ANÁLISIS AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA: UN VISTAZO A LA ACTUALIDAD DE LA ERA DIGITAL.

THE ANALYSIS OF THE GENERAL DATA PROTECTION REGULATION OF THE EUROPEAN UNIÓN: A LOOK AT THE CURRENT DIGITAL ERA.

Olbin Mejía Cambar [1]
DOI: https://doi.org/10.5377/lrd.v40i1.8909

RESUMEN

Esta investigación jurídica examina y analiza el contexto actual de la protección de los derechos fundamentales en la era digital, como el derecho a la privacidad, que es especialmente vulnerable debido a las constantes violaciones perpetradas por los motores de búsqueda y las redes sociales. Por otro lado, se explorarán las primeras reacciones al Reglamento General de Protección de Datos (RGPD) en la Unión europea sobre si bastará con regular los servidores digitales como los mencionados anteriormente de la academia europea y tratar de analizar cuál será la ruta para los próximos años para que la región centroamericana pueda tener una regulación cohesionada con las economías más importantes del mundo.

PALABRAS CLAVE: Big Data, RGDP, Red Social, Protección de Datos Personales, Derechos Fundamentales, Privacidad, Unión Europea, Facebook.

ABSTRACT

This legal investigation examines and analyzes the current context regarding the protection of fundamental rights in the digital era such as the right of privacy, which is especially vulnerable because of the constant breaches perpetrated by search engines and social networks. On the other hand, it will be explored the first reactions to the General Data Protection Regulation (GDPR) in the European union on whether if it will be enough to regulate digital servers as the above mentioned from the European Academy and try to analyze which will be the route for years to come in order for the Central American region to have a cohesive regulation with the most important economies of the world.

KEY WORDS: Big Data, GDPR, Social Network, Personal Data Protection, Fundamental Rights, Privacy, European Union, Facebook.

Fecha de recepción: 09 de agosto del 2019
Fecha de aprobación: 19 de agosto del 2019

[1] Master y Doctorando Universidad Carlos III de Madrid. International Commercial Law LL.M. University of Westminster. Email olbin.meca@gmail.com

I. INTRODUCCIÓN

Los debates relativos a la protección de datos personales en la red pueden parecer novedosos, sin embargo, es un tema que tiene bastante tiempo de ser debatido y estudiado en el viejo continente y en el país de las barras y las estrellas. Ahora bien, en muchos países latinoamericanos se ha regulado la actividad del tratamiento de datos personales de los ciudadanos dentro de sus jurisdicciones; no obstante, en diferentes grados de desarrollo. En el caso de Honduras, lastimosamente aún no se cuenta con una Ley de Protección de Datos Personales. En este sentido, su regulación se concentra en la figura del habeas data en la Ley de Justicia Constitucional hondureña y la referencia al concepto de datos personales confidenciales desarrollado en la Ley de Acceso a la Información Pública en su artículo 3 numeral 7[2].

En el desarrollo del presente artículo, hay dos conceptos que el lector deberá tener en cuenta. El primero a exponer, es el de "información personal" y la ahora derogada Directiva 95/46[3] del Parlamento Europeo la define como *"toda información sobre una persona física identificada o identificable; se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*. Por otro lado, debe tenerse en cuenta el concepto del "tratamiento de datos", y la Directiva antes mencionada la desarrolla como "c*ualquier operación o conjunto de operaciones efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta , utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión; así como su bloqueo, supresión o destrucción."* Estos conceptos siguen siendo muy completos y son importantes para fines académicos en la materia. Además, los mismos no han sido socializados de manera extensiva en nuestra sociedad, por lo cual se considera vital hacer una referencia previa de los mismos, esperando así, facilitar la lectura del presente trabajo.

Con fundamento en lo antes expuesto, en las presentes líneas se realizará un estudio comparativo entre la nueva normativa en la materia perteneciente a la Unión Europea además de algunos países de la región incluyendo a Honduras, la cual desnuda la deuda pendiente del legislador nacional de proporcionar un instrumento adecuado a nuestra realidad social, el cual será trascendental en diversas áreas, como ser la actividad comercial en internet y fundamentalmente, la protección de la intimidad de la persona humana en la red.

En primer término, se desarrollará un apartado dedicado a hacer una sucinta referencia a la denominada "Era Digital", y como se ha ido desarrollando el desenvolvimiento de nuestras sociedades haciendo énfasis a las necesidades que han ido surgiendo por los avances tecnológicos. En el siguiente apartado se hará referencia a la protección de datos y su conceptualización como derecho humano fundamental y como ha venido siendo violentado por actividades comerciales en la red además de las redes sociales como Facebook, haciendo una referencia especial a la controversia suscitada en el escándalo de "Cambridge Analytica" en los Estados Unidos de América. De igual manera, se hará una referencia un poco más detallada de la regulación hondureña con algunos apuntes referentes a la regulación en otros países de la región. Por último, se analizarán las principales novedades dentro del Reglamento General de Protección de Datos que entró en vigencia en el continente europeo, reemplazando la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[2] Art. 3 Numeral 7) Datos personales confidenciales: Los relativos al origen étnico o racial, características físicas, morales o emocionales, domicilio particular, número telefónico particular, dirección electrónica particular, participación, afiliación a una organización política, ideología política, creencias religiosas o filosóficas, estados de salud, físicos o mentales, el patrimonio personal o familiar y cualquier otro relativo al honor, la intimidad personal, familiar o la propia imagen.

[3] Directiva 95/46 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

II. METODOLOGÍA

El presente estudio desarrollará un análisis teórico doctrinal tomando como fuente principal estudios académicos realizados en Europa además del análisis comparativo entre la normativa regional de países como El Salvador, Guatemala, Costa Rica, y Colombia y la reciente regulación en la materia en el viejo continente por medio del Reglamento General de Protección de Datos (RGDP) con la finalidad de introducir al lector a la realidad y conflictividad que surge de las actividades de tratamiento de datos a nivel mundial y cuales deberán ser las prioridades para el legislador hondureño en esta materia.

III. LA ERA DIGITAL.

Las redes sociales han evolucionado de un simple pasatiempo, a una parte importante de nuestra vida cotidiana en las cuales se realiza el tratamiento de grandes cantidades de información, incluyendo datos personales de sus usuarios. Con el paso del tiempo, el flujo de datos se ha vuelto abrumador y poco a poco se ha ido creando una "identidad digital" de cada ser humano. En este sentido, hay autores que hablan de la existencia de una "digital personae" y Roosendaal expone que *"[...] es una representación digital de un individuo del mundo real, e incluye una cantidad suficiente de datos personales para servir, dentro del contexto y con el propósito de su uso, en representación del individuo"*[4].

Con el pronto acceso generalizado de Internet a nivel mundial durante los años 90, la protección de los derechos y libertades fundamentales de las personas naturales, y, en particular, el derecho a la privacidad relacionada con el procesamiento de datos personales se convirtió en una cuestión importante de tratar en las grandes potencias económicas y las organizaciones internacionales. Teniendo en cuenta estos argumentos, los legisladores europeos comprendieron este contexto y comenzaron a construir una regulación adecuada para todas las actividades en las que los datos personales podrían ser tratados a través de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas en relación con el tratamiento de datos personales y la libre circulación de dichos datos (D/95/46 en adelante). Esta Directiva se convirtió en un instrumento imprescindible en esta materia y ha sido el modelo no sólo para las naciones de la UE, sino también para el resto del mundo.

Ahora la información es un recurso increíblemente valioso para gobiernos y empresas multinacionales por una gran variedad de factores. Una vez procesada y clasificada la misma, puede proporcionar insumos útiles para muchos fines, entre ellas una de las más comunes es la actividad publicitaria. En este orden de ideas, es notorio que algunos de los gigantes de la red como Facebook se han lucrado al tratar información personal, y esta actividad ha representado un instrumento importante para diferentes modelos de negocio rentables a costas de violación de la privacidad de millones de personas. Por tanto, estas actividades solo confirman la pertinencia de una regulación adecuada de todas las actividades económicas que reúnan, agreguen, analicen y moneticen datos relacionados con una persona física[5].

Varios años después de la entrada en vigor de la D/95/46, nos dirigimos a la era del "Big Data", y 2018 fue un año en el que ocurrieron varios hechos importantes de mencionar. Por un lado, el mundo fue testigo del testimonio otorgado por Mark Zuckerberg ante el Senado de los Estados Unidos de Norteamérica sobre el escándalo "Cambridge Analytica" por la violación masiva de los derechos de privacidad (y recolección de datos) de millones de usuarios para beneficiar supuestamente campañas políticas en Norteamérica y Europa[6]. Este escándalo ha demostrado las amenazas y la gran responsabilidad de los Estados en cuanto al control del flujo de información y la protección de los derechos humanos en la era digital. Por lo tanto, es posible cambiar el curso de todo un proceso electoral nacional

[4] Roosendaal, A. (2013). "Digital personae and profiles in law". City: Wolf Legal Publishers, 255. p. 41.

[5] Esteve, A. (2017), "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA" [February] Volume 7(Issue 1) International Data Privacy Law 36–47, p. 36.

[6] Rosemberg, M., Confessore, N., Cadwallardr, C. (2018). "How Trump Consultants Exploited the Facebook Data of Millions". New York Times, 17 de marzo, pág. A1. Accesible en:https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html .

manipulando a los votantes a través del acceso invasivo a su privacidad en las redes sociales para comprender sus gustos y preferencias. Por lo tanto, el trasfondo político que puede tener esta actividad es impresionante y preocupante al mismo tiempo si se piensa en las posibles consecuencias de su utilización en contra de los intereses generales de la sociedad.

De igual manera, Isaak & Hanna exponen que estas actividades tienen una influencia tangible en los derechos de los ciudadanos tales como el debido proceso, y derechos constitucionales como la libertad de expresión, votar, y no discriminación. Por lo tanto, nunca ha sido más imperativo tener una discusión abierta sobre la proliferación de la tecnología y cómo afectarán los derechos de privacidad y seguridad personal y a nivel nacional[7]. Por tanto, es notoria la importancia de una adecuada y efectiva regulación de las nuevas tecnologías en las sociedades modernas.

También durante 2018, los trabajos finales relativos al Reglamento General de Protección de Datos (RGDP) estaban en camino y este entró en vigencia en los países de la UE el 25 de mayo de 2018. Por otro lado, miembros del Parlamento Europeo afirmaron que "*el cambio de una Directiva a un Reglamento en sí mismo es un cambio revolucionario: En lugar de que los Estados miembros tengan que transponer todas y cada una de las disposiciones al derecho interno con amplia discreción, el RGDP regula ahora casi todas las cuestiones directamente*[8] *y sólo deja poderes de especificación excepcionales a los Estados miembros que entonces tienen que justificar siempre cualquier divergencia con el objetivo de un marco jurídico plenamente armonizado, como lo concerniente a las leyes de medios de comunicación y prensa o a la seguridad y defensa nacionales"*[9]. Más adelante en el presente ensayo se detallarán algunas de las novedades principales incorporadas en el RGDP.

[7] Isaak, J., & Hanna, M. J. (2018). "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection". *Computer,* 51(8), 56-59, p. 57.

[8] Vid. Tratado de Funcionamiento de la Unión Europea Artículo 288 (antiguo artículo 249 TCE) Para ejercer las competencias de la Unión, las instituciones adoptarán reglamentos, directivas, decisiones, recomendaciones y dictámenes. El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

[9] Albrecht, J. P. (2016), "How the GDPR Will Change the World" Volume 2 (Issue 3) European Data Protection Law Review 287 – 289, p. 287.

IV. PROTECCIÓN DE DATOS PERSONALES COMO DERECHO HUMANO.

No es un hecho nuevo que el derecho de acceso y control de nuestros datos personales se considere un derecho humano fundamental como una extensión del derecho a la privacidad e intimidad. Esto puede interpretarse en numerosos tratados y convenciones de todo el mundo[10], tal es el caso de los artículos 17 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[11] y el artículo 11 de la Convención Americana sobre Derechos Humanos[12] solo para dar unos ejemplos.

No siempre ha existido una vinculación expresa entre el derecho a la intimidad y la protección de la información personal; sin embargo, la doctrina se ha construido a base de jurisprudencia, y algunos de los casos más notorios del Tribunal Europeo de Justicia son "Google Spain SL, Google Inc. v Mario Costeja González"[13] en donde se introdujo el concepto de "derecho al olvido" con respecto a la información personal contenida en los motores de búsqueda en la web y "Facebook v. Irlanda en Safe Harbour", donde se afirmó que en virtud del artículo 25 de la D/95/46, se prohíben las transferencias de datos a terceros países a menos que dichos países proporcionen "un nivel adecuado de protección de datos"[14].

En el caso del Sistema Interamericano de Derechos Humanos (SIDH), falta un largo camino por recorrer, si bien hay jurisprudencia en materia de violación de la privacidad (de comunicaciones telefónicas para ser más preciso)[15], aún no existe una referencia expresa

[10] Bygrave Asunción (1998), "Data protection pursuant to the right to privacy in human rights treaties" [1 January 1998] Volume 6 (Issue 3) International Journal of Law and Information Technology 247–284 p. 247.

[11] ECHR Caso Halford v Reino Unido (27 de mayo de 1997) 1997-III 1 pars. 44 y 45

[12] Corte IDH Caso Escher y otros v Brasil, (6 de julio de 2009) pars.113 y 114.

[13] ECJ C-131/12 Google Spain SL, Google Inc. v AEPD, Mario Costeja González (December 2014) Human Rights Law Review, Volume 14, Issue 4, 761–777. The "right to be forgotten" [...] in the Google case suggests that the erasure of irrelevant or unwanted data is a necessary.

[14] Esteve (2017) op. cit. p. 37.

[15] Corte IDH Case Escher and others v Brasil, parr. 114. En cuanto a este caso, es importante mencionar que en el Sistema Interamericano

a la materia de protección de datos personales en la red. Sin embargo, con fundamento en la doctrina moderna del derecho a la privacidad, algunos Estados de la región latinoamericana han introducido en su normativa constitucional la acción judicial constitucional de "habeas data"[16]. La misma procura conceder a una persona física el acceso/control/ modificación de sus datos personales en poder de una institución específica (normalmente instituciones financieras como bancos) que previamente se le ha negado el acceso a él por cualquier razón en particular y será discutido en mayor detalle en el próximo apartado.

Basándose en los argumentos antes expuestos, y teniendo en cuenta la naturaleza del derecho fundamental a la privacidad en la sociedad de la información, los modelos de negocio de las redes sociales y los motores de búsqueda que en esencia implican procesos de recolección de datos, siguen siendo una gran preocupación para las autoridades de todo el mundo. Bajo estos modelos, la mayor parte de la información personal es otorgada voluntariamente por los usuarios cuando se registran y crean un perfil en una red social. En el caso de Facebook, se suele animar a revelar información sobre otras personas y también ha tratado de rastrear los datos personales del no-usuario por lo general a través del Botón de "me gusta". Inclusive, hay autores como Gordon Hull de la Universidad de Carolina del Norte que exponen que en la sociedad se ha creado una especie de "paradoja de la privacidad", y se refiere a la discrepancia entre la preocupación que las personas expresan por su privacidad y el valor aparentemente bajo que realmente asignan cuando intercambian fácilmente información personal por productos de bajo valor en línea[17].

Después de clasificar la "materia prima" por parte de los servidores de una red social, se ofrecen a las empresas las herramientas para, inter alia, publicidad contextual[18]. En esta línea de ideas, exponen Isaak & Hanna que *"la ubicuidad de la recopilación de datos, almacenamiento y análisis en nuestros dispositivos, sistemas, aplicaciones y plataformas de medios sociales destinados a personalizar experiencias, optimizar ventas y maximizar el retorno han sido disruptivas en la configuración de la economía global, el flujo de ideas y el acceso a la información que han dado lugar al avance de la innovación en torno al mercado de la información"*[19]. De esta manera, detallan que, si bien la tecnología siempre buscará simplificar tareas diarias o mejorar condiciones comerciales, siempre uno de los grandes peligros será la invasión indiscriminada a nuestra información personal. Por consiguiente, y como consideran los expertos y la jurisprudencia en la materia, la mayoría de estas actividades pueden constituir una violación importante de la intimidad y privacidad este tipo de actividades son prioridad en la regulación del RGDP.

V. RÉGIMEN CONSTITUCIONAL HONDUREÑO

Ahora bien, en el caso de Honduras, en la Constitución de la República de 1982 en su artículo 76 la manifestación que se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen. Por otro lado, en principio la carta magna reconocía solamente las garantías Constitucionales[20] como el recurso de Amparo, la Inconstitucionalidad, Recurso de Revisión, y el Habeas Corpus. Transcurrieron más de 20 años para dar el siguiente paso con la introducción del Habeas Data en la normativa hondureña en el Decreto 243-2003 en el artículo 182 de la Constitución. Dicho artículo expresa que *"toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y o enmendarla"*. Ya en el año 2004 se introdujo el Habeas Data en la Ley de Justicia Constitucional en su artículo 13.

de Derechos Humanos aún no hay un precedente que haga mención propiamente a la protección de datos personales en la red. No obstante, la sentencia en mención incluye una referencia interesante a la protección de la privacidad de la persona humana, que a su vez es el fundamento principal en cuanto a protección de datos personales.

[16] Decreto 244-2003 Ley Sobre Justicia Constitucional Art.13.2. en el caso hondureño.

[17] Hull, G. (2015). "Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data". Ethics and Information Technology, 17(2), 89-101, p. 89.

[18] Esteve (2017) op. cit. p. 39 y 40.

[19] Isaak, J., & Hanna, M. J. (2018). Op. Cit. p. 57.

[20] Se desarrollan en el título IV: Garantías Constitucionales de la Constitución de la República.

Por otro lado, son escasos los casos en esta materia en tribunales hondureños. Existen fallos de la Sala Constitucional de la Republica de Honduras que hacen referencia a la materia, como ser en el fallo SCO-0095-2014 del 3 de junio 2014[21] en donde un particular recurre contra la Central de Información Crediticia de la Comisión Nacional de Banca y Seguros (CNBS). El recurrente estableció que lo que motivó su recurso fue que se le negó acceder a sus datos relacionados al registro de su nombre en la Central de Información Crediticia de la CNBS, como deudor moroso a causa de una deuda sin cancelar desde 1996, lo cual afectó en su momento su historial crediticio. En ella la Sala dio con lugar el recurso y expuso lo siguiente:

> *"CONSIDERANDO: [..] esta Sala de lo Constitucional reconoce el derecho que asiste al señor G.M.M. de ser informado debidamente acerca de la deuda que se afirma tiene pendiente con la empresa [...], así como el derecho que tiene a que esta empresa le exhiba y le permita acceder, sin más trámite ni formalidad, a todos los documentos en los que se ampara la manifestada deuda[22]".*

En este sentido, la Sala Constitucional es del criterio que el derecho que se tutela a través del Habeas Data, incluye fundamentalmente el derecho de acceder a los registros públicos o privados, en los cuales estén incluidos datos personales y conlleva, además, la facultad de poder verificar la exactitud de esos registros. La mayoría de las causales de los Recursos de Habeas Data tienen que ver con el régimen de consumo financiero, donde los principales conflictos surgen a través del ente regulador de las instituciones financieras en Honduras.

VI. PROTECCIÓN DE DATOS EN LA REGIÓN CENTROAMERICANA.

Como se expuso anteriormente, en Latinoamérica, la protección de datos personales se ha regulado en diferentes grados de ejecución. En este sentido, es importante hacer un repaso también del corpus iuris regional en la materia. En esta línea de ideas, en la nación hermana de Guatemala, se encuentra una estructura similar a la hondureña, en el sentido de que los conceptos referentes a la protección de datos personales se han encasillado dentro de una "Ley de Acceso a la Información Pública", y en su art. 1 numeral dos expone que dicha ley busca *"Garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos",* siendo el instrumento para su garantía el habeas data, la cual se encuentra desarrollada en la dicha ley de acceso a la información pública[23].

De igual manera, hacen un acercamiento interesante en cuanto al otorgamiento del consentimiento por parte de un usuario para el tratamiento de datos personales. En sus artículos 31 al 35 se plantea que: *"Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información".*

Es importante señalar que debe entenderse por "sujeto obligado" la persona o institución que pretende realizar un tratamiento de datos personales. Por otro lado, se introduce una sanción por comercialización de datos personales[24].

[21] Sentencia nº HD-0095-14 de Corte Suprema de Justicia, 3 de Junio de 2014 https://hn.vlex.com/vid/593450722 Revisado por última vez en fecha 5/11/19.

[22] Ídem.

23 DECRETO NÚMERO 57-2008 LEY DE ACCESO A LA INFORMACIÓN PÚBLICA (Guatemala) ARTICULO 30. Habeas data. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán: 1. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos que sean, presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos; 2. Administrar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido; 3. Poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento; 4. Procurar que los datos personales sean exactos y actualizados; 5. Adoptar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado. Los sujetos activos no podrán usar la información obtenida para fines comerciales, salvo autorización expresa del titular de la información.

[24] ARTICULO 64. Comercialización de datos personales. Quien

En el caso de El Salvador, seguimos con la misma tendencia de incluir la protección de datos en la normativa de acceso a la información pública, y en su artículo 3 literal h expone que dentro de los fines de su ley existe el deber de *"Proteger los datos personales en posesión de los entes obligados y garantizar su exactitud"*[25]. A diferencia del caso hondureño y guatemalteco, en El Salvador únicamente se presenta un procedimiento administrativo a fin de que una persona afectada pueda tener acceso a su información personal.

En Costa Rica, existe la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales Ley n.º 8968 Publicada en La Gaceta n.º 170 de 05 de setiembre de 2011 y en su artículo 4 presenta un concepto que me gustaría rescatar para el presente estudio, el cual es la "Autodeterminación informativa", la cual consiste en que *"toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección. Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias"*. De esta manera, se considera que el modelo tomado por el legislador de Costa Rica podría ser considerado por el poder legislativo y el Instituto de Acceso a la Información Pública (IAIP) de Honduras, considerando que esa ha sido la tendencia en el resto de Latinoamérica siendo liderados por países como Colombia y su ley 1581 de 2012[26], la cual es reconocida por su rica jurisprudencia en materia de garantías constitucionales, como ser, inter alia, el Habeas Data[27].

VII. PRINCIPALES NOVEDADES EN CUANTO A LOS PRINCIPIOS RECTORES DE LA PROTECCIÓN DE DATOS EN EL RGPD Y LA ERA DEL BIG DATA.

Como se mencionó anteriormente, el flujo masivo de información es esencial en la era digital, e instrumentos como el Big Data pueden considerarse un ejemplo de su potencial abrumador y de cómo evolucionan las tecnologías de manera acelerada. Los gigantes orientales, como la República Popular de China, han reconocido su valor y han realizado importantes avances y estudios sobre los beneficios para el desarrollo económico y social que el "Big Data" puede ofrecer al mundo.[28] Según Zarsky, en el proceso de Big data, "la información se recopila utilizando múltiples sensores, así como a través de varias aplicaciones que registran los movimientos de los usuarios, comunicaciones y transacciones. Se almacena utilizando mecanismos sofisticados en bases de datos distribuidas, cuyo costo se reduce constantemente. Por último, se utiliza en procesos analíticos avanzados y posteriormente se aplica en

comercialice o distribuya por cualquier medio, archivos de información de datos personales, datos sensibles o personales sensibles, protegidos por la presente ley sin contar con la autorización expresa por escrito del titular de los mismos y que no provengan de registros públicos, será sancionado con prisión de cinco a ocho años y multa de cincuenta mil a cien mil Quetzales y el comiso de los objetos instrumentos del delito. La sanción penal se aplicará sin perjuicio de las responsabilidades civiles correspondientes y los daños y perjuicios que se pudieran generar por la comercialización o distribución de datos personales, datos sensibles o personales sensibles.

[25] DECRETO No. 534 LEY DE ACCESO A LA INFORMACIÓN PÚBLICA DE EL SALVADOR Art. 36. Los titulares de los datos personales o sus representantes, previa acreditación, podrán solicitar a los entes obligados, ya sea mediante escrito libre, en los términos del artículo 66 de ésta ley o formulario expedido por el Instituto, lo siguiente: a. La información contenida en documentos o registros sobre su persona. b. Informe sobre la finalidad para la que se ha recabado tal información. c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control, en los términos del artículo 63 de ésta ley. d. La rectificación, actualización, confidencialidad o supresión de la información que le concierna, según sea el caso, y toda vez que el procedimiento para tales modificaciones no esté regulado por una ley especial.

[26] Ley Estatutaria 1581 DE 2012 (octubre 17) Diario Oficial No. 48.587 de 18 de octubre de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales República de Colombia.

[27] Vid. Corte Constitucional de Colombia Sentencia C-748-11 de 6 de octubre de 2011 " [...] Ciertamente, del derecho al habeas data se desprenden no solamente las facultades de conocer, actualizar y rectificar las actuaciones que se hayan recogido sobre el titular, sino también otras como autorizar el tratamiento, incluir nuevos datos, o excluirlos o suprimirlos de una base de datos o archivo. Por tanto, si bien la disposición se ajusta a la Carta, no debe entenderse como una lista taxativa de las garantías adscritas al derecho". Resumen Accesible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html (Revisado por última vez en 2/11/19).

[28] Uno de los mejores ejemplos es "Jusfoun Big Data Information Group Co., Ltd", una corporación china dedicada a servicios basados en Big Data para las economías emergentes de todo el mundo. Vid. http://en.jusfoun.com/ABOUT/index.jhtml. (Revisado por última vez 12/11/19).

diversos contextos"[29]. Además, se puede afirmar que en el caso de "Cambridge Analytica", las redes sociales eran la herramienta perfecta para este tipo de actividad, que, bajo los motivos equivocados, puede tener consecuencias nefastas.

Teniendo en cuenta todas estas amenazas, la UE se esmeró en presentar al mundo el Reglamento General de Protección de Datos (RGDP) y se considera el proyecto más ambicioso en la materia desde la Directiva 95/46/CE[30]. Este *corpus iuris* propone renovar y adaptar la regulación a las normas actuales que han surgido a través de los nuevos avances tecnológicos. El profesor Zarsky expresa que *"lo más probable es que el impacto del RGDP sea profundo. Tal vez sea el instrumento legislativo más completo y orientado hacia el futuro para abordar los retos a los que se enfrenta la protección de datos en la era digital"*[31].

Por otro lado, según el IT GOVERNANCE PRIVACY TEAM *"El RGDP en términos generales establece los requisitos específicos que deben cumplir las entidades incluidas en el ámbito de aplicación del reglamento"*[32], y continúan explicando que tiene dos objetivos principales:

"Proteger los derechos, la privacidad y las libertades de las personas físicas en la UE y reducir los obstáculos a las empresas facilitando la libre circulación de datos en toda la UE".

Además, otros académicos de la UE han mencionado que el RGDP amplía las obligaciones de los procesadores de datos, y se introducen sanciones más severas por no cumplir con sus disposiciones, formando un cambio importante tanto para relaciones contractuales como para las relaciones no contractuales entre los procesadores de datos y los controladores de datos.[33]

Entrando ya en materia, el Reglamento tiene dos objetivos principales, regular un derecho (la protección de datos personales) y garantizar una libertad (libre circulación de datos[34])[35], además contiene varias novedades puntuales en su texto, la primera es en relación a sus principios rectores en su artículo 5. Es importante mencionar que los principios más importantes son los de tratamiento licito y leal de los datos personales. Estos implican, que el tratamiento de datos personales debe responder a fines determinados, explícitos y legítimos y que estos no podrán ser tratados posteriormente de manera incompatible con tales fines. Por otra parte, esta información no deberá ser conservada más tiempo que el preciso para realizar los fines que motivaron el tratamiento[36].

Junto al principio de licitud y de lealtad, la primera novedad es el principio de transparencia en el tratamiento de los datos de carácter personal. El mismo supone el derecho que tiene el titular de los datos a estar informado de manera clara e inequívoca sobre dicho tratamiento. En este sentido Mayor Gómez expone que "el interesado debe poder conocer en todo momento quién, cómo y para qué están tratando sus datos personales, así como qué datos personales exactamente están siendo tratados e incidencias que

[29] Zarsky, T. Z. (2017) "Incompatible: The GDPR in the Age of Big Data" 47 Seton Hall Law Review 995-1018 p. 999.

[30] En España, fue aprobado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos (BOE núm. 183, de 30/07/2018) Vid. Dopazo Fraguío, P. (2018) "El derecho a la protección de datos y delimitación del "derecho al olvido" en la Unión Europea". RUE: Revista Universitaria Europea, Nº. 30, 2019, págs. 57-90 p. 89.

[31] Zarsky (2018) Op. Cit. p. 995.

[32] ITGP Governance Privacy Team (2016), "EU General Data Protection Regulation (GDPR) : An Implementation and Compliance Guide". IT Governance Publishing.

[33] Lindqvist, J. (2018) "New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?" [Spring 2018] Volume 26 (Issue 1) International Journal of Law and Information Technology P. 45–63, p. 46.

[34] De igual manera, es importante mencionar que también está el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea. Vid. *Artículo 1:* Objeto El presente Reglamento tiene por objeto garantizar la libre circulación en la Unión de datos que no tengan carácter personal mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales.

[35] Piñar Mañas J. L. (dir.), Álvarez Caro, M. (coord.), Recio Gayo, M (coord.) (2018). Reglamento general de protección de datos: Hacia un nuevo modelo europeo de protección de datos. Editorial Reus p. 52.

[36] Guerrero Picó, M. C. (2005). "El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea". Revista de derecho constitucional europeo, (4), 293-332. pág. 302.

se produzcan sobre los mismos. *[...]. El reconocimiento del principio de transparencia implicará, indirectamente, un aumento de la información que el responsable del fichero debe facilitar al titular de los datos con carácter previo al momento de obtener sus datos personales o al momento de aplicar los ya recabados a una nueva finalidad"*[37].

Otro aspecto importante que desarrolla en mayor medida el RGPD es lo relativo al consentimiento, aspecto que conforme a la doctrina de la protección de datos personales representa un pilar en la validez del tratamiento de información en cualquier tipo de actividad. En su artículo 7 se presentan algunas condiciones para el consentimiento de los usuarios. En su apartado primero expone *"Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales"*. El resto del articulo pretende que el consentimiento sea otorgado de manera expresa, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo (numeral 2).

En cuanto al acceso de niños a servicios de la sociedad de la información, el Reglamento en su artículo 8 busca regular dicha situación. En su redacción expone que *"el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó"*. Hay que hacer hincapié en que este aspecto no estaba incluido en la Directiva 95/46 y viene a reforzar todos los posibles escenarios que pudieran surgir en cuanto al consentimiento. Un ejemplo claro de la importancia de este nuevo apartado, podría ser el caso de los juegos de video en teléfonos móviles, en donde los menores se pueden ver vulnerados al querer registrar su progreso y compartirlo en redes sociales sin estar conscientes de las posibles consecuencias de sus acciones.

[37] Mayor Gómez, R. (2016). "Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)". Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha, (6), 243-280 p. 255.

Algo que hay que resaltar, es la trascendencia de la jurisprudencia europea en la materia, y su influencia se tradujo en la redacción del artículo 17 del RGDP, en donde se exponen los principios relativos al "Derecho al olvido" desarrollado en la sentencia de "Costeja vs Google Spain" y expone que *"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales"*. De igual manera sucede con lo referente a las reformas realizadas en cuanto a las transferencias internacionales de información con fundamento en la sentencia de "Safe Harbour" en sus artículos 44 a 50. En este sentido el profesor Mayor Gómez expone que "si los datos personales se transfieren de la Unión Europea a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión Europea por el nuevo reglamento de protección de datos, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional"[38].

VIII. PRIMEROS RESULTADOS DEL RGDP EN 2019.

Conforme a datos de la Comisión Europea, el primer año de vigencia del RGDP ha sido alentador, y las acciones por parte de los interesados han ido encaminadas a cumplir a cabalidad con el texto del Reglamento a pesar de las dificultades que surgen del proceso de adaptación a un cambio considerable como el que presenta el Reglamento. En su informe "Special Eurobarometer 487a", la Comisión expone que más de dos tercios de los europeos han oído hablar del GDPR y de la mayoría de los derechos garantizados por este. Además casi seis de cada diez han oído hablar de una autoridad nacional que protege sus datos[39].

Otro dato interesante que expone dicho informe es

[38] Mayor Gómez, R. (2016). Op. Cit. p. 264

[39] Comisión Europea (2019) "Special Eurobarometer 487ª The General Data Protection Regulation" June 2019, p. 2. Revisado por última vez el 05/11/19. Accesible en: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222

que la mayoría de usuarios de redes sociales (56%) han intentado cambiar la configuración de privacidad predeterminada de su perfil[40].

En cuanto a números, la Comisión Europea reporta 89,271 denuncias presentadas por usuarios ante autoridad competente por violación a la privacidad. Por otro lado, en cuanto a multas, se reportó que en Francia se multó a Google por no solicitar su consentimiento a usuarios en cuanto a publicidad en su buscador, y en Alemania, una red social fue multada por no proteger la información de sus usuarios conforme a los estándares desarrollados en el Reglamento[41].

Como se observa, hay un progreso considerable en el continente europeo, y mientras se siga socializando de manera masiva y se desarrolle la infraestructura necesaria en todos los Estados, para el 2020 pueda que se tengan mejores estadísticas en esta materia. Mientras tanto, en Latinoamérica quedamos pendientes del futuro desarrollo de esta regulación tan importante y por medio de sus futuros resultados, se podrá tener insumos importantes para nuestra región.

IX. CONCLUSIONES

- Han surgido grandes expectativas con respecto a esta normativa que pretende garantizar la privacidad de los ciudadanos de la UE en la era del Big Data descrita por Zarsky, y las normas desarrolladas por todos los principales casos en el continente europeo. Las sociedades se adaptan constantemente a sus necesidades a lo largo del tiempo, que pueden verse afectadas, entre otras cosas, por indicadores económicos, políticos o tecnológicos; en consecuencia, también por su legislación. De hecho, con el RGDP, las redes sociales tienen una regulación más compleja y quizás más precisa, no obstante, será vital para la UE revisar periódicamente su legislación considerando que pueden surgir nuevos modelos económicos digitales, tal y como se ha observado con el "Big Data". Además, esta supervisión no puede efectuarse únicamente entre los Estados de la Unión Europea, también será imperativo trabajar en políticas públicas y acuerdos multilaterales sobre el tema con las economías más fuertes del mundo.

- Por otro lado, a pesar de pertenecer a una región que no tiene esta materia tan arraigada en su normativa interna como a nivel regional, es importante estar informados en cuanto a las nuevas tendencias en el continente europeo tomando en consideración que estas terminan siendo referentes para Latinoamérica. Hay que recordar que no estamos exentos de la influencia de estas nuevas tecnologías en nuestras democracias, además que el comercio electrónico cada vez se va extendiendo en el mercado global. Por tanto, si se desea crear mayor apertura comercial en nuestra región será importante contar con la regulación correspondiente en esta materia y muchas otras. En este sentido, el Sistema de Integración Centroamericano (SICA), debería de tomar cartas en el asunto considerándolo parte de los objetivos relativos al desarrollo económico y protección de garantías fundamentales en la región.

- Se espera que nuestro país logre salir de la crisis existente con varios sectores importante de nuestra sociedad, contexto para nada propicio para el resguardo de garantías fundamentales de los hondureños. Está claro que esa debe ser la prioridad de nuestras autoridades previo a desarrollar de manera amplia temas como los expuestos en este ensayo. Sin embargo, este es un tema importante a fin de crear mayor seguridad jurídica en nuestro país y tiene que dársele la importancia correspondiente.

[40] Comisión Europea (2019) Op. Cit. p. 3.

[41] Comision Europea (2019) Infographic: GDPR in numbers 22 May 2019. Revisado por última vez el 05/11/19. Accesible en: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en#library

X. BIBLIOGRAFÍA

LIBROS Y ARTÍCULOS DE REVISTAS ESPECIALIZADAS.

- **Albrecht, J.P. (2016)** "How the GDPR Will Change the World" *European Data Protection Law Review Volume 2* (Issue 3) 287 – 289, p. 287.
- **Bygrave, L. (1998)** "Data protection pursuant to the right to privacy in human rights treaties" *International Journal of Law and Information Technology* [1 January 1998] Volume 6 (Issue 3)247–284 p. 247.
- **Dopazo Fraguío, P. (2018)** "El derecho a la protección de datos y delimitación del "derecho al olvido" en la Unión Europea. RUE: Revista Universitaria Europea, Nº. 30, 2019, págs. 57-90.
- **Esteve, A. (2017)** "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA" [February 2017] International Data Privacy Law Review Volume 7(Issue 1) 36–47.
- **Guerrero Picó, M. C. (2005).** "El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea". *Revista de Derecho Constitucional Europeo*, (4), 293-332.
- **Hull, G. (2015).** "Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data". *Ethics and Information Technology,* 17(2), 89-101, p. 89.
- **Isaak, J., & Hanna, M. J. (2018).** "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection". *Computer,* 51(8), 56-59.
- **Lindqvist, J. (2018)** "New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?" *International Journal of Law and Information Technology* [Spring 2018] Volume 26 (Issue 1) P. 45–63
- **Mayor Gómez, R. (2016).** "Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)". *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha* (6), 243-280.
- **Piñar Mañas J. L.** (dir.), Álvarez Caro, M. (coord.), Recio Gayo, M (coord.) (2018). *"Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de protección de datos".* Editorial Reus p. 52.
- **Roosendaal, A. (2013)**." Digital personae and profiles in law". City: *Wolf Legal Publishers, 255.*
- **Zarsky, T. Z. (2017)** "Incompatible: The GDPR in the Age of Big Data" 47 Seton Hall Law Review 995-1018.

JURISPRUDENCIA:

- Corte Constitucional de Colombia Sentencia C-748-11 de 6 de octubre de 2011.
- TEDH Caso Halford v Reino Unido (27 de mayo de 1997) 1997-III.
- Corte IDH Caso Escher y otros v Brasil, (6 de julio de 2009).
- ECJ C-131/12 Google Spain SL, Google Inc. v AEPD, Mario Costeja González (December 2014) Human Rights Law Review, Volume 14, Issue 4, 761–777.
- ECJ C-362/14 Petición de decisión prejudicial planteada por la High Court-Irlanda-Maximillian Schrems/Data Protection Commissioner, (6 de octubre de 2015).
- Sentencia nº HD-0095-14 de Corte Suprema de Justicia de Honduras, 3 de junio de 2014.

OTRAS FUENTES:

- ITGP Governance Privacy Team, EU General Data Protection Regulation (GDPR) : an implementation and compliance guide. [2016] IT Governance Publishing.

- Comisión Europea (2019) "Special Eurobarometer 487ª The General Data Protection Regulation" June 2019.

- Comisión Europea (2019) Infographic: GDPR in numbers 22 May 2019.

- Rosemberg, M., Confessore, N., Cadwallardr, C. (2018). "How Trump Consultants Exploited the Facebook Data of Millions". New York Times, 17 de marzo, pág. A1.