charter/pdf/text_es.pdf

[9] Convenio 108 del Consejo de Europa https://rm.coe.int/16806cae9f

[10] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

[11] DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_es.pdf

[12] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 , sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE - https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.L_.2006.105.01.0054.01.SPA

homogeneizador, desde el momento que pretende crear un marco global de confianza, ya no solo a nivel comunitario sino incluso desde una perspectiva internacional" (p. 102).

El Reglamento tiene como eje principal cumplir con un doble objeto, el cual se encuentra no solo implícito en el título[13] sino también en el artículo 1.1, por tanto, este doble objeto es: regular el derecho fundamental de la protección de datos de las personas físicas y regular las normas relativas a la libre circulación de tales datos.

Ahora bien, en lo relativo al ámbito territorial y para comprender como afecta y a quienes, es de previo necesario aclarar los conceptos de establecimiento, responsable del tratamiento y encargado del tratamiento. El Considerando 22 del Reglamento define que el establecimiento "implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto". Mientras tanto, el responsable del tratamiento es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento" (artículo 4.7) y finalmente, el encargado del tratamiento es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento" (artículo 4.8).

Explicado lo anterior, es el artículo 3 el que establece el ámbito territorial de aplicación del RGPD: aplica para establecimientos ubicados en la Unión Europea y que realicen tratamiento de datos personales, aplica además para establecimientos que no se encuentren en la Unión Europea, pero que realicen actividades de tratamiento de datos de ciudadanos que residan en la Unión Europea, en ambos casos, ya sean estos establecimientos en condición de responsables o encargados del tratamiento de datos.

a) Principios rectores del Reglamento de Protección de Datos

El RGPD recoge en sus preceptos normativos un conjunto de principios que informan y articulan su texto legal. Estos principios se caracterizan "porque van a informar al ordenamiento jurídico con esta materia, de manera que deben ser considerados tanto en la elaboración como en la aplicación de las normas" (Puyol, 2016, p. 135). De acuerdo con el Considerando No. 26, estos principios "deben aplicarse a toda la información relativa a una persona física identificada o identificable". Por tanto, la importancia de estos principios de acuerdo con Puyol (2016) es que informan

> al ordenamiento jurídico en esta materia, de manera que deben ser considerados tanto en la elaboración como en la aplicación de las normas, y, por otro lado, también son utilizados para hallar las soluciones concretas a casos y supuestos determinados en defecto de normativa aplicable (p. 135).

El Reglamento contiene dos tipos de principios, los principios rectores: Responsabilidad Proactiva y Privacidad desde el Diseño, y los principios relativos al tratamiento de datos de carácter personal, definidos en el artículo 5: licitud, lealtad y transparencia, limitación de la

[13] Reglamento "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…"

finalidad, minimización de datos, exactitud, limitación del plazo de conservación e integridad y confidencialidad.

1-. Responsabilidad proactiva

El RGPD hereda este principio de la opinión 3/2010 redactada por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, pero fue hasta el Reglamento 2016/679 que se estableció a nivel normativo. Lo que el grupo de trabajo estableció originalmente acerca de este principio es la manera de cómo se ejerce la responsabilidad y cómo hacer que esta sea
verificable **(**Article 29 Data Protection Working Party, 2010). En este documento (2010), queda establecido que el principio de responsabilidad proactiva son las medidas que deben tomarse o proporcionarse para garantizar el cumplimiento en el campo de la protección de datos.

El principio de responsabilidad proactiva lo establece el Reglamento en el artículo 2.2 y recoge que el responsable del tratamiento de datos será responsable del cumplimiento de la normativa y capaz de demostrar este cumplimiento. Este principio se complementa con lo exigido en el artículo 24 del Reglamento, el cual establece la obligatoriedad de: implementar "medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento" (artículo 24.1); aplicar e implementar políticas de protección de datos; y crear e implementar códigos de conducta o un mecanismo de certificación.

2-. Privacidad desde el Diseño y por Defecto

El principio de Privacidad desde el Diseño es un concepto que la Dra. Ann Cavoukian desarrolló en los años noventa. De acuerdo con Cavoukian (s. f.), este principio

se caracteriza por medidas proactivas en lugar de reactivas, anticipa y previene los eventos invasivos de privacidad antes de que ocurran. El Principio de Privacidad desde el Diseño, no espera que los riesgos de privacidad se materialicen, ni ofrece remedios para resolver las infracciones de privacidad una vez que han ocurrido, ya que tiene como objetivo evitar que ocurran. En resumen, la Privacidad por Diseño viene antes, no después (p. 2).

Por su parte, la Privacidad por Defecto, es "una medida proactiva que persigue integrar las garantías en materia de privacidad por defecto, es decir, de modo pre-instalado o pre- construido en cualquier proyecto o actividad" (Garcerán et al, 2018, p. 106).

En el RGPD, estos principios vienen expresados en el artículo 25 y exige que: el responsable del tratamiento de datos aplique medidas técnicas y organizativas como la seudonimización y la minimización de datos (24.1); por defecto, solo sean objeto de tratamiento los datos personales necesarios de acuerdo con el fin específico (24.2); y la utilización de un mecanismo de certificación como elemento que acredite el cumplimiento de las obligaciones del Reglamento (24.3).

3-. Licitud, lealtad y transparencia

El artículo 5.1 inciso a) del Reglamento establece que los datos personales serán "tratados de manera lícita, leal y transparente en relación con el interesado".

De acuerdo con Puyol (2016) "para que el tratamiento de datos sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho" (p. 141).

El artículo 6 del Reglamento establece todos los presupuestos bajo los cuales el tratamiento de datos será lícito:

a. El consentimiento del interesado.
b. La legitimación contractual: el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte.
c. Legitimación legal: el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
d. Intereses vitales: del interesado u otra persona física.
e. Interés legítimo: el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.
f. Interés público: el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.

Respecto a la lealtad, Garcerán et al (2018) señala que el tratamiento de datos debe proporcionar "todas las salvaguardas y garantías necesarias en el marco del tratamiento" (p. 109). El mismo autor explica que el principio de transparencia se cumple cuando se proporciona "información detallada sobre el tratamiento y sobre sus finalidades, de modo sencillo, claro y fácil de entender" (Garcerán et al, 2018, p. 109).

4-. Limitación de la finalidad

Este principio establece que "los datos personales deben ser recogidos únicamente para el cumplimiento de fines específicos y explícitos y en ningún caso, deben ser tratados posteriormente de manera incompatible con dichos fines" (Garcerán et al, 2018, p. 109).

5-. Minimización de datos

El RGPD regula este principio en el artículo 5.1 inciso b) y expresa que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". Garcerán et al. (2016) destaca que únicamente resulta lícito solicitar al interesado aquellos datos personales realmente necesarios de acuerdo con el fin, así como aquellos datos necesarios cuando la finalidad perseguida no pueda ser cumplida sin tratar los datos de los interesados.

6-. Exactitud

El principio de exactitud ordena en el artículo 5.1 inciso d) que los datos personales serán "exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".

7-. Limitación del plazo de conservación

El Reglamento expresa que los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales (artículo 5.1.e). Deberá además implementarse medidas organizativas, "como el establecimiento de políticas de conservación de datos y '*record retention*'" (Garcerán et al, 2018, p. 110).

8-. Integridad y confidencialidad

El artículo 5.1 inciso f) regula que el tratamiento debe garantizar una seguridad adecuada de los datos personales, previniendo el tratamiento no autorizado o ilícito y su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

b) Derechos y otros alcances del Reglamento 1-. Derecho al olvido

El derecho a la supresión de datos o derecho al olvido lo establece el RGPD en el artículo 17. Si bien es el Reglamento que por primera vez eleva este derecho a nivel normativo en materia de protección datos, no se trata de un nuevo derecho, así Álvarez (2016) expresa que es "la manifestación de un derecho ya existente, en un entorno muy concreto. En este sentido, se trataría de la manifestación del derecho a la cancelación de datos en el entorno de Internet" (p. 242).

En lo que respecta al Derecho al olvido en el Reglamento, el Considerando 65 y 66 refieren que "los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo" (Considerando 65). Por su parte, el Considerando 66 consigna que

en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos.

2-. Derechos del interesado

Además del Derecho al olvido ya mencionado, el RGPD contempla también los siguientes derechos:

a. *Derecho de acceso*: el interesado tendrá derecho a conocer los datos que el responsable del tratamiento tenga sobre él y cómo los están tratando (artículo 15).
b. *Derecho de rectificación*: derecho de rectificación de los datos personales inexactos que le conciernan al interesado, teniendo en cuenta los fines del tratamiento (artículo 16).
c. *Derecho de Oposición*: derecho a oponerse al tratamiento de datos que un establecimiento este realizando de los datos personales (artículo 21).

d. *Derecho de portabilidad*: derecho a obtener una copia de los datos que una compañía este tratando, en un formato estructurado, de uso común y lectura mecánica. La copia de los datos se podrá transferir a otra compañía (Garcerán et al, 2018).
e. *Derecho de limitación de tratamiento*: derecho a limitar el tratamiento que una compañía realiza sobre los propios datos (artículo 18).
f. *Derecho a no ser objeto de decisiones individuales automatizadas:* derecho a impedir que el responsable del tratamiento tome decisiones completamente automatizadas, que tengan efectos legales sobre el interesado o le afecten significativamente (Garcerán et al, 2018).

3-. Registro de actividad de tratamiento

El artículo 30 del RGPD obliga al responsable del tratamiento de datos, llevar un registro de las actividades relativas al tratamiento de datos efectuadas bajo su responsabilidad. De acuerdo con Garcerán et al (2018) dicho artículo "impone a los responsables la obligación proactiva de documentar todas las actividades de tratamiento de datos que se lleven a cabo en la organización, generando y manteniendo un registro" (p. 113).

4-. Delegado de Protección de Datos

El Delegado de Protección de Datos "se trata de una figura clave en lo que respecta al marco actualizado de cumplimiento basado en la responsabilidad que impulsa el Reglamento" (Recio, 2016, p. 368). Si bien no es nueva la figura, si es el RGPD el que le da rango obligatorio de acuerdo con las características, condiciones y funciones establecidas en los artículos 37, 38 y 39. El Delegado de Protección de Datos o DPD es de acuerdo con la European Commision (Como se citó en Recio, 2016)

> una persona responsable en el seno de un responsable del tratamiento o un encargado del tratamiento de supervisar y monitorear de manera independiente la aplicación interna y el respeto de las normas sobre protección de datos. EL DPD puede ser tanto un empleado interno como un consultor externo (p. 375).

No todos los responsables del tratamiento o encargados del tratamiento deberán tener un DPD, según el artículo 37 será necesaria esta figura si es una institución pública (art. 37.1.a), si el tratamiento realizado por el responsable o encargado requiere una observación habitual y sistemática de interesados a gran escala (art. 37.1.2) y si el tratamiento realizado por el responsable o encargado es a gran escala de una de las categorías especiales de datos personales enumeradas en el artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10 (artículo 37.1.c).

Entre sus principales funciones y en arreglo al artículo 39 se encuentran:

a) Informar y asesorar al responsable o al encargado del tratamiento de las obligaciones que les incumben (artículo 39.1.a).
b) Supervisar el cumplimiento de lo dispuesto en el Reglamento (artículo 39.1.b).
c) Ofrecer asesoramiento acerca de la evaluación de impacto relativa a la protección de datos (artículo 39.1.c)
d) Cooperar con la autoridad de control (artículo 39.1.d).

e) Ser punto de contacto de la autoridad de control para cuestiones relativas al tratamiento (artículo 39.1.e).

5-. Enfoque basado en riesgos

Como parte de las acciones derivadas del principio de responsabilidad proactiva, el Reglamento exige al responsable y al encargado aplicar en materia de protección de datos, una metodología trabajo enfocada en el riesgo. Este enfoque de acuerdo con Garcerán et al. (2016) que

el responsable de tratamiento deberá llevar a cabo un análisis de riesgos de cada uno de los tratamientos de datos que desarrolle con la finalidad de identificar los riesgos que implica dicho tratamiento para los derechos y libertades de los interesados y, consecuentemente, aplicar las medidas de seguridad que resulten adecuados para mitigar los riesgos previamente identificados (p. 121).

Esta exigencia del Reglamento lo que busca es mejorar el cumplimiento de la normativa en protección de datos, por parte del responsable del tratamiento, ya que como lo expresa Recio (2016) este enfoque "debe servir para que el responsable del tratamiento pueda tomar decisiones por lo que se refiere a la aplicación de medidas concretas en función del riesgo del tratamiento y dar así cumplimiento al principio de responsabilidad" (p. 358).

6-. Violaciones de la seguridad (*Data Breach*)

El RGPD define una violación de la seguridad de datos personales como "toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos" (Artículo 4 inciso 12). En este sentido, establece el Reglamento al responsable del tratamiento, la obligación de notificar a la autoridad de control las violaciones a la seguridad de los datos personales en un plazo máximo de 72 horas después de que el responsable del tratamiento haya tenido conocimiento (Considerando 85).

El Considerando 86 por su parte consigna que el responsable del tratamiento debe, además, comunicar al interesado sin dilación la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y de esta forma, permitirle tomar las precauciones necesarias.

Conclusiones

La economía digital ha impulsado un nuevo paradigma económico que reúne diversos participantes globales a través de múltiples plataformas digitales, en consecuencia, a diario surgen millones de interacciones y relaciones que no son ajenas al Derecho. Uno de estos fenómenos que importan al Derecho, es el masivo tratamiento de datos personales que las empresas del sector digital realizan a través del *Big Data*. Es en este punto donde el Reglamento de Protección de Datos de la UE ha venido a dotar de seguridad jurídica las relaciones nacidas en el Ciberespacio, haciéndolo en un doble sentido, por un lado, contempla que es indispensable la libre circulación de los datos para el desarrollo de la economía digital,

pero a su vez, garantiza el derecho fundamental a la protección de datos de carácter personal de los ciudadanos europeos.

Si bien hasta la actualidad, el Derecho ha intervenido de manera reactiva, lenta y tardía, en lo que respecta a los fenómenos nacidos de la tecnología (ésta última va mucho más rápido que el Derecho), se puede concluir que el RGPD pretende ser un marco legal proactivo, el cual, a través de sus principios rectores de responsabilidad, privacidad desde el diseño y privacidad por defecto, así como su enfoque en la gestión de riesgos, persigue garantizar que los responsables y encargados de tratamiento de datos, cumplan de manera proactiva y preventiva lo ordenado en el Reglamento.

El RGPD regula en materia de protección de datos un mercado de más de 500 millones de habitantes[14], persigue armonizar las leyes relativas al tratamiento de datos dentro de la comunidad europea y exige su cumplimiento además a cualquier otra empresa que realice actividades con ciudadanos europeos. En consecuencia, gran cantidad de estas empresas, han decidido armonizar todas sus políticas globales de tratamiento de datos de acuerdo con lo establecido en el Reglamento, tal es el caso de Microsoft, la cual anunció en abril del 2018 que extenderían los derechos principales del RGPD a todos sus usuarios globales (Brill, 2018), de igual forma lo dio a conocer HP Inc. en sus políticas de privacidad (HP, 2018). Por lo tanto, el RGPD ha logrado tener un impacto no solo a nivel europeo sino a nivel global, siendo la normativa más novedosa y completa en la actualidad en lo concerniente a protección de datos personales, y es por esta razón que muchas empresas tecnológicas estandarizan sus procesos internos para cumplir con el Reglamento dentro de sus organizaciones y de esta manera ofrecer un tratamiento de datos más seguro.

Finalmente, el propósito del RGPD de ser una regulación proactiva y preventiva se pondrá a prueba durante los próximos años, ya que el avance acelerado de los algoritmos y la exponencial capacidad de computo abren paso al desarrollo de la Inteligencia Artificial, el Internet de las Cosas (*IoT*), el Blockchain y los robots, los cuales prometen hacer la mayoría de las tareas que realizan hoy los humanos. Dichos adelantos, convierten estas tecnologías en potenciales amenazas de la intimidad, la privacidad y el tratamiento de los datos personales de sus usuarios. Es allí donde una implementación adecuada del RGPD por parte del sector tecnológico, convertirán el Ciberespacio en un lugar más seguro del que es hoy día.

[14] La Unión Europea: 500 millones de habitantes en 28 países https://europa.eu/european-union/sites/europaeu/files/docs/body/eu_in_slides_es.pdf

Referencias

Allen, A.L. (2016). *Protecting One's Own Privacy in a Big Data Economy*. Harvard Law Review. Recuperado de https://harvardlawreview.org/2016/12/protecting-ones-own- privacy-in-a-big-data-economy/

Álvarez C., M. (2016). *El derecho a la supresión o al olvido*. En Piñar M., J. (Director), Reglamento General de Protección de Datos Hacia un nuevo modelo europeo de privacidad (pp. 241-256). Madrid España: Editorial Reus.

Article 29 Data Protection Working Party, (2010). *Opinion 3/2010 on the principle of accountability*. Recuperado de https://ec.europa.eu/justice/article- 29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

Brill, Julie (2018). *Microsoft's commitment to GDPR, privacy and putting customers in control of their own data*. Recuperado de https://blogs.microsoft.com/on-the- issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers- in-control-of-their-own-data/

Castells, M. (2000). *La era de la información: economía, sociedad y cultura*, Volumen I, LA SOCIEDAD RED [Versión digital]. Recuperado de http://www.felsemiotica.org/site/wp-content/uploads/2014/10/LA_SOCIEDAD_RED-Castells-copia.pdf

Cavoukian, A. (s. f.). *Privacy by Design The 7 Foundational Principles*. Recuperado de https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

CEPAL. (2013). *Economía Digital para el cambio estructural y la igualdad*. Recuperado de https://repositorio.cepal.org/bitstream/handle/11362/35408/1/S2013186_es.pdf

CMSI. (2004). *Declaración de principios: Construir la Sociedad de la Información: un desafío global para el nuevo milenio.* Recuperado de https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html

Corredor, G. R. (Diciembre, 2015). Consolidación de la economía digital y desafíos en materia de protección de la privacidad. *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, (14), 1–26. Universidad de los Andes (Colombia). Recuperado de https://doi.org/10.15425/redecom.14.2015.01

Crovi, D. (2002). Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza. *Revista Mexicana de Ciencias Políticas y Sociales*, Año XLV (185), mayo-agosto 2002, 13-33. Recuperado de http://www.redalyc.org/pdf/421/42118502.pdf

Davara R., M.A. (2008). *Manual de Derecho Informático*. 10ª Edición. Madrid: Thomson Aranzadi.

Deloitte, (s. f.). *What is digital economy?* Sitio Web de Deloitte. Recuperado de https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital- economy.html

DOMÍNGUEZ, A. G. (2018). La Elaboración De Perfiles Y Su Impacto en Los Derechos Fundamentales. Una Primera Aproximación a Su Regulación en El Reglamento General De Protección De Datos De La Unión Europea. *Revista Derechos y Libertades*, (38), 107–139. https://doi.org/10.14679/1058

El Parlamento Europeo y el Consejo, (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las*

personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Recuperado de https://eur- lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0679

Enciclopedia Britannica, (s. f.). *Amazon.com*. Recuperado de https://www.britannica.com/topic/Amazoncom

Enciclopedia Britannica (s. f.). *Iphone*. Recuperado de https://www.britannica.com/technology/iPhone

Estudillo, G. J. (2001). *Surgimiento de la Sociedad de la Información*. Biblioteca Universitaria, vol. 4, núm. 2, julio-diciembre, 2001, pp. 77-86. Recuperado de http://www.dgb.unam.mx/servicios/dgb/publicdgb/bole/fulltext/volIV22001/pgs_77-86.pdf

European Commission. (2014). Case No COMP/M.7023 - PUBLICIS / OMNICOM. Bruselas. Recuperado de http://ec.europa.eu/competition/mergers/cases/decisions/m7023_20140109_20310_3566669_EN.pdf

European Commission. (2012). *SEC(2012) 72 final, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Recuperado de https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN

Facebook. (s. f.). *Our History*. Recuperado del sitio web de Facebook en: https://newsroom.fb.com/company-info/#our-history

FMI (Fondo Monetario Internacional). (2018). *Measuring the digital economy*. Washington D.C.: IMF Policy Papers. Recuperado de https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818- measuring-the-digital-economy

Gada, K. (2016). The Digital Economy in 5 minutes. *Forbes*. Recuperado de https://www.forbes.com/sites/koshagada/2016/06/16/what-is-the-digital-economy/#28aece207628

Garcerán, C., García, M., Cernuda, G., García, C., Ferrete D., & Níguez, M. (2018). *Máster en Ciberderecho - Módulo 2 Curso 2018 - 2019. La Regulación del ciberespacio*. Madrid España: ecix Group y UCAM.

Gómez-Barroso, J., & Feijóo-González, C. (2013) Información personal: la nueva moneda de la economía digital, *El profesional de la información*, julio-agosto 2013, vol 22, núm 4, pp. 290-296, Recuperado de https://recyt.fecyt.es/index.php/EPI/article/view/epi.2013.jul.03/17790

Google. (s. f.) *From the garage to the Googleplex*. Recuperado del sitio web de Google en: https://www.google.com/about/our-story/

HP Inc. *HP Policy Position, Security, Privacy and Data Protection*. Recuperado de http://h20195.www2.hp.com/V2/getpdf.aspx/c05033586.pdf

Internet Society. (s. f.). *History of the Future*. Recuperado del sitio de Internet Society en: https://www.internetsociety.org/internet/history-internet/brief-history-internet/#History-of-the-Future

Kuneva, M. (2009). *Keynote speech at the roundtable on online data collection, targeting and profiling.* Ref.: Speech/09/156. Bruselas, March 31. Recuperado de http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

Miège, Bernard (2000), *Les industries du contenu face à l'ordre informationnel*, Presses Universitarires de Grenoble, Francia.

Pardo, O. (26 de enero 2018). El pastel es de Google y de Facebook. *El Mundo*, España. Recuperado de https://www.elmundo.es/extras/dia-publicidad/2018/01/26/5a6aece022601db94b8b4607.html

Peña-Lopez, I. (2010). *Fundamentos tecnológicos del Derecho de la Sociedad de la Información*. En Peguera Poch, M. (Coord.), Principios de Derecho de la Sociedad de la Información (pp. 51-123). Pamplona España: Editorial Aranzadi.

Pérez, A. (2011). *Internet y los derechos humanos*. Anuario de Derechos Humanos, Nueva Época. Vol. 12. 2011 (287-330). Recuperado de http://revistas.ucm.es/index.php/ANDH/article/view/38107

Puyol M., J. (2016). *Los Principios del Derecho a la Protección de Datos*. En Piñar M., J. (Director), Reglamento General de Protección de Datos Hacia un nuevo modelo europeo de privacidad (pp. 135-150). Madrid España: Editorial Reus.

Recio G., M. (2016). *Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control*. En Piñar

M., J. (Director), Reglamento General de Protección de Datos Hacia un nuevo modelo europeo de privacidad (pp. 351-366). Madrid España: Editorial Reus.

Recio G., M. (2016). *El Delegado de Protección de Datos*. En Piñar M., J. (Director), Reglamento General de Protección de Datos Hacia un nuevo modelo europeo de privacidad (pp. 367-387). Madrid España: Editorial Reus.

Schwabe, J. (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán*. Recuperado de https://www.kas.de/c/document_library/get_file?uuid=0a66a4a6- 1683-a992-ac69-28a29908d6aa&groupId=252038

Vilasau, M. y Vila, M.A. (2010). *Intimidad y datos personales en Internet*. En Peguera Poch, M. (Coord.), Principios de Derecho de la Sociedad de la Información (pp. 151-216). Pamplona España: Editorial Aranzadi.