TRABAJO DE FIN DE GRADO

EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y EL EFECTO BRUSELAS:

¿UN MODELO PARA PAÍSES EN DESARROLLO?

Autor:

Adrián Morcillo Pazos

Directora del Trabajo:

María Jesús García Morales

Entrega: 10/05/2021

Grado:

6º Doble Grado en Derecho y Administración y Dirección de Empresas

RESUMEN

El Reglamento General de Protección de Datos (RGPD) adoptado en la Unión Europea ha establecido los estándares más altos de todas las políticas de privacidad de datos existentes. Para garantizar su cumplimiento extraterritorial, la UE ha adoptado un enfoque estricto: los países que deseen interactuar con los usuarios digitales en la UE deben cumplir obligatoriamente con las amplias obligaciones del RGPD o renunciar al acceso al bloque comercial más grande del mundo.

Esto ha provocado una oleada de reformas, tanto en organizaciones internacionales o empresas, como en terceros países ajenos a la UE, que adaptan sus propias regulaciones nacionales para intentar actualizarse conforme a la normativa europea. No obstante, esto presenta obstáculos importantes para los países en desarrollo. En estos últimos, los múltiples requisitos de adecuación y sus costes asociados, la ausencia de leyes nacionales que cumplan con el RGPD, la carencia de un Estado de derecho estable para hacer cumplir tales leyes y la infraestructura tecnológica deficiente, son algunos de los factores por los que la inspiración en el RGPD tal vez no sea la mejor vía de inicio.

RESUM

El Reglament General de Protecció de Dades (RGPD) adoptat a la Unió Europea ha establert els estàndards més alts de totes les polítiques de privacitat de dades existents. Per garantir el seu compliment extraterritorial, la UE ha adoptat un enfocament estricte: els països que desitgin interactuar amb els usuaris digitals a la UE han de complir obligatòriament amb les àmplies obligacions del RGPD o renunciar a l'accés del bloc comercial més gran del món.

Això ha provocat una onada de reformes, tant en organitzacions internacionals o empreses, com en tercers països aliens a la UE, que adapten les seves pròpies regulacions nacionals per intentar actualitzar-les d'acord amb la normativa europea. No obstant, això presenta obstacles importants per als països en desenvolupament. En aquests últims, els múltiples requisits d'adequació i els costos associats, l'absència de lleis nacionals que compleixin amb el RGPD, la manca d'un

Estat de dret estable per fer complir aquestes lleis i la infraestructura tecnològica deficient, són alguns dels factors pels quals la inspiració en el RGPD potser no és la millor via d'inici.

ABSTRACT

The General Data Protection Regulation (GDPR) adopted in the European Union has established the highest standards of all existing data privacy policies. To ensure the extraterritorial enforcement, the EU has taken a strict approach: countries wishing to interact with digital users in the EU must either comply with the broad obligations of the GDPR or renounce to access the world's largest trading bloc.

This has caused a wave of reforms, both in international organizations or companies, and in third countries outside the EU, which adapt their own national regulations to try to update themselves in accordance with european regulations. However, this presents significant obstacles for developing countries. In the latter, the multiple adequacy requirements and their associated costs, the absence of national laws that comply with the GDPR, the lack of a stable rule of law to enforce such laws and the deficient technological infrastructure, are some of the reasons why inspiration in the GDPR may not be the best way to start.

ÍNDICE

ABREVIATURAS

BCR: Reglas corporativas vinculantes

BRI: Belt and Road Initiative

C108: Convenio 108

C108+: Convenio 108+ (actualizado en línea con el RGPD)

CCPA: Ley de Protección al Consumidor de California

CE: Comisión Europea

CEDH: Convenio para la protección de los derechos humanos y de las libertades fundamentales

CEPD/EDPB: Comité Europeo de Protección de Datos

CoE: Consejo de Europa

DPA: Ley de Protección de Datos (en referencia a Kenia)

DPD: Directiva de Protección de Datos

ECIPE: Centro Europeo para la Economía Política Internacional

EEUU: Estados Unidos

EEE: Espacio Económico Europeo

PRIDA: Asociación de Economía Digital África-Europa

PYMES: Pequeñas y Medianas Empresas

RGPD/GDPR: Reglamento General de Protección de Datos

SCC: Cláusulas contractuales estándar

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

TJUE: Tribunal de Justicia de la Unión Europea

UA: Unión Africana

UE: Unión Europea

UNCTAD: Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

INTRODUCCIÓN

"¿Por qué Europa no estaría orgullosa de contribuir con sus exigentes estándares de respeto de los derechos fundamentales al mundo en general?"[1], respondió Koen Lenaerts, presidente del Tribunal de Justicia de la Unión Europea, durante una entrevista en 2015, haciendo referencia a cómo las exigencias del derecho de la Unión Europea (UE) estaban afectando al comercio internacional.

Es muy ilustrativa también la declaración que el presidente del TJUE realizó al ser preguntado por la anulación de "*Safe Habor*", al afirmar que se trataba de negociar entre iguales, pero cada parte haciéndolo desde la base de su identidad constitucional, donde los valores europeos de respeto al Estado de derecho no "estaban a la venta" (*"the rule of law is not up for sale"*).

La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo ha indicado que 128 de 194 países han implementado leyes de privacidad de datos recientemente[2]. De esta forma, aproximadamente el 66% de los países del mundo han promulgado legislaciones sobre protección de datos, lo que muestra la importancia que otorgan a la regulación de la transferencia de información en la era digital, especialmente importante a raíz del COVID-19.

El Reglamento General de Protección de Datos (RGPD), implementado en mayo de 2018 por la Unión Europea, ha marcado una nueva era para la protección de datos en todo el mundo. Aunque el RGPD sirve para armonizar las regulaciones de protección de datos dentro de los Estados miembros de la UE, muchos países fuera de la UE se han inspirado en él.

En consecuencia, muchos países de Europa, además de los Estados miembros de la UE, como Islandia, Liechtenstein, Noruega y Suiza, han cambiado

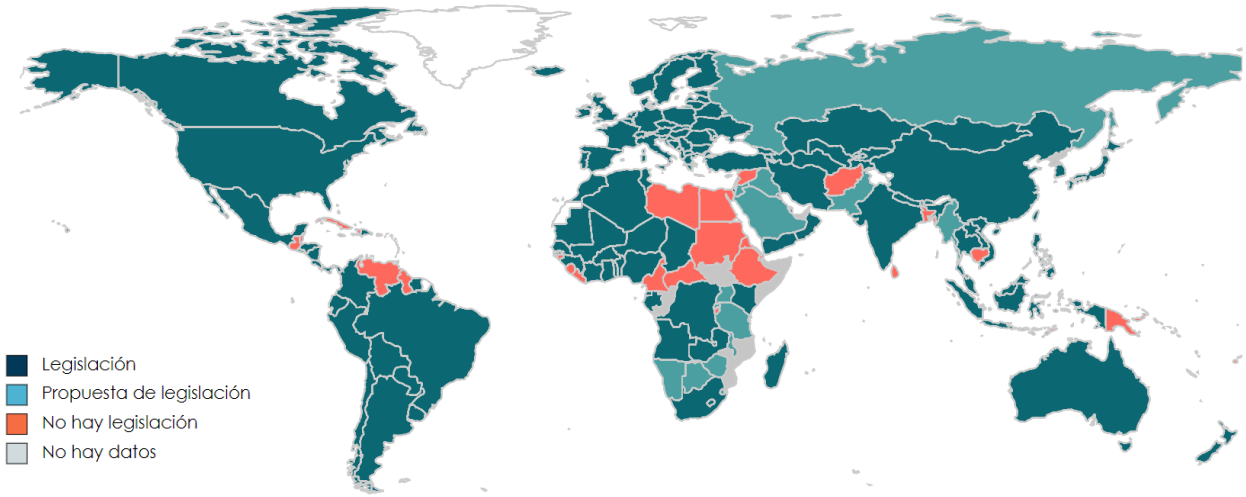
---

[1] POP, V., "*ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust*", en https://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/ (Fecha consulta: 06/03/2021).

[2] UNCTAD, "*Data Protection and Privacy Legislation Worldwide",* en https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Fecha de consulta: 16/01/2021).

sus leyes de protección de datos en armonía con el RGPD. Incluso otros países no europeos, como numerosos países de África, Asia, el Caribe y América Latina, están promulgando nuevas leyes de privacidad de datos o enmendando leyes anteriores para garantizar que la ley nacional esté en armonía con la norma europea. Incluso Estados Unidos no es inmune al enfoque de la UE: la Ley de Protección al Consumidor de California (CCPA) así lo demuestra.

Legislaciones de protección de datos en el mundo



Fuente: UNCTAD 2020

He elegido realizar mi trabajo de final de grado sobre la influencia del derecho de la UE en el mundo, eligiendo como ámbito comparativo a los países en desarrollo, en representación de esos terceros Estados que deben cumplir con las exigencias de los valores fundamentales que emanan de la tradición y jurisprudencia europea.

Considero que es un tema de relevancia principalmente por dos motivos. El primero es que la digitalización se ha globalizado y la pandemia ha acelerado estos procesos, afectando la privacidad de los individuos. Personalmente, concuerdo con la visión humanista de los principios del RGPD y los derechos que confiere me parecen necesarios para el respeto a la dignidad de la persona, por parte de Estados, empresas u organizaciones internacionales.

No obstante, países en desarrollo con recursos limitados tienen pocas posibilidades de lograr cumplir con estos requisitos. El presidente del TJUE afirmaba, en aquella entrevista de 2015, que Europa debería estar orgullosa de contribuir con sus exigencias del Estado de derecho al mundo y que "el mundo vería que hace con ellas". Si bien no tendría sentido que en transferencias internacionales se renunciase al rigor que el derecho de la UE tiene dentro de sus fronteras, me resultaría un error no ser conscientes del efecto perjudicial que este puede causar en otras partes del mundo.

El segundo motivo por el que considero que este es un tema muy interesante a tratar, reside precisamente en esos terceros Estados, como Kenia o India, que han establecido el RGPD como guía a seguir. Las exigencias del RGPD son profundas y los costes asociados muy elevados. Que prolifere entre países en desarrollo la visión europea de protección de datos en contraposición a las visiones más autoritarias y controladoras (China) o que priorizan la seguridad nacional y los poderes del Estado (EEUU), lo considero un gran éxito.

No obstante, deseo comprobar las posibilidades de éxito que tienen estas naciones de lograr una decisión de adecuación por parte de la Comisión. Los tribunales de la UE en su jurisprudencia respecto a la adecuación, no juzga a países ni sus sistemas, sino el respeto a los principios requeridos. A pesar de esto, tengo dudas de que países con recursos muy limitados puedan cumplir con estas exigencias sin reformas profundas en infraestructuras y a nivel legislativo, político y social.

Este interés personal me lleva a querer repasar las iniciativas y declaraciones de las instituciones europeas, con el fin de desarrollar unas conclusiones respecto mi pregunta inicial: ¿el RGPD supone una oportunidad para los países en desarrollo que han cedido a la visión europea de protección de datos (la más estricta del planeta) o, por el contrario, supondrá un aumento significativo de los costes para los empresarios de estos territorios y una herramienta controladora en manos de sus gobiernos?

La primera parte de este trabajo, comienza con un análisis de las posibles hipótesis de aceptación global y difusión de la norma europea. Posteriormente, estudiamos el articulado jurídico donde reside la extraterritorialidad y los requisitos para lograr una decisión de adecuación. La segunda parte se centra en si este modelo es apto para economías en desarrollo, respondiendo a la creciente proliferación de legislaciones inspiradas en el RGPD.

I. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1. Enfoque europeo: la privacidad como derecho humano

El reciente brote de COVID-19 ha llevado la tensión de proteger los datos personales en un contexto internacional a un punto álgido. Para Europa, el enfoque integral de protección de datos se basa en gran medida en los derechos humanos. De hecho, el surgimiento del foco en la dignidad, que es el núcleo de la privacidad en Europa, es consecuencia de una reacción contra el fascismo y, especialmente, contra el nazismo[3].

Durante la Segunda Guerra Mundial, el régimen nazi utilizó datos personales muy sensibles del censo local para localizar y arrestar a los judíos, con consecuencias atroces. Más tarde, en la Alemania Oriental, el alcance de la policía secreta y la agencia de inteligencia (Stasi) se extendió a todos los aspectos de la vida civil[4]. No es sorprendente que, en este contexto, Europa haya otorgado una importancia descomunal a garantizar la privacidad de sus ciudadanos.

En la UE, la privacidad se considera un derecho fundamental que no puede sustraerse[5]. Sobre la base del Convenio Europeo de Derechos Humanos de 1950,

[3] CUNNINGHAM, M., "*Diminishing sovereignty: how European privacy law became international norm",* Santa Clara Journal of International Law, Volumen 11, Nº 2, 2013, pp. 428-430.

[4] JABLONKA, I., "*The Origins of Mass Surveillance Interview with Sophie Cœuré*", en http://www.booksandideas.net/The-Origins-of- Mass-Surveillance.html (Fecha de consulta: (06/03/2021).

[5] HUANG, J., "*Applicable law to transnational personal data: Trends and dynamics*", German Law Journal, Volumen 21, Nº 6, 2020, pp. 1287.

que reconoce el derecho a la privacidad, el Tratado de Lisboa de 2009 elevó la protección de datos como un derecho fundamental garantizado por las instituciones de la UE. Específicamente, el Tratado de Lisboa dio fuerza legal a la Carta de los Derechos Fundamentales de la UE. Se reconoce en el Convenio Europeo de Derechos Humanos como parte integrante del derecho a la intimidad, en su artículo 8 y en la Unión Europea con los artículos 7 y 8 de la Carta de Derechos Fundamentales.

Desde 1995 hasta el 25 de mayo de 2018, la Directiva de protección de datos (DPD) estuvo en vigor en Europa. La Directiva 95/46 / CE, tenía dos objetivos[6]: (1) proteger el derecho fundamental a la protección de datos y (2) garantizar el libre flujo de datos personales entre los Estados miembros armonizando sus legislaciones. El 25 de mayo de 2018, entró en vigor el RGPD. Esta legislación es la última etapa de un esfuerzo de cincuenta años de la UE para proteger los datos personales de los consumidores de la UE.

La Comisión Europea define el Reglamento como "una medida esencial" para fortalecer los derechos fundamentales de las personas en la era digital y facilitar con ello la actividad económica, al aclarar las normas aplicables a las empresas y los organismos públicos en el mercado único. Además, se pone fin a la fragmentación de las distintas legislaciones de los Estados miembros[7].

La nueva normativa comunitaria adopta la forma de Reglamento por su aplicabilidad directa. Esto supone un incremento de la seguridad jurídica. Además, está basada en una serie de objetivos: (1) ampliar la dimensión del mercado interior, (2) conseguir un ejercicio adecuado de aquellos derechos que, en este sentido,

---

[6] Supra nota 3, pp. 430-431.

[7] Puede verse más información en https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es (Fecha de consulta: 07/02/2021).

corresponden a los ciudadanos y (3) configurar un contexto global y homogéneo que abarque aquellos ámbitos de los que la Unión Europea es competente[8].

1.1. Teorías de difusión del RGPD: imposición del modelo europeo

Debido a su poder de mercado y el amplio alcance extraterritorial, el RGPD aparece como el estándar dorado de privacidad de datos, cuyas implicaciones son indiscutibles desde cualquier parte del mundo[9]. Hoy en día, tiene enormes efectos sobre cómo se gestionan los datos dentro y fuera de la UE y desempeña un papel importante en la configuración de la privacidad.

Múltiples disciplinas han examinado la cuestión de la difusión de principios y normas entre diferentes jurisdicciones. A pesar de haber distintas teorías sobre el derecho de la Unión Europea y su inmenso poder regulatorio, me centraré en la propagación mundial de su ley de protección de datos.

Entre los académicos que veremos en este capítulo, se encuentra el influyente trabajo de Paul M. Schwartz[10], Jack Goldsmith[11] y Tim Wu[12], o por

[8] CAZURRO BARAHONA, V., *"Antecedentes y fundamentos del Derecho a la protección de datos"*, 2020, pp. 125.

[9] ISLAM, T. & ERSHADUL KARIM, M., *"Extraterritorial Application of the Eu General Data Protection Regulation: an International Law Perspective*", IIUM Law Journal, Volumen 28, Nº 2, 2020, pp. 533-537.

[10] Paul M. Schwartz es profesor de derecho en la Universidad de California-Berkeley y director del Berkeley Center for Law & Technology. Es experto en derecho de la privacidad y se ha desempeñado como asesor de la Comisión Europea y otras organizaciones internacionales. Puede verse más en https://www.law.berkeley.edu/our-faculty/faculty-profiles/paul-schwartz/.

[11] Jack Goldsmith es un abogado estadounidense y profesor de derecho en la Universidad de Harvard. Sus trabajos sobre la gobernanza de internet han tenido mucha repercusión, en especial su colaboración con Tim Wu. Puede verse más en https://hls.harvard.edu/faculty/directory/10320/Goldsmith/.

[12] Tim Wu es un abogado estadounidense y profesor de derecho en la Universidad de Columbia. Fue nombrado en 2013 como uno de los 100 abogados más influyentes de Estados Unidos en "*The National Law Journal"*. Puede verse más en https://www.law.columbia.edu/faculty/timothy-wu.

supuesto, la aportación de Anu Bradford[13], creadora del término efecto Bruselas. Según ellos, el RGPD ha recibido una acogida sin precedentes debido, principalmente, a tres factores[14].

El primero es (1) su esquema legal comprensible, junto con (2) el efecto Bruselas y (3) un poder de mercado muy influyente. Además de los tres factores anteriores, la adecuación de las decisiones de la Comisión Europea (CE) también es un factor que contribuye de manera significativa al reconocimiento y aceptación global del RGPD[15], como muestra la flexibilidad del acuerdo logrado con Japón[16].

Goldsmith y Wu argumentan que las razones detrás de su impacto global se deben a que emplea una "ley de privacidad global unilateral que resulta de la combinación inusual del poder de mercado de Europa y su preocupación inusual por la privacidad de sus ciudadanos".[17] Las empresas internacionales que operan en la UE, no tienen la opción de "salir del mercado europeo por completo"[18], ya que eso supondría renunciar a gran parte de sus ingresos.

Finalmente, debido a que la UE se preocupa mucho por la privacidad y ha estado involucrada durante mucho tiempo en la legislación de las normas en esta área, sus regulaciones tienen alcance extraterritorial, siguiendo los datos personales de los residentes de la UE, aunque se transfieran fuera del territorio europeo.

---

[13] Anu Bradford es profesora de derecho en la Universidad de Columbia y creadora del término efecto Bruselas. También es autora de "El efecto Bruselas: cómo la Unión Europea gobierna el mundo". Puede verse más en https://www.law.columbia.edu/faculty/anu-bradford.

[14] Supra nota 9, pp. 537-540.

[15] Id 540-542.

[16] WANG, F.Y., *"Cooperative Data Privacy: The Japanese Model of Data Privacy and the Eu-Japan Gdpr Adequacy Agreement*", Harvard Journal of Law & Technology, Volumen 33, Nº 2, 2020, pp. 670-674.

[17] GOLDSMITH, J. & WU, T., "*Who Controls the Internet? Illusions of a Borderless World*", Nueva York: Oxford University Press, 2006, pp. 176.

[18] Id 175.

El efecto Bruselas es un término acuñado por Anu Bradford en 2012 y más elaborado por ella en 2015 y 2020. La noción de Bradford del efecto Bruselas se centra en que las reglas relativamente estrictas de la UE han dado forma al desarrollo de políticas en diversas áreas fuera de Europa. Es una variación del tema del efecto California[19] presentado por primera vez por David Vogel[20] en 1995.

La tesis de Vogel es que los modelos de los mercados grandes y estrictamente regulados en las naciones ricas, se difunde a otros países a través de las empresas que se acaban rindiendo a esos estándares. Esto conduce a un aumento general de los niveles de protección. A veces, las industrias orientadas a la exportación regulan sus negocios siguiendo el modelo de la UE y presionan a los responsables políticos de sus gobiernos para que promulguen leyes que se ajusten a las normas de la UE.

El objetivo de este activismo es obtener beneficios competitivos en su propio país frente a los rivales que no tienen relación comercial con esta[21]. Por ejemplo, después de que se adoptase el RGPD en la UE, gigantes tecnológicos como Google, Facebook, Microsoft[22] y Apple, instaron al gobierno federal de los EEUU a promulgar una legislación federal de privacidad de datos similar a la europea.

En cuanto a la elasticidad de los mercados de datos personales[23], Bradford encuentra que las empresas pueden tener dificultades para aislar los servicios para las operaciones de la UE. Una empresa siente un mayor incentivo para adoptar un estándar global siempre que su producción no sea divisible en diferentes

[19] BRADFORD, A.,*" The Brussels Effect: How the European Union Rules the World"*, Oxford University Press, Nueva York, 2020, pp. 3 y ss.

[20] David Vogel es profesor emérito de la Haas School of Business de la Universidad de California en Berkeley. Es el creador del efecto California que influyó en la teorización del efecto Bruselas. Puede verse más en https://haas.berkeley.edu/faculty/vogel-david/.

[21] Supra nota 9, pp. 538.

[22] CANNATACI, J., "*Report of the Special Rapporteur on the Right to Privacy*", en https://undocs.org/A/73/438 (Fecha de consulta: 28/04/2021).

[23] Supra nota 19, pp. 48.

mercados[24]. Al analizar los beneficios y desventajas, muchas empresas comprueban que no pueden seleccionar geográficamente a sus clientes de la UE e, incluso si pudieran, no desean crear servicios separados para ellos, ya que ese tipo de diferenciaciones supondría costes y seguramente malestar entre los clientes que recibieran menos derechos.

Según Bradford, el factor de no divisibilidad tiende a estar presente en el campo de la protección de datos, por ser difíciles, tecnológica o económicamente, de segmentar, por lo que los beneficios de acogernos a un estándar único siempre superarán a fragmentarlo[25]. El sector privado obtiene de esta forma un papel clave en el efecto Bruselas, creando casos como el de California (CCPA)[26], donde un país como EEUU empieza a tener dilemas en torno a la privacidad en su propio terreno.

Colin Bennett[27] examinó cinco hipótesis elementales para la convergencia: (1) similitud de amenazas tecnológicas percibidas; (2) el deseo de extraer lecciones de las políticas adoptadas anteriormente en otros países y replicarlas; (3) acuerdo entre una pequeña red internacional de expertos sobre la política de protección de datos adecuada; (4) esfuerzos de armonización de las organizaciones internacionales (en particular podemos destacar al CoE, dada su relevancia con el RGPD); y (5) la percepción que sienten ciertos Estados de obligatoriedad para adoptar ciertas políticas debido a las acciones de otros países[28].

Desde el estudio de Bennett, hemos sido testigos de una notable expansión en el número de países que adoptan leyes de protección de datos y, en especial, el

[24] Id 54.

[25] Id 58.

[26] Id 816.

[27] Colin Bennett es profesor en el departamento de Ciencias Políticas de la Universidad de Victoria. Su investigación se ha centrado en las implicaciones sociales de las nuevas tecnologías de la información y en el desarrollo e implementación de políticas de protección de la privacidad a nivel nacional e internacional.

[28] BYGRAVE, L. A., "*The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects",* Computer Law & Security Review, Volumen 40, 2021, pp. 3.

modelo europeo. En estos últimos años la tendencia es evidente y las leyes de protección de datos de estándar europeo se están convirtiendo en la norma en la mayor parte del mundo.[29]

Los requisitos de adecuación para los regímenes de protección de datos de países no europeos en virtud de los artículos 44 a 49 del RGPD, combinados con normas de aplicación extraterritorial de la UE en virtud del artículo 3 del RGPD, que veremos en los próximos apartados, han jugado un papel importante en este sentido, al requerir reformas profundas en las legislaciones internas[30]. Durante los últimos cuatro a cinco años, el régimen de sanciones reforzado del RGPD, en particular en virtud del artículo 83 RGPD, también lo ha hecho, dados los riesgos económicos de quebrantarla.

Como observa Schwart, este modelo tan estudiado, y con tanto recorrido, esquematiza unas pautas generales basadas en principios que, ofreciendo altos estándares de protección de datos, son relativamente simples y comprensibles[31], tanto para el sector público como para el privado. El interés se corresponde con la accesibilidad del modelo de la UE, anclado primero en una Directiva y luego en un Reglamento. En comparación con el enfoque estadounidense, exclusivamente sectorial[32], el enfoque simplificado de la UE ofrece un modelo muy atractivo para el resto de los países.

[29] GREENLEAF, G., *"Global Data Privacy Laws 2019: New Eras for International Standards"*, Privacy Laws & Business International, Volumen 157, Nº 19-20, 2019.

[30] SCHWARTZ, P. M., "*Global Data Privacy: The EU Way*", New York University Law Review, Volumen 93, Nº 4, 2019, pp. 783-786.

[31] Id 810.

[32] Id 811.

1.2. Concepto de transferencia internacional de datos

Ni la Directiva 95/46/CE ni el RGPD define qué se entiende por transferencia internacional de datos[33]. El concepto europeo debe entenderse desde la perspectiva del Convenio del Consejo de Europa 108[34], relativo a la protección de los individuos en el tratamiento automatizado de datos personales. La definición de transferencia internacional de datos podemos encontrarla en el Informe explicativo del artículo 14 del Convenio 108+ diciendo que "sucede cuando se divulgan datos personales o cuando estos se encuentran disponibles para un destinatario sujeto a la jurisdicción de otro Estado u organización internacional"[35].

La definición presentada por el texto deriva de una construcción doctrinal y jurisprudencial a raíz de la STJUE Lindqvist[36]. El objeto principal de la cuestión planteada al TJUE era determinar si la publicación de datos personales en una página web, almacenada por su proveedor de servicios de alojamiento domiciliado en la Unión y de la que se puede acceder desde cualquier lugar, debe ser considerada como una transferencia internacional[37]. Se determinó que no debe considerarse como tal, aunque sí se considera un tratamiento de datos[38].

El acto de haber publicado en una página web los datos personales, no implica una transmisión directa entre dos sujetos (facilitar o poner a disposición

---

[33] ABERASTURI GORRIÑO, U., "*Movimiento internacional de datos. Especial referencia a la transferencia internacional de datos sanitarios*", Revista de administración pública, Nº 186, 2011, pp. 333-340.

[34] Actualizado conforme al RGPD por el protocolo adicional 223 (Convenio 108+).

[35] CoE, "*TRADUCCIÓN N° 058/2019) - Informe Explicativo de Convenio*" en https://rm.coe.int/informe-explicativo-de-convenio/1680968479 (Fecha de Consulta: 13/03/2021).

[36] ORTEGA GIMÉNEZ, A., *"La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español",* Tesis doctoral: Universidad de Alicante, 2014, pp. 42 y 45.

[37] STJUE, de 6 de noviembre de 2003, asunto C 101-01, Lindqvist (ECLI:EU:C:2003:596), apartado 71, en http://curia.europa.eu/.

[38] DURAN CARDO, B., "*La figura del responsable en el derecho a la protección de datos*", 2015, pp. 97-98 y 538-539.

información en internet no implicaría una transferencia de datos)[39], sino que se han transmitido con ayuda de una infraestructura informática[40]. Esto quiere decir que uno de los elementos constituyentes de una transferencia internacional de datos es la existencia de dos sujetos en el proceso (un exportador de datos y un importador de estos).

Sin embargo, la prestación de servicios de computación en la nube sí que lo sería, pues es un caso donde hay tratamiento de datos que exigen el envío de información, en su caso a terceros países[41] ajenos a la UE. De esta forma, según la doctrina establecida, una transferencia internacional de datos deberá constar de los siguientes elementos[42]:

1) Deben ser datos de carácter personal concernientes a personas físicas identificadas o identificables, sin importar si la fuente es numérica, alfabética, gráfica, fotográfica, acústica o de otra clase.

2) Los datos de carácter personal que vayan a transmitirse engloban tanto a los tratados de forma automatizada (medios informatizados) como a los tratados de forma no automatizada (medios convencionales).

3) La transferencia internacional debe tener por objeto el tratamiento de datos de carácter personal por parte del destinatario, sin importar si lo realizan

---

[39] PIÑAR MAÑAS, J. L., "*El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas*", Cuadernos de Derecho Público, Nº 19-20, 2013, pp. 58-60. Y ORTEGA GIMÉNEZ, A., "*Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE "Lindqvist", de 6 de noviembre de 2013*", Revista de derecho de Extremadura, Nº 7, 2010, pp. 101-105.

[40] Id, apartado 60 y 61.

[41] ÁLVAREZ RIGAUDIAS, C., *"Condiciones para las transferencias internacionales de datos personales en servicios de cloud"*, MARTÍNEZ MARTÍNEZ, R. (Editor), Derecho y Cloud Computing, Aranzadi, Navarra, 2012, pp. 5-6.

[42] GONZALO DOMENECH, J. J., "*Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros*", Cuadernos de Derecho Transnacional, Nº 1, 2019, pp. 353-354.

mediante cesión (a otro responsable) o como prestación de un servicio (encargado de tratamiento).

4) Desde el Espacio Económico Europeo (EEE) se produce el traslado físico efectivo de los datos de carácter personal a cualquier otro Estado, región, u organización internacional.

5) El lugar de destino de la transferencia de carácter personal debe encontrarse en un territorio no perteneciente al EEE o ajeno a las partes no contratantes.

6) Existirá transferencia internacional de datos personales si: (1) constituye una cesión (o comunicación) de datos o, (2) cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable mediante un encargo de tratamiento.

En el marco del Reglamento, la transferencia de datos se trata en los artículos 44 a 50 RGPD del Capítulo V del RGPD[43]. En la Directiva 95/46/CE re regulaban únicamente en sus artículos 25 y 26. Este hecho es una referencia clara a la importancia que han adquirido las transferencias internacionales en un mundo globalizado y, en particular, en la legislación europea actual[44].

Con ellos podemos sintetizar y extraer que existen 2 tipos de transferencia de datos en el contexto europeo[45]: (1) las transferencias transfronterizas (4.23 RGPD) entre Estados miembros, que quedan automáticamente amparadas por el RGPD al cumplir las leyes nacionales con dicha ley y; (2) las transferencias a

[43] Artículos 44 al 50 RGPD.

[44] PIÑAR MAÑAS, J. L., "*Transferencias de datos personales a terceros países u organizaciones internacionales"*, ÁLVAREZ CARO, M. / RECIO GAYO, M. (Coordinador), Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Edición I, Reus, Madrid, 2016, pp. 428-429.

[45] ORTEGA GIMÉNEZ, A., "*Transferencias Internacionales de Datos de Carácter Personal Ilícitas*", Aranzadi, Navarra, 2017, pp. 55-59.

terceros Estados u organizaciones internacionales ajenas a la UE (transferencias internacionales de datos).

El ámbito clave del primer tema de este trabajo, consiste en exponer los requisitos que tendrían que afrontar los terceros Estados ajenos a la UE durante el proceso de adecuación, para poder comprobar si los países en desarrollo (con un Estado de derecho débil o recursos muy limitados) que regulen leyes similares, tienen posibilidades de acceder al mercado de la UE. A continuación, inicia el análisis de los niveles para ser considerado adecuado en el ámbito de la protección de datos para su transferencia internacional.

2. Nivel de adecuación: el obstáculo principal al mercado europeo

El término nivel adecuado fue incluido, por primera vez en la Unión Europea, en el párrafo primero del artículo 25 de la Directiva 95/46/CE, derogada el 24 de mayo de 2016 por la entrada en vigor del Reglamento General de Protección de Datos (RGPD). A pesar de esto, el Tribunal de Justicia de la Unión Europea (TJUE) tuvo oportunidad de pronunciarse al respecto en la sentencia de 6 de octubre de 2015[46], en la que anuló el Acuerdo de Puerto Seguro ("*Safe Harbor*") entre la Unión Europea y EEUU. En concreto, el TJUE indicó al respecto que:

> "debe entenderse la expresión "nivel de protección adecuado" en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta"[47].

Se realiza así un examen de ese tercer país para comprobar que su nivel de protección es "sustancialmente equivalente", aunque esto no significa que deba ser una copia idéntica. Así lo reflejan en dicha sentencia su apartado 74. No obstante, como indica Piñar Mañas, "Europa no puede consentir que el derecho fundamental

[46] Maximillian Schrems c. Data Protection Commissioner. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 6 de octubre de 2015. Asunto C-362/14. ECLI:EU:C:2015:650.

[47] Id, apartado 73.

a la protección de datos, hoy reconocido en la Carta de Derechos Fundamentales de la Unión Europea, quede desprotegido más allá de las fronteras"[48].

En el contexto europeo, el enfoque actual del RGPD difiere del Convenio 108+ del Consejo de Europa, puesto que exige una declaración de adecuación de la Comisión Europea para la transferencia de datos personales, aunque formen parte de dicho Convenio. De esta forma, aunque México haya accedido al Convenio 108, requeriría de una decisión de adecuación u otra garantía adecuada para que pudiese llevar a cabo una transferencia internacional de datos desde la Unión Europea.

Es importante aclarar que el Convenio 108+ impone la regla general del libre movimiento de datos entre las partes contratantes del Convenio, sin que se pueda darse ninguna prohibición a este movimiento, más que la existencia de un riesgo en el Estado contratante sobre el incumplimiento de las disposiciones del tratado. No obstante, también limita su aplicación en los Estados que tuviesen normas armonizadas sobre transferencias internacionales de datos personales (como el RGPD)[49].

En este sentido, aunque la decisión de adecuación de la Comisión Europea es el primero de los instrumentos que se menciona en el RGPD, no es el único mecanismo. Son tres las bases principales para la transferencia de datos mantenidas en el RGPD[50]: (1) decisiones de adecuación de la Comisión Europea; (2) salvaguardas adecuadas; y (3) excepciones para situaciones específicas. A modo de

[48] PIÑAR MAÑAS, J. L., *"El Tribunal de Justicia anula de nuevo las transferencias de datos entre la Unión Europea y Estados Unidos*", en https://www.eleconomista.es/opinion-legal/noticias/10702030/08/20/El-Tribunal-de-Justicia-anula-de-nuevo-las-transferencias-de-datos-entre-la-union-europea-y-estados-unidos.html (Fecha de consulta: 28/04/2020)

[49] Artículo 14.1 de la Convención 108+.

[50] KUNER, C., "*Reality and Illusion in EU Data Transfer Regulation Post Schrems*", German Law Journal, Volumen 18, Nº 4, 2017, pp. 904.

esquema, los instrumentos que no requieren de autorización por parte de una autoridad de protección de datos son los siguientes[51]:

• Una decisión de adecuación de la Comisión Europea (artículo 45 RGPD).

• Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos (artículo 46.2 a) RGPD).

• Normas corporativas vinculantes (artículo 46.2 b) RGPD).

• Cláusulas tipo de protección de datos (adoptadas por la Comisión Europea, como indica el artículo 46.2 c) RGPD)

• Cláusulas tipo de protección de datos (adoptadas por una autoridad de control y aprobadas por la Comisión Europea, como indica el artículo 46.2 d) RGPD).

• Código de conducta con arreglo al artículo 40 RGPD, junto con los compromisos vinculantes y exigibles del responsable o el encargado del tratamiento, en el tercer país, para aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados (artículo 46.2 d) RGPD).

• Mecanismo de certificación con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento, en el tercer país, para aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados (artículo 46.2 d) RGPD).

Así mismo, los instrumentos que requieren de una autorización expresa son los expuestos a continuación:

[51] RECIO GAYO, M., "*Nivel adecuado para transferencias internacionales de datos*", Derecho PUCP, Nº 83, 2019, pp. 207-240.

• Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional (artículo 46.3 a) RGPD).

• Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados (artículo 46.3 b) RGPD).

Finalmente, existen también excepciones para situaciones específicas, que pueden verse en su artículo 49 RGPD. Así mismo, el RGPD introduce como novedad las transferencias a terceros Estados que ofrezcan suficientes garantías y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas (esto no fue respetado en los acuerdos entre EEUU-UE)[52].

Asegurar las suficientes garantías en una transferencia internacional, no se limita a ofrecer garantías adecuadas únicamente a la transferencia realizada desde cualquier territorio del EEE a un tercer país u organización internacional, sino también sobre las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Como indica Díaz Díaz, si un responsable pretende transferir datos personales a un tercer Estado, región u organización internacional además se ser "segura" y acreditar que cumple con todos los elementos obligatorios, debe demostrar que, en caso de efectuar sucesivas transferencias internacionales de datos a otros proveedores, también estos adoptarán las garantías tecnológicas suficientes[53].

[52] Artículo 46.1 RGPD

[53] DÍAZ DÍAZ, E., "*El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*", Revista Aranzadi Doctrinal, Nº 6, 2016, pp. 13.

2.1. Prerrequisitos básicos

Siendo el objetivo principal obtener una decisión de adecuación, hay que atender a los elementos que se tienen en cuenta para determinar a un tercer Estado (u organización) como seguro para la transferencia. La Comisión Europea ha publicado en la "Comunicación al Parlamento Europeo y al Consejo sobre Intercambio y Protección de los datos personales en un mundo globalizado", una sucesión de criterios que valorará como punto de partida[54]:

1. El alcance de las relaciones comerciales (efectivas o posibles) de la UE con un determinado tercer país, incluida la existencia de un acuerdo de libre comercio o de negociaciones en curso.

2. La magnitud de los flujos de datos personales con origen en la UE, que reflejan lazos geográficos o culturales.

3. Si el tercer país es pionero en el ámbito de la protección de datos y la privacidad y puede servir de modelo para otros países de su región.

4. La relación política global con el tercer país en cuestión, en particular por lo que respecta al fomento de valores comunes y objetivos compartidos a escala internacional.

Parece indicar que se priorizarán los intereses comerciales, otorgando una decisión de adecuación para aumentar las relaciones con dichos sujetos. No obstante, no es el único peso determinante para lograr esta hazaña. En 2003, (aunque con multitud de críticas) la Comisión determinó que Argentina tenía protección de datos adecuada en una breve decisión de cuatro páginas[55].

[54] Comisión Europea, "*Memo/17/15, Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers*", en http://europa.eu/rapid/press-release_MEMO-17-15_en.htm (Fecha de consulta: 25/02/2021)

[55] 2003/490/CE: Decisión de la Comisión, de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

Este suceso fue la recompensa por adoptar una ley de protección de datos al estilo de la UE en un momento en que dicha legislación aún no se había extendido por América Latina y, por tanto, era pionero. En 2017, la Comisión reconoció su uso de este criterio general, al menos, con el fin de decidir si continuar con un diálogo sobre adecuación. La importancia que se la ha dado a este tercer apartado hace presagiar una ruta posible para que economías en desarrollo que ven con imposibilidad acoger el modelo de la UE, se lo replanteen.

2.2. Elementos específicos: el artículo 45

Una vez verificados los prerrequisitos para entablar el diálogo con los sujetos en cuestión, nos adentramos en la valoración conforme al artículo 45 RGPD[56]. Actualmente, el artículo 45.2 a) RGPD contiene los elementos que tendrá en consideración la Comisión Europea al evaluar la adecuación del nivel de protección:

> "el Estado de derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos"

Este artículo fue recordado por el Tribunal de Justicia en el caso Schrems II. Esa cuestión prejudicial la sitúa Ricard Martínez en la órbita de los artículos 7 y 8 de la Carta de Derechos Fundamentales de la UE[57]. Este derecho fundamental a la protección de datos en la Unión Europea exige que el tratamiento de los datos se

[56] DOWERS, A., "*The transnational reach of GDPR: a comprehensive framework that can regulate data privacy internationally, or is that unrealistic?",* UGA UFR Droit, 2019, pp. 18.

[57] MARTÍNEZ MARTÍNEZ, R., "*Schrems II. Una breve reflexión desde los derechos fundamentales*", en https://diariolaley.laleynext.es/ (Fecha de consulta: 28/04/2021)

lleve a cabo de modo leal, para fines concretos y sobre una base de legitimación, además de reconocer a toda persona los derechos de acceso y rectificación[58].

Del mismo modo, el acceso a la justicia debe ser efectiva, pues el artículo 47 de la Carta de los Derechos Fundamentales reconoce el derecho a la tutela judicial efectiva y a un juez imparcial. Esto será muy relevante, dado que en numerosas naciones la independencia suele estar en juicio constante, en particular, en países en desarrollo con escasa división de poderes.

El segundo de los elementos es la existencia y el funcionamiento efectivo de las autoridades independientes en el tercer país. Este aspecto es muy complejo y lleno de matices[59] y será muy complicado de asegurar en países con un Estado de derecho débil. Así, el artículo 45.2 b) RGPD indica que:

"la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros"

El tercer elemento radica en los compromisos internacionales y el cumplimiento de obligaciones derivadas de instrumentos vinculantes. También se valora positivamente, la participación en sistemas o foros multilaterales o regionales, en particular, en materia de protección de datos (en especial el Convenio 108+).

Es así como el artículo 45.2.c) del RGPD indica lo siguiente:

"los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de

[58] Supra nota 51, pp. 219.

[59] TRONCOSO REIGADA, A., "*Autoridades de control independientes*", ÁLVAREZ CARO, M. / RECIO GAYO, M. (Coordinador), Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Edición I, Reus, Madrid, 2016, pp. 428-429.

acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales"

Esto también se refleja en la orientación adoptada por el Comité Europeo de Protección de Datos que actualiza las directrices del Grupo de Trabajo del Artículo 29[60]. En particular, en el llamado "referencial de adecuación", una síntesis de los elementos fundamentales que deberían estar en toda legislación para que pueda considerarse como "equivalente" a efectos de la Comisión Europea[61].

El estándar de equivalencia no implica una réplica punto a punto de las normas de la UE, dado que los medios para garantizar un nivel comparable de protección pueden variar entre diferentes sistemas de privacidad, a menudo reflejando diferentes tradiciones legales, sin embargo, requiere un alto nivel de protección.

La Comisión Europea monitorizará la evolución de las nuevas decisiones sobre el carácter adecuado de la protección y tendrán que revisarse al menos cada cuatro años[62]. Las autorizaciones seguirán en vigor hasta que se modifiquen, sustituyan o deroguen. En definitiva, el Reglamento introduce un mecanismo de control de otras jurisdicciones para evitar que la evolución tecnológica haga inútiles las garantías legales y deje a los ciudadanos desprotegidos en sus derechos[63].

No obstante, el marco de revisión cada 4 años (45.4 RGPD) debería adaptarse según las necesidades de ese tercer Estado al que se refiera la Decisión de Adecuación. En el caso de países que requieran de reformas posteriores a esa

[60] El Grupo de Trabajo del Artículo 29 se integró, el 25 de mayo de 2018, en el Comité Europeo de Protección de Datos (CEPD).

[61] Article 29 Data Protection Working Party, "*Adequacy Referential (WP 254 rev.01)*", en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 (Fecha de consulta: 02/03/2021).

[62] Artículo 45.4 y 45.5 RGPD.

[63] Supra nota 53, pp. 10.

decisión de adecuación, se tendría que adelantar ese control para evaluar nuevamente la legislación[64].

3. Aplicación extraterritorial del Reglamento: el artículo 3

Desde la entrada en vigor del Reglamento General de Protección de Datos se introdujeron nuevas reglas para la aplicación extraterritorial de la normativa europea. De esta forma, organizaciones, empresas y países ubicados fuera de la Unión Europea quedaban sujetos a su aplicación y régimen sancionador.

Los redactores del RGPD buscaron redactar este artículo de una manera que maximizara la protección otorgada a los interesados dentro de la UE. Como resultado de este objetivo, el artículo 3 contiene una redacción que hace que el RGPD sea aplicable fuera de las fronteras de los Estados miembros[65].

Este capítulo examinará las disposiciones del artículo 3.1 RGPD, enfocado en el establecimiento de la entidad en la UE y el artículo 3.2 RGPD. Este último es donde aparecen las reglas de extraterritorialidad, estableciendo en sus supuestos múltiples posibilidades en las que los responsables del tratamiento de datos, ubicados fuera de la UE, podrían verse sometidos a las reglas de juego marcadas por Europa.

La tendencia en la Unión Europea mostraba una clara inclinación por la exigibilidad del cumplimiento de normas de protección de datos europeas a las entidades, indistintamente de su ubicación o nacionalidad, cuando llevasen a cabo actividades de índole empresarial con acceso a los datos personales de ciudadanos de la UE.

El RGPD consolida esa hoja de ruta que tenía como base interpretativa el contexto tecnológico de digitalización, cada vez más presente en múltiples sectores,

[64] Supra nota 42, pp. 360-361.

[65] Supra nota 56, pp. 6.

que facilitaba el acceso al mercado europeo a entidades extracomunitarias, sin necesidad alguna de tener recursos presentes físicamente en la UE.

3.1.Artículo 3.1 RGPD: el principio de establecimiento

Su ámbito primario de aplicación se encuentra estipulado en el apartado 3.1 RGPD, al establecer que será aplicable a aquellos tratamientos de datos personales que se realicen "en el contexto de las actividades de un establecimiento" del responsable o del encargado en la UE. No se exige la existencia de una entidad con una forma jurídica concreta de nacionalidad europea, es suficiente con la mera presencia de un establecimiento en la UE[66].

Las autoridades europeas han interpretado con flexibilidad y de manera extensiva el concepto establecimiento. Así podemos comprobarlo en el Reglamento, ya que el considerando 22 RGPD nos aclara:

> "Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un 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."

Dicha interpretación extensiva de establecimiento ha sido confirmada tanto por el TJUE (caso C- 230/14 en Weltimmo[67] vs. NAIH o caso C-131/12 en Google vs. Costeja[68]) así como por el Comité Europeo de Protección de Datos. Este último,

---

[66] Supra nota 56, pp. 6-10.

[67] JERKER SVANTESSON, D., "*The CJEU's Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, Yet So Very Important*", Maastricht Journal of European and Comparative Law, 2016, pp. 332-341. Para más información: STJUE de 1 de octubre de 2015, asunto C-230/14, Weltimmo, ECLI:EU:C:2015:639.

[68] Supra nota 38, pp. 533-548. Para más información: STJUE de 13 de mayo de 2014, asunto C-131/12, Google Spain y Google, ECLI:EU:C:2014:317.

en la Guía 3/2018 sobre la aplicación territorial del RGPD[69], que establece que es suficiente con que ejerzan una actividad real y efectiva mínima, para que sea de aplicación el RGPD (sobre todo en negocios online).

Debe cumplirse el requisito de la existencia de establecimiento, aunque sea con actividad limitada, para que se aplique el artículo 3.1 RGPD. Por último, también se aclara que el RGPD será exigible a todo tratamiento realizado por el establecimiento europeo, con independencia de que el tratamiento de los datos tenga lugar en la UE o no.

Aclarado este apartado sobre la aplicación primaria del RGPD, podemos adentrarnos en las reglas extraterritoriales, que son las que buscan de forma expresa su aplicabilidad a responsables o encargados no nacionales de Estados miembros. El RGPD abre ahora la posibilidad para que la norma europea sea vinculante para organizaciones extranjeras sin establecimiento presente en la UE y es, en parte, lo que ha provocado la oleada de reformas extranjeras.

3.2. Artículo 3.2 RGPD: extraterritorialidad

El artículo 3.2 RGPD determina que será de aplicación la norma de manera extraterritorial a tratamientos de datos personales de interesados que residan en la UE por parte de cualquier responsable no establecido en la UE, en los siguientes casos:

a) Cuando el tratamiento de los datos esté relacionado con la oferta de bienes o servicios a interesados en la UE, independientemente de si a estos se les requiere su pago.

b) Cuando el tratamiento de los datos esté relacionado con el control del comportamiento de los interesados, en la medida en que este tenga lugar en la UE.

[69] EDPB, "*Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)"*, en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf (Fecha de consulta: 04/03/2021).

Además de las principales, también hay una regla extraterritorial adicional prevista el apartado 3 del artículo 3 RGPD, en el que establece que será de aplicación para el tratamiento de datos personales realizados por un responsable no establecido en la UE, sino en un lugar donde el derecho de los Estados miembros se aplica en virtud del Derecho Internacional Público, como es el caso de una misión diplomática u oficina consular de un Estado miembro (art. 25 RGPD)[70].

El alcance del apartado 2, que es el elemento esencial de esa extraterritorialidad[71], lo encontramos definido con cierta ambigüedad, por lo que resultado acertado recurrir a los considerandos 23 y 24 para comprender mejor los alcances de aplicabilidad del 3.2 RGPD. Así, el considerando 23, destaca que la extraterritorialidad del RGPD tiene como finalidad garantizar que las personas físicas no sufran de privaciones indiscriminadas de sus derechos.

Además, nos presenta las claves para interpretar el concepto de oferta de bienes o servicios a los interesados. Para determinar si un responsable o encargado ofrece bienes o servicios a interesados que residen en la UE, debe estarse a un criterio de materialidad, es decir, si resulta evidente que el responsable o el encargado busca ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión, previéndose intencionalidad.

Debe entenderse excluida, por tanto, cualquier situación donde excepcionalmente esos bienes o servicios acaben siendo ofertados en la UE. Es decir, la voluntad es uno de los criterios indispensables a tener en cuenta para determinar la aplicabilidad de la norma[72].

---

[70] DE MIGUEL ASENSIO, P. A., *"Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea*", Revista Española de Derecho Internacional (REDI), Nº 1, 2017, pp. 7-8.

[71] Supra nota 56, pp. 10-16.

[72] LÓPEZ-LAPUENTE, L., "*La aplicación extraterritorial del Reglamento General de Protección de Datos"*, Actualidad Jurídica Uría Menéndez, 2019, pp. 138-140.

En este sentido, el considerando 23 aporta otro criterio interpretativo relevante para detectar esa voluntad, cuando señala que hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la UE, que pueden revelar que el responsable del tratamiento sí busca ofrecer bienes o servicios a interesados en la UE.

Desde la entrada en vigor del Reglamento, una de las dudas recurrentes la definición de los sujetos respecto de los que el tratamiento de sus datos personales activaría la aplicabilidad del RGPD. El debate principal residía en el estatus jurídico que debía tener asignado el residente en el territorio de la UE.

El RGPD no parece vincular la aplicación a ningún requisito de nacionalidad o residencia legal, por lo que se infiere que basta con la mera presencia del sujeto en cuestión para que la norma se vuelva obligatoria y le sean otorgados estos derechos[73]. Distinta interpretación encontramos en la Guía ya mencionada, para la aplicabilidad hacia ciudadanos nacionales de un Estado miembro pero residentes fuera de la UE, ya que en esa situación las organizaciones no europeas están exentas del deber de utilizar el Reglamento.

Avanzando hacia el supuesto redactado en el artículo 3.2 b) RGPD ("el control de su comportamiento, en la medida en que este tenga lugar en la Unión")[74]. El concepto definido es nuevamente indeterminado, por lo que debemos recurrir al considerando 24 para vislumbrar la interpretación adecuada. Así nos señala que debe referirse a interesados ubicados en la UE y el comportamiento monitorizado debe tener lugar y desarrollarse por dicho interesado también en el territorio de la UE.

[73] Id

[74] Supra nota 56, pp. 11.

Para determinar si se puede considerar que un tratamiento controla el comportamiento de los interesados, el considerando 24 señala que debe tenerse en consideración si las personas físicas son objeto de un seguimiento en Internet, "inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes".

Aquí debemos destacar la interpretación realizada en la Guía del CEPD, al no limitar la monitorización al ámbito de internet y ampliar su definición a otras tecnologías y redes. A pesar de venir expresamente referenciada en el considerando 24 como seguimiento de comportamiento a través de Internet, su uso debe interpretarse más allá[75].

Podemos contextualizarlo en aquellas situaciones en las que ese control, mediante el uso de archivos o programas informáticos que almacenan y permiten el acceso a información en el equipo de un usuario, como cookies, no tiene lugar en el marco del ofrecimiento al interesado de productos o servicios[76].

Es relevante tener en cuenta que el concepto de dato personal que aplican las autoridades europeas de protección de datos alcanza datos técnicos, como la dirección IP, por lo que no es obligatorio que se recopilen datos como nombre o dirección para que se considere que existe recogida y tratamiento de datos conforme al RGPD. A la luz del citado Considerando 24, también debe englobarse dentro de este precepto los tratamientos realizados por Big Data[77].

[75] Supra nota 72.

[76] Supra nota 70, pp. 16.

[77] COMISIÓN EUROPEA, "*Digital Single Market. Big data*". Big data (grandes datos o volúmenes de datos) es un término que se refiere a grandes cantidades de datos generados rápidamente y procedentes de diversas fuentes, pudiendo ser generados por personas o de manera automatizada. En https://ec.europa.eu/ (fecha de consulta: 27/04/2021)

Dado el elevado coste que suponen los controles del RGPD, deben analizarse con precaución los casos de cada empresa, para asegurarse de que les afecta. Aunque como vimos en las teorías de difusión, es posible que los estándares se normalicen entre sectores y obligue a empresas que no estarían sujetas a este artículo, a realizar profundas reformas organizativas.

La determinación de los casos en los que es de aplicación el RGPD a organizaciones no europeas requiere de un análisis del modelo de negocio y de la tecnología utilizada, que ya supone una inversión inicial elevada. Si nuestro país tiene una decisión de adecuación, bastará con estar sometidos a las leyes nacionales. De no ser así, deberemos demostrar que disponemos de las salvaguardas adecuadas.

Como podemos observar, el principio general de transferencias internacionales ha evolucionado con el nuevo RGPD. A diferencia de la Directiva 95/46/CE, las transferencias internacionales pueden realizarse, no solamente cuando garanticen un nivel adecuado de protección (actual artículo 45 RGPD), sino también cuando ofrezcan garantías adecuadas (artículo 46 RGPD).

4. Salvaguardias adecuadas

Según el artículo 46 RGPD, incluso si la entidad que transfiere no puede basarse en una decisión de adecuación, aún puede transferir datos a una entidad ubicada en el tercer país si se implementan las "salvaguardas adecuadas" para proteger los datos[78]. A continuación, mostramos las principales.

4.1. Cláusulas contractuales estándar

El primer grupo de estos instrumentos se refiere a las herramientas contractuales, que como mostramos antes esquematizadas, pueden ser cláusulas de protección de datos personalizadas, acordadas entre un exportador de datos de la UE y un importador de datos fuera de la UE, autorizado por la autoridad de

[78] Supra nota 56, pp. 18 y 30-32.

protección de datos competente (artículo 46.3 a) RGPD) o cláusulas modelo aprobadas previamente por la Comisión (artículo 46.2 c), d) RGPD).

Lo más importantes de estos instrumentos son las llamadas cláusulas contractuales estándar (SCC), es decir, cláusulas modelo de protección de datos que el exportador de datos y el importador de datos pueden incorporar en sus acuerdos contractuales voluntariamente. Su amplio uso indica que son muy útiles para empresas que no tienen los recursos para negociar contratos individuales con cada uno de sus socios comerciales.

A través de su estandarización, las SCC brindan a las empresas una herramienta para cumplir con los requisitos de protección de datos en un contexto de transferencia. Sin embargo, tras las sentencias Schrems I y II, los exportadores e importadores deberán observar si la legislación nacional de destino suprime las garantías de las SCC ya que, si existe riesgo de perjuicio en los datos trasladados, las autoridades de control europeas podrán prohibirlas[79].

4.2.Normas corporativas vinculantes

Otro instrumento importante son las denominadas reglas corporativas vinculantes (BCR). Se trata de políticas y acuerdos legalmente vinculantes que se aplican a los miembros de un grupo empresarial, incluidos sus empleados (artículos 46.2 b) y 47 RGPD). El uso de BCR permite que los datos personales se muevan libremente entre los diversos miembros del grupo.

Con las BCR se prescinde de la necesidad de tener acuerdos contractuales entre todas y cada una de las entidades corporativas, al tiempo que se garantiza que se cumpla un alto nivel de protección de los datos personales. Ofrecen una solución particularmente buena para grupos corporativos grandes y complejos y para una

[79] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ2010 L39, p.5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L344, pp.100).

estrecha cooperación de empresas que intercambian datos en múltiples jurisdicciones.

4.3.Privacy Shield: una alternativa a la adecuación

El 16 de julio de 2020, casi cinco años después de la anulación del Acuerdo de Puerto Seguro ("*Safe Harbor Agreement*") entre la Unión Europea y los Estados Unidos, la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) dictada en el asunto C-311/18 (caso Schrems II), ha invalidado también el Escudo de Privacidad *("Privacy Shield")*, adoptado para reemplazar al anterior.[80].

Aquellas transferencias que se hubiesen llevado a cabo con base al *"Privacy Shield"*, devienen ilegales de forma inmediata[81]. El CEPD así lo confirmó, en un documento clarificador con dudas frecuentas sobre la sentencia[82]. Esta decisión permitía que las entidades de EEUU que estuviesen adheridas al sistema del Escudo de Privacidad fueran consideradas como entidades que garantizan un nivel de protección adecuado en materia de protección de datos.

Cuando el TJUE anuló *"Safe Habor"* [83], la única alternativa para realizar transferencias internacionales era la utilización de las cláusulas contractuales tipo de la Comisión Europea. Esa situación produjo un terremoto jurídico que causó enormes problemas a todas las empresas que transferían datos a EEUU o que utilizaban prestadores de servicios ubicados en EEUU. La aprobación en

[80] TORRE DE SILVA, J., LUIS PIÑAR, J. & RECIO, M., "*Guía sobre transferencias internacionales de datos*", CEMS ESPAÑA, 2020.

[81] GARCÍA MICÓ, T. G. & GARCÍA-PERROTE, I., *"Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II*", Revista para el Análisis del Derecho, 3, 2020, pp. 551-559.

[82] Se puede acceder al documento a través del siguiente enlace: https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

[83] URÍA GAVILÁN, E., "*Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems*", Revista de Derecho Comunitario Europeo, Nº 53, 2016, pp. 267 y ss .

2016 del Escudo de Privacidad volvió a facilitar las transferencias internacionales de una forma sencilla y fluida.

La consecuencia de todo ello es que la gran mayoría de las transferencias internacionales que se producían todos los días entre Europa y EEUU se volvían ilegales[84], debiendo las empresas exportadora e importadora adoptar otras garantías adecuadas o modificar sus políticas de privacidad, si no querían arriesgarse a las sanciones por incumplimiento del RGPD, que pueden llegar hasta los 20 millones de euros o el 4% de su volumen de facturación anual.

José Luis Piñar Mañas, se pronunció recientemente sobre Schrems II, acogiendo el resultado con agrado[85]. Así declaraba que los derechos fundamentales, entre los que se encuentra la protección de datos, seguían siendo la base de la construcción europea. Además, afirmaba que estos eran imprescindibles para poder avanzar en la consolidación de la sociedad y de la economía.

Y es que como refleja la sentencia y recuerda Piñar Mañas, el Tribunal de Justicia, a raíz de la demanda de un particular, ha querido proteger los derechos fundamentales dejando constancia jurisprudencial de su posición prioritaria, por encima de las decisiones que pudiese acordar la Comisión Europea.

En este mismo sentido se ha pronunciado Ricard Martínez, al declarar que el TJUE se ha reafirmado en un criterio claro: la subordinación de los Estados miembros a las decisiones que les vinculan no implica un deber de

[84] PADÍN, A., *"El Tribunal de Justicia de la Unión Europea anula el Escudo de Privacidad*", en https://www.garrigues.com/es_ES/noticia/tribunal-justicia-union-europea-anula-escudo-privacidad-privacy-shield.

[85] Supra nota 48.

abstención de las autoridades de protección de datos en la tutela y garantía del derecho fundamental a la protección de datos[86].

Junto con esta declaración, este mismo autor recordó lo manifestado por el Tribunal de Justicia en su Sentencia de 13 de mayo de 2014, entre Google Spain y la Agencia Española de Protección de Datos (AEPD), en el que nuevamente el derecho fundamental a la protección de datos prevalecía sobre el interés económico de los responsables y encargados.

No obstante, el TJUE se pronuncia favorablemente sobre la validez de las cláusulas contractuales tipo aprobadas en virtud de la 2010/87/UE de la Comisión, de 5 de febrero de 2010[87]. A pesar de que concluye que a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales esta decisión es válida, se incluyen obligaciones para responsables (exportadores) y encargados del tratamiento (importadores).

El Tribunal de Justicia declara que mientras no exista una decisión de adecuación adoptada por la Comisión, las autoridades de control están obligadas[88] a suspender o a prohibir una transferencia de datos personales a un país tercero, cuando consideren a la luz de las circunstancias específicas de la transferencia, que las cláusulas tipo de protección de datos pueden no respetarse en ese país y que la protección exigida por el derecho de la Unión no puede garantizarse.

Al reconocer la conformidad de EEUU con el Escudo de privacidad, la UE creó una valiosa apertura para otras naciones. Es importante destacar que la ley de la Organización Mundial del Comercio (OMC) sobre el comercio de servicios exige

---

[86] MARTÍNEZ MARTÍNEZ, R., "*Schrems II. Una breve reflexión desde los derechos fundamentales*", en https://diariolaley.laleynext.es (Fecha de consulta: 28/04/2021)

[87] Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[88] Nota supra 81, pp. 6-8.

que la UE ofrezca a otros países la oportunidad de negociar acuerdos comparables[89]. Ha habido defensores que promulgaban un acuerdo similar para los países en desarrollo.

Defendían que podrían aprovechar esta oportunidad para negociar un acuerdo similar y fortalecer su reconocimiento[90]. Este tipo de acuerdo con la UE tendría grandes ventajas sobre las opciones existentes. En primer lugar, a diferencia de las BCR y las SCC, no se exigiría a las empresas que establecieran una presencia costosa en la UE ni un aumento tan significativo de la inversión.

Además, a diferencia del caso de obtener una decisión de adecuación, las empresas no estarían obligadas a adoptar estándares más estrictos o costosos para los datos involucrados en transacciones que tienen lugar exclusivamente en casa o con países que son menos exigentes que la UE[91]. En países en desarrollo, como el caso de las naciones africanas, es muy posible que sus vecinos tampoco ostenten regulaciones rigurosas, o tan estrictas como la europea.

Sin embargo, esta iniciativa parece altamente improbable dados los hechos acaecidos a lo largo de 2020, con la invalidación del "*Privacy Shield".* A continuación, analizaremos algunas de las debilidades comunes en los países en desarrollo, para evaluar si la tendencia a adoptar legislaciones inspiradas en el RGPD por parte de estas naciones es acertada o un grave error.

---

[89] GAY, C., "*The GDPR's Effect on Transatlantic Relations*", International Program Papers (Chicago Unbound), Nº 105, 2019, pp. 13 y ss.

[90] MATOO, A. & MELTZER, J., "*Resolving the conflict between privacy and digital trade*", Center for Economic and Policy Research, en https://voxeu.org/article/resolving-conflict-between-privacy-and-digital-trade (Fecha de consulta: 13/01/2021)

[91] Id

II. **ECONOMÍAS EN DESARROLLO Y EL EFECTO BRUSELAS**

1. Debilidades de economías en desarrollo

La pregunta principal de este trabajo, una vez mostrado el entramado jurídico del Reglamento, es si los estándares de protección de datos europeos deben servir como modelo para los países que no pertenecen a la UE, en particular los países en desarrollo, sin regímenes de privacidad establecidos o sólidos. Para responder a esta pregunta, debemos considerar las debilidades comunes entre los países en desarrollo.

Si buscan una determinación de adecuación, entonces deben promulgar una ley de privacidad nacional esencialmente equivalente a la de la UE. Sin embargo, una ley nacional impone el mismo estándar de protección de datos a todas las empresas del país, independientemente de que vendan exclusivamente en el país o también en el extranjero. Este estándar uniforme y estricto podría tener efectos adversos. Lo que puede ser apropiado en un país avanzado, con mercados bien desarrollados y acceso integral a los servicios, no es necesariamente apropiado en los países más limitados.

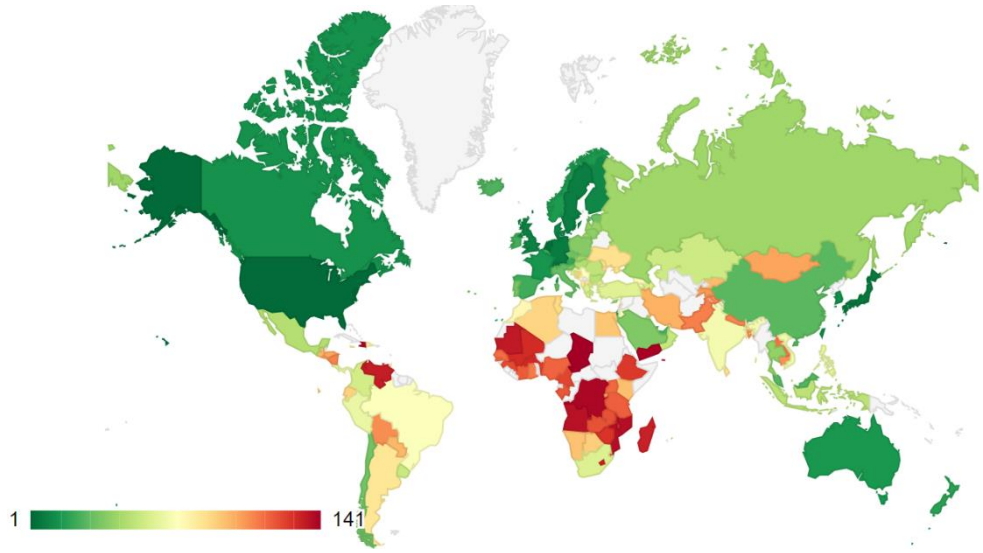
1.1.Inferioridad técnica

Aunque las capacidades tecnológicas de muchos países en desarrollo se han disparado en las últimas décadas, la inferioridad tecnológica aún puede ser un obstáculo para las empresas que buscan cumplir con el RGPD. La inferioridad técnica y las deficientes infraestructuras son un obstáculo importante para las empresas de procesamiento de datos en los países en desarrollo[92].

[92] CURTISS, T., *"Privacy Harmonization and The Developing World: The Impact of The EU's GDPR on Developing Economic*", Washington Journal of Law, Technology & Arts, Volumen 12, Nº 1, 2016, pp. 109-110.

Esto puede deberse a la falta de oportunidades de educación técnica local o a la migración de mano de obra cualificada, conocida como "fuga de cerebros"[93]. Bajo un modelo integral como el europeo, que abarca todas las organizaciones que recopilan información personal, incluidos los datos de los empleados, sería difícil para una nación en desarrollo sin organismos educativos equivalentes, asumir la carga. Así mismo, podemos observar en el siguiente mapa, una distribución de la competitividad global:

Índice de Competitividad



Fuente: Foro Económico Mundial 2019

Podemos observar el Informe de Competitividad Global del Foro Económico Mundial, donde la mayoría de países en desarrollo (normalmente los últimos puestos son de países africanos) son menos capaces de mantener su fuerza laboral educada. El ex presidente de Sudáfrica[94], Thabo Mbeki, etiquetó el problema de la fuga de cerebros en África como "aterrador" en 2016.

[93] DODANI, S. & LAPORTE R. E., *"Brain drain from developing countries: how can brain drain be converted into wisdom gain?"*, Journal of the Royal Society of Medicine, Nº 98, 2005, pp. 487-490.

[94] La ley de protección de datos de Sudáfrica (POPIA), también está inspirada en el RGPD.

De manera similar, la privacidad en el mundo digital actual requiere esencialmente conocimiento técnico[95], ya que son un ingrediente clave para la protección de datos. Para algunos países en desarrollo, esto puede ser un desafío. Cuando una población carece de acceso a agua potable o salud básica, la inversión en capacitación en ciberseguridad son prioridades menores, al menos, en la práctica.

En este sentido, el Reglamento recoge los requisitos para el nombramiento de miembros de la autoridad de control, indicando que cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes (art. 53.2 RGPD). Existen, por tanto, "unas cualificaciones y condiciones de idoneidad necesarias" para ser nombrado miembro de una autoridad de control (art. 54.1 b) RGPD).[96]

Como indica Antonio Troncoso, disponemos de un amplio margen de discrecionalidad y de apreciación a la hora de valorar si un candidato posee la cualificación y la idoneidad para ser nombrado. Esto limita el control jurisdiccional, pero debe ejercerse en los supuestos en los que de manera clara el candidato propuesto no posee la titulación y la experiencia necesarias en el ámbito de la protección de datos. Estos elementos están más reglados que la simple aptitud de un candidato que es siempre difícilmente valorable y equiparable[97].

Antonio Troncoso resalta dentro de los principios relativos al tratamiento, el de responsabilidad proactiva[98] (art. 5.2), por el que el responsable del tratamiento será garante del cumplimiento de lo dispuesto en el apartado 1. El Reglamento, en

---

[95] MANNION, C., "*Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets*", Vanderbilt Journal of Transnational Law, Volumen 53, Nº 2, 2020, pp. 704-705.

[96] Supra nota 59, pp. 447.

[97] La propuesta de la Comisión era aún más exigente en este punto al establecer que los miembros de las autoridades de control deben ser elegidos entre personas que ofrezcan "absolutas garantías de independencia y que posean experiencia y aptitudes acreditadas para el ejercicio de sus funciones, en particular, en el ámbito de la protección de datos personales" (art. 48.2).

[98] Supra nota 59, pp. 464.

el artículo 24.1, señala que "éste aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento".

Se dibuja un responsable que debe velar de manera proactiva porque el tratamiento de datos personales respete la legislación. El responsable del tratamiento debe aplicar medidas técnicas y organizativas apropiadas "teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas" (art. 24.1 RGPD).

El RGPD obliga al responsable a ser reflexivo, llevando a cabo una valoración de la naturaleza del tratamiento y de los riesgos para los derechos de las personas y que debe realizar una evaluación de los riesgos adoptando aquellas medidas adecuadas a cada asunto determinado, con un claro enfoque al riesgo, obligando incluso al responsable a valorar en términos de probabilidades[99].

Además, Troncoso señala que hay ahora un mayor dinamismo y fluidez en el análisis del cumplimiento de las medidas, al establecerse que "dichas medidas se revisarán y actualizarán cuando sea necesario". Por tanto, se trata de un responsable diligente, que no se limita a cumplir una norma porque la solución "no a venir definida en ésta". Es decir, desde Europa se reclama un profesional de la protección de datos con amplio conocimiento técnico y resolutivo.

Además, el Reglamento introduce nuevas obligaciones generales del responsable del tratamiento (art. 25 RGPD) como hacer la protección de datos desde el diseño y por defecto. De esta forma, la protección de datos en el diseño y por defecto no son principios genéricos sino obligaciones que debe cumplir el responsable y cuyo incumplimiento es gravemente sancionable[100].

Como resalta Troncoso, el RGPD introduce otra obligación al responsable para antes del tratamiento. Debe realizar una evaluación de impacto relativa a la

[99] Supra nota 59, pp. 465-466.

[100] Id

protección de datos "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas" (art. 35.1 RGPD).

Resulta evidente que países en desarrollo con limitados profesionales expertos en protección de datos, no lograrían cubrir la totalidad de un mercado nacional, siendo necesaria una inversión en educación para atender a estas necesidades, lo que llevaría tiempo y nuevamente, recursos. Es posible que al igual que los países que se promocionan a sí mismos como paraísos fiscales, los países en desarrollo que no se vean capaces de gestionar estas exigencias comentadas, ofrezcan una aplicación más indulgente de la normativa de protección de datos.

Sin embargo, un riesgo obvio al elegir un país en desarrollo como autoridad ejecutora puede ser una falta de estabilidad política y una abundancia de corrupción, además de las sanciones, si quebrantan las normas[101]. El RGPD puede ofrecer la oportunidad de posicionar a un país en desarrollo. Al lograr la adecuación o unos estándares aceptados internacionalmente, un país en desarrollo podría convertirse en una nación aprobada para transferencias internacionales de datos, siendo un puente comercial seguro para los negocios.

1.2. Limitación del crecimiento económico y la innovación

El cumplimiento de la normativa europea de protección de datos supone, lógicamente, un incremento significativo de costes. Así queda reflejado por Antonio Troncoso, al afirmar que la industria tiene una tendencia natural a reducir cargas económicas para ser más competitiva o para obtener más beneficios[102]. Cualquier país, pero en especial los que se encuentran en desarrollo, deben analizar el impacto económico de cualquier obligación nueva que se imponga a las

[101] Supra nota 92, pp. 111-112.

[102] TRONCOSO REIGADA, A., *"Hacia un nuevo marco jurídico europeo de la protección de datos personales*", 2012, pp. 179-180. Y Supra nota 59, pp. 463.

empresas, además de encontrar la proporcionalidad en las sanciones económicas, con el fin de no debilitar el tejido empresarial.

En este sentido, "también las empresas deben ser conscientes de que tienen que cumplir la normativa de protección de datos, como también cumplen la de prevención de riesgos laborales o la de medio ambiente, porque se trata de respetar un derecho fundamental"[103]. La tradición heredada de la directiva ya promovía el desarrollo de productos y servicios que tecnológicamente permitiesen la protección de datos de una forma integrada sin depender únicamente del responsable[104].

En este sentido, un informe reciente de la Comisión ha valorado positivamente la capacidad de adaptación del RGPD. El resultado de ese análisis concluye que el RGPD ha demostrado su flexibilidad para apoyar soluciones digitales en circunstancias imprevistas, como el COVID-19[105]. El informe también señala que las empresas están desarrollando una cultura del cumplimiento y recurren cada vez más a una sólida protección de datos como ventaja competitiva.

José Luis Piñar Mañas se mostró crítico con ciertos aspectos del RGPD[106]. Así, considera que el nuevo modelo (RGPD), no es más sencillo que el modelo anterior (Directiva). Considera que el RGPD exige a cada empresa adoptar decisiones propias en función de los tratamientos de datos y la naturaleza de estos, incorporando un alto riesgo de discrecionalidad, al conceder mayor margen de apreciación a los responsables del tratamiento. Un exhaustivo control que asume

[103] Id

[104] Nota supra 38, pp. 572-575.

[105] COMISIÓN EUROPEA, "*Informe de la Comisión: las normas de protección de datos de la UE empoderan a los ciudadanos y están adaptadas a la era digital*", en https://ec.europa.eu/commission/presscorner/detail/es/ip_20_1163 (Fecha de consulta 28/04/2021).

[106] PIÑAR MAÑAS, J. L., "*Introducción*", ÁLVAREZ CARO, M. / RECIO GAYO, M. (Coordinador), Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Edición I, Reus, Madrid, 2016, pp. 15.

alcanzable para las grandes compañías y Administraciones públicas, pero más complicado para pymes y pequeños organismos.

Antonio Troncoso hacía cierta defensa del modelo europeo cuando afirmó que es innecesario decir que la vía que le interesa a la industria para la protección de los datos personales es la autorregulación[107]. En este sentido, para hacer frente al coste asociado a este sistema, Troncoso defiende como imprescindible que las instituciones públicas eviten las posiciones frentistas en relación con las empresas y sean capaces de generar entornos de colaboración, lo que no significa ceder ante la industria, sino alcanzar un diálogo que permita una mayor protección de los datos personales.

De esta misma forma, continúa su análisis afirmando que es necesario tratar de poner este derecho fundamental en positivo[108], involucrando al propio sector. La privacidad se debe mostrar como una oportunidad de negocio, como una ventaja competitiva para las empresas. En este mismo sentido, se posicionan otros autores relevantes del ámbito de la protección de datos, como Ricard Martínez, que afirma que[109]:

"La privacidad y el desarrollo tecnológico pueden armonizarse. La protección de datos no puede ser un freno a la innovación. Con el compromiso de la industria, el desarrollo tecnológico y la protección de datos no serían sólo compatibles, sino que podrían retroalimentarse. Para ello es necesario potenciar una imagen del derecho fundamental a la protección de datos como una ventaja competitiva que permita, a quien cumpla, ofrecer a la sociedad seguridad y confianza".

Así mismo se pronunció recientemente Věra Jourová, vicepresidenta responsable de Valores y Transparencia de la UE, declarando que el régimen

---

[107] Supra nota 102, pp. 179.

[108] Id, pp. 48-49.

[109] MARTÍNEZ MARTÍNEZ, R., "*Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos*", pp. 160. Y MARTÍNEZ MARTÍNEZ, R., *"La protección de datos no puede ser un freno a la innovación*", en https://confilegal.com/20150611-ricard-martinez-proteccion-datos-freno-innovacion-11062015-2104/ (Fecha de Consulta: 28/04/2021).

europeo puede ser un ejemplo a seguir a través de la transición digital centrada en el ser humano y como un pilar para la construcción del resto de políticas, profundamente vinculadas con los derechos fundamentales[110]. Aparicio es otro de los autores en defensa de este sistema e insiste en que[111]:

> "es necesaria la asunción de una cultura de protección de datos, por cuya virtud empresas y ciudadanos tomen conciencia de su importancia. Los datos personales son más que simples accesorios de la personalidad de los individuos: son su propia proyección en diversos ámbitos, definiendo su persona, afectándoles a nivel moral y económico (tienen un auténtico valor patrimonial)"

No obstante, el cambio a regímenes integrales de privacidad de datos también puede motivar a algunas empresas a asumir riesgos indebidos[112]. Al sopesar los altos costes del cumplimiento con la posibilidad de ser descubiertos por incumplimiento, algunas empresas pueden arriesgarse y continuar con las prácticas comerciales existentes incumpliendo con el RGPD. No obstante, las multas pueden ser de hasta 20 millones de euros o el 4 por ciento de la facturación global anual[113], lo que supone para muchas empresas, la quiebra.

Dos economistas, Krasteva et al. (2015)[114] y Campbell et al. (2015)[115], muestran que la inversión de cumplimiento y regulación de datos, respectivamente, puede crear barreras de entrada y, por lo tanto, pueden dañar la innovación. En

---

[110] Supra nota 106.

[111] APARICIO VAQUERO, J. P., *"La protección de datos que viene: el nuevo Reglamento General europeo*", Ars Iuris Salmanticensis, pp. 33.

[112] Supra nota 92, pp. 115-117.

[113] SAFARI, B., *"Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection",* Seton Hall Law Review, Volumen 47, Nº 3, 2017, pp. 809-836.

[114] KRASTEVA, S., SHARMA P. & WAGMAN, L., "*The 80/20 rule: Corporate support for innovation by employees*", International Journal of Industrial Organization, Nº 38, 2015, pp. 5 y 10.

[115] CAMPBELL, J., GOLDFARB, A. & TUCKER, C., *"Privacy regulation and market structure*", Journal of Economics & Management Strategy, Volumen 24, Nº 1, 2015, pp. 47-73.

particular, un estudio de 2018[116], demostró que las leyes de localización de datos pueden obstaculizar el crecimiento económico en las economías en desarrollo.

Muchos países en desarrollo exportan servicios comerciales y de procesamiento de datos proporcionados digitalmente, que requieren flujos internacionales de datos. El fortalecimiento de la regulación dificulta la transferencia de datos y, por lo tanto, amenaza algunas de estas exportaciones[117].

Como hemos comentado, una ley nacional impone el mismo estándar a todas las empresas del país. Esto podría afectar negativamente a los países más pobres. Las leyes de privacidad prematuramente estrictas podrían dañar el desarrollo de los mercados al inhibir el flujo de información y podrían crear importantes asimetrías de información afectando a la eficiencia de los mercados[118].

En diversos estudios académicos, se ha analizado el impacto que el RGPD tenía sobre el ecosistema "s*tartup*", es decir, sobre las empresas emergentes con alto contenido tecnológico que requerían de baja inversión inicial. Campbell (2015) muestra que, aunque la regulación de la privacidad impone costes a todas las empresas, son las pequeñas y las nuevas empresas las que se ven más afectadas negativamente.[119]

Un estudio de ECIPE[120] sobre el impacto de regulaciones estrictas con requisitos de localización de datos, señaló que si economías como India, Brasil,

---

[116] MELTZER, J. P. & LOVELOCK, P., "*Regulating for a digital economy: Understanding the Importance of Cross-Border Data Flows in Asia*", Global Economy and Development at Brookings, 2018, pp. 19 y 20.

[117] BAUER, M, ERIXON, F., KROL, M., LEE-MAKIYAMA, H. & VERSCHELDE, B, "*The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce"*, European Center for International Political Economy, 2013.

[118] KITCHENMAN, W. F. "*U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns*", The Tower Group, 1999.

[119] JIA, J., ZHE JIN, G. & WAGMAN, L., *"The short-run effects of GDPR on technology venture investment",* National Bureau of Economic Research, 2018, pp. 6-10.

[120] BAUER, M., LEE-MAKIYAMA, H., VAN DER MAREL, E. & VERSCHELDE, B. *"The Costs of Data Localisation: Friendly Fire on Economic Recover*y", ECIPE Occasional Paper, Nº 3, 2014.

Indonesia, Corea del Sur o Vietnam, también imponen medidas similares, podrían experimentar pérdidas significativas del PIB. En India, por ejemplo, estimó una pérdida de hasta el 0,8 por ciento del PIB si el país adoptaba un requisito de localización. El estudio también estima una reducción de hasta el 1,4 por ciento de las inversiones nacionales en India debido a los requisitos de localización.

Además, otro estudio encontró que los costes de cumplimiento de la normativa europea en su momento tendrían un impacto negativo significativo en las pymes de la UE, ya que el cumplimiento requeriría que las empresas de la UE rediseñaran completamente sus sistemas y procedimientos para la protección de datos[121]. Para muchas pymes de países en desarrollo, la falta de una ley de protección de datos preexistente haría de este un esfuerzo descomunal.

Las autoridades de protección de datos han desarrollado una serie de actividades para ayudar a las pymes a cumplir con el RGPD, por ejemplo, mediante el suministro de plantillas para procesar contratos y registros para actividades de procesamiento, seminarios y líneas directas para consultas. Varias de estas iniciativas se beneficiaron de la financiación de la UE[122]. Este tipo de facilidades tal vez no estaría al alcance de economías en desarrollo con experiencia y recursos limitados.

Como ejemplo, vemos Kenia, conocida como "Silicon Savannah" y representando el epicentro del movimiento tecnológico de África[123]. Sin embargo, varios escándalos de privacidad relacionados con las elecciones llevaron al país a redactar una legislación de protección de datos, que ofrecería a los ciudadanos

---

[121] CHRISTENSEN, L., COLCIAGO, A., ETRO, F. & Rafert, G., *"The Impact of the Data Protection Regulation in the EU*", Intertic Policy Paper, 2013, pp. 42-43.

[122] La Comisión proporcionó apoyo financiero a través de tres oleadas de subvenciones, por un total de 5 millones EUR, y las dos más recientes se destinaron específicamente a apoyar a las autoridades nacionales de protección de datos en sus esfuerzos por llegar a las personas y las pequeñas y medianas empresas. Puede verse más en: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supportingimplementation-gdpr_en.

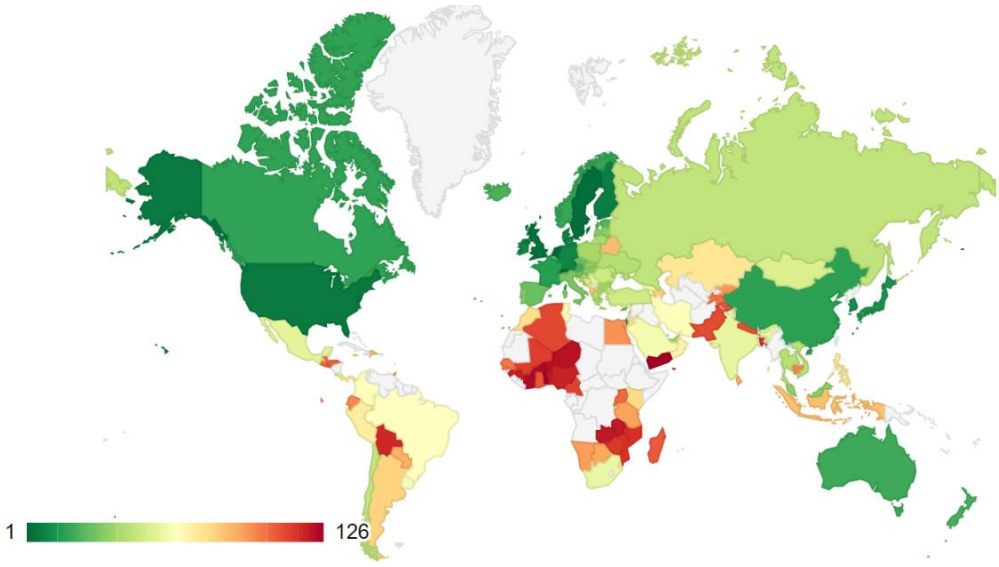
[123] BRIGHT, J & HRUBY, A., *"The Rise Of Silicon Savannah And Africa's Tech Movement",* TECH CRUNCH, en https://techcrunch.com/2015/07/23/therise-of-silicon-savannah-and-africas-tech-movement (Fecha de consulta: 21/01/2021).

protecciones sustanciales para sus datos[124]. La Ley de Protección de Datos de Kenia (DPA) entró en vigor el 25 de noviembre de 2019 y se basa en gran medida en el RGPD de la Unión Europea.

Como hemos presenciado en algunos estudios académicos previamente mencionados, esta ley con un cambio de criterio tan abrupto puede resultar demasiado restrictivo. De esta forma, mientras que las empresas más grandes y las multinacionales ya asentadas en el país, podrán asumir los requisitos de cumplimiento, las empresas más pequeñas se verán sometidas a unos costes elevados y probablemente inasumibles, lo que conllevará su cierre.

El Índice Mundial de Innovación muestra las limitaciones de países en desarrollo, donde deberían vigiar las reformas que puedan socavar aún más al movimiento emprendedor:

Índice de innovación



Fuente: Foro Económico Mundial 2018

[124] NISELOW, T., *"Five massive data breaches affecting South Africans*", Mail & Guardian, en https://mg.co.za/article/2018-06-19-five-massivedata-breaches-affecting-south-africans (Fecha de consulta: 03/03/2021).

Este hecho en entornos subdesarrollados, donde prolifera el comercio local, puede suponer la destrucción de los avances realizados por los emprendedores y pequeños empresarios. En general, supondría una limitación de la capacidad de aprovechar los beneficios económicos del flujo de datos transfronterizos[125].

La crítica de Piñar no ha sido desacertada pues las autoridades europeas reconocen las dificultades que afrontan las pequeñas y medianas empresas, en las que si detecta mayor dificultad de adaptación. Didier Reynders, comisario de Justicia de la UE, declaró que el RGPD cumplió con éxito sus objetivos y era referencia en todo el mundo, pero había áreas en las que tenía que mejorar. Una de estas era que la aplicación de las normas en toda la Unión debe ser más uniforme, sobre todo para las pymes[126].

Si bien una potencia económica como la UE es capaz de afrontar programas de financiación y apoyo a los sectores que se ven más afectados por las políticas regulatorias de protección de datos, los países en desarrollo difícilmente podrían implementar una normativa estricta sin que eso conllevase la destrucción de su mercado interior. Encontrar el equilibrio y plasmarlo en un instrumento "robusto, vinculante y adaptable" facilita el poder maximizar los beneficios que ofrece la innovación, impulsando la confianza y la competitividad[127].

El debate entre innovación y protección de datos personales tiene un recorrido de ya varias décadas[128]. Como han resaltado los autores anteriormente señalados, la importancia de ver nuestros datos como una parte de nuestra intimidad es esencial para no dañar al tejido empresarial, pues solamente una visión de estos

[125] FRIZELL, S., "*How Kenya's New Data Privacy Bill Could Hurt Its Economy*", Council on Foreign Relations, en https://www.cfr.org/blog/howkenyas-new-data-privacy-bill-could-hurt-its-economy (Fecha de consulta: 23/01/2021).

[126] Supra nota 107.

[127] Supra nota 104, pp. 18, 87 y 174.

[128] En su artículo "*The right to Privacy*", ya trataban la cuestión de la necesidad de proteger a la persona frente a intromisiones indebidas o mal uso de los datos personales en el caso de nuevas invenciones (innovación) o de modelos de negocio.

derechos como fundamentales puede lograr integrarlos con forma de ventaja competitiva y no como imposición autoritaria o desmesurada.

La innovación necesita estar en equilibrio con la protección de datos personales, pero difícilmente va a poder darse si la ley no la entiende por haberse adoptado de manera apresurada, o estar obsoleta porque se intentan aplicar esquemas que nada tienen que ver con la realidad y las necesidades del mercado y de la sociedad[129]. Es muy posible que los países en desarrollo se encuentren dentro de esta definición.

1.3. Estado de derecho subdesarrollado

Como se discutió anteriormente, las economías en desarrollo tienen algunos atributos deseables para las empresas, sin embargo, a menudo también se caracterizan por regímenes subdesarrollados, que abarcan desde corrupciones políticas hasta sistemas judiciales muy deficientes que no aseguran imparcialidad ni eficacia para hacer cumplir las leyes.[130]

Países que no reconocen la importancia de la independencia judicial, solo perjudicarán a las empresas de procesamiento de datos que existen dentro de sus fronteras y se esfuerzan por cumplir con el RGPD a través de salvaguardas. Además, al tener un sistema legal que no proporciona vías de reparación para los ciudadanos extranjeros, los esfuerzos para armonizar con la UE seguirán siendo incompletos.

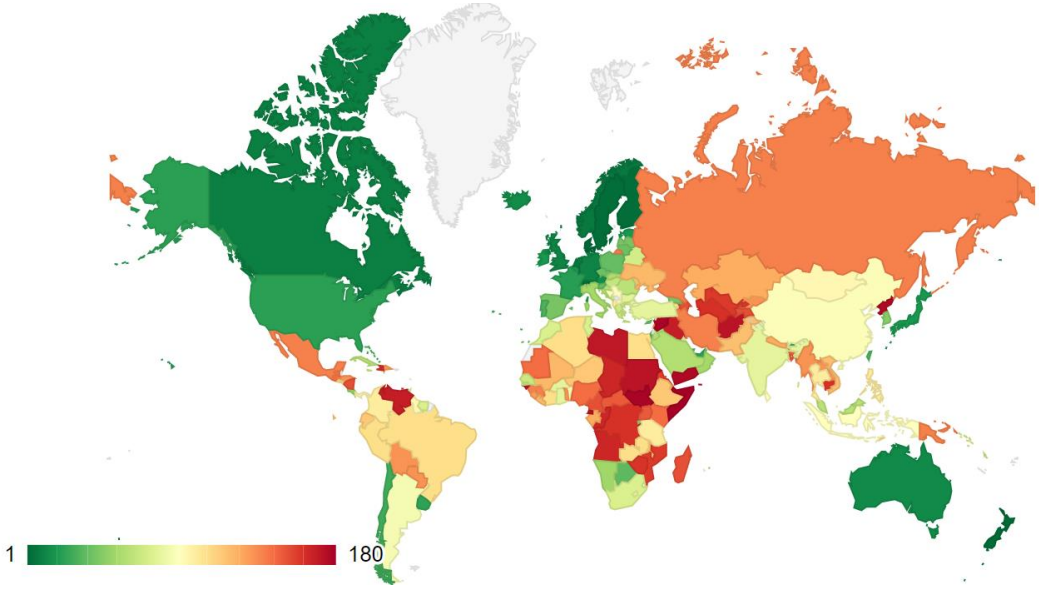
Por lo tanto, muchos países en desarrollo no podrían beneficiarse desde su adopción, obteniendo solamente gastos. De hecho, el Informe del Foro Económico Mundial, indica que la independencia judicial (a raíz de las imposiciones sobre el control poblacional) es una de las áreas donde más se ha retrocedido a raíz del COVID-19. Esto es preocupante teniendo en cuenta que los datos en años previos

[129] Supra nota 104, pp. 45.

[130] Supra nota 92, pp. 112-114.

ya denotaban una alta corrupción y falta de transparencia en el mundo en desarrollo, especialmente los gobiernos africanos:

Índice de corrupción



Fuente: Foro Económico Mundial 2018

En este sentido, la reparación judicial de los interesados, por ejemplo, fue la razón principal detrás de la invalidación de los acuerdos entre los Estados Unidos y la UE, junto con las preocupaciones en torno a la vigilancia gubernamental[131]. Si un país avanzado y potencia comercial no pasó ese filtro, es muy difícil augurar un buen resultado en el examen que desarrolle la Comisión hacia países en desarrollo.

A la hora de evaluar la adecuación del nivel de protección de un tercer país para lograr una decisión de adecuación, el RGPD resalta que la Comisión tendrá en cuenta la existencia de una o varias autoridades de control independiente[132] con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos (incluidos poderes de ejecución adecuados), de

[131] LOMAS, N., *"Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement With U.S."*, TechCrunch, en https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s (Fecha de consulta: 23/01/2021).

[132] Supra nota 59, pp. 487-488.

asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros (art. 45.2.b).

Como vimos en el apartado de las debilidades técnicas, detrás de cada artículo hay muchas exigencias complementarias. De esta forma, una asistencia y asesoramiento no pueden darse sin unas titulaciones y conocimientos que son requeridos por los responsables. Se deduce que, para lograr una adecuación, si bien no es necesario replicar los mismos procedimiento ni características, se tendrá en valor si supone un entendimiento equivalente de lo que significan conceptos como independencia o transparencia.

Antonio Troncoso hace un análisis profundo del refuerzo de independencia demandada en el RGPD para las autoridades de control, en el que dedican a esta cuestión la Sección 1ª del Capítulo VI (art. 51-54 RGPD). Se concreta en qué consiste esta independencia, señalando tanto las garantías sustanciales de independencia como las garantías formales[133]. De su análisis podemos deducir la complejidad y la importancia que otorgan a ese propio concepto de independencia.

El Reglamento, recogiendo la jurisprudencia del TJUE, es más explícito que la Directiva y establece que los miembros de cada autoridad de control deben ser ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes, a toda influencia externa (directa o indirecta), y no solicitarán ni admitirán ninguna instrucción (art. 52 RGPD)[134]. Gobiernos de un país sin división de poderes, deberán asegurar con reformas de su sistema que este hecho será realizable en la práctica.

En este sentido, la independencia funcional de las autoridades de control (que no estén sujetas a instrucción alguna en sus funciones), como señala el TJUE, "es un requisito necesario para que dichas autoridades puedan ajustarse al criterio de la independencia". El TJUE ha señalado que la mera posibilidad de que las

[133] Id, pp.472 y ss.

[134] Id, pp. 475.

autoridades del Estado puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de sus funciones[135].

Antonio Troncoso destaca, dentro de las garantías formales de independencia, la regulación que el Reglamento hace de la forma y requisitos de nombramiento de los miembros de la autoridad de control en el art. 53.1 RGPD, donde se señala que los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente[136].

Aunque deja libertad a los gobiernos en la forma de elección, como deduce Troncoso, un nombramiento por un organismo independiente o por una mayoría cualificada del Parlamento puede favorecer más su independencia que el nombramiento por parte del Gobierno. Recordemos nuevamente que, sin establecer un mecanismo concreto de elección, deberán cumplir con esas obligaciones de fondo en cuanto a titulación, entre otras[137] (tiempo de mandato, incompatibilidad con otros cargos…) para ser considerado apto para el cargo.

El Reglamento establece unas garantías formales de independencia relativas al funcionamiento de la propia autoridad de control como son la disponibilidad de recursos humanos y económicos para el cumplimiento de sus funciones y su autonomía de personal, presupuestaria y financiera[138]. Troncoso define como un elemento necesario, tanto para la independencia de las autoridades de control como para el correcto cumplimiento de sus funciones, el que estas cuenten con los medios humanos, técnicos, financieros y organizativos para poder ejercer sus poderes.

Como hemos establecido en apartados anteriores, los recursos en países en desarrollo son limitados y una legislación inspirada en el RGPD puede no ser

[135] Id, pp. 475-476.

[136] Id, pp. 476-477.

[137] Id, pp. 479-481.

[138] Id, pp. 481 y ss.

aplicable en la práctica, pues la falta de herramientas y autonomía presupuestaria, acompañada por un historial de escasa separación de poderes, hacen complicada la transparencia e independencia.

Siguiendo este criterio, varios países en desarrollo recibieron bajas calificaciones en el Índice de Estado de derecho del Banco Mundial, un conjunto de datos que evalúa cuánta confianza tienen los agentes en el sistema judicial de cada país, el grado en que se hacen cumplir los derechos contractuales y de propiedad en cada país, y la probabilidad que se sigan las reglas de la sociedad en cada país.

Por ejemplo, la República Centroafricana tiene una puntuación general negativa de -1,73 y Somalia con -2.35, se sitúa al final de la lista[139]. Por lo tanto, los países con estructuras judiciales cuestionables enfrentan una batalla cuesta arriba para intentar demostrar que su legislación sobre privacidad de datos es equivalente.

Muchos países sufren de sistemas judiciales con retrasos muy elevados o carecen de agencias independientes para implementar y hacer cumplir con la protección de datos. Por ejemplo, aunque Mauricio estableció una Autoridad de Protección de Datos, ésta dependía institucionalmente de la Oficina del Primer Ministro[140]. Además, en 2020 fue incluido en la lista negra de la Unión Europea por sus legislaciones laxas contra el blanqueo de capitales (aunque meses más tarde actualizó su legislación para adaptarse a las exigencias[141]).

---

[139] Rule of Law Index, WORLD BANK, en https://tcdata360.worldbank.org/indicators/hf5cdd4dc?indicator=370&viz=choropleth&years=2017&compareBy=region / (Fecha de consulta: 25/01/2021).

[140] Supra nota 95, pp. 702-704.

[141] BEEHAREE, Y., "*Mauritius updates to the Anti-Money Laundering and Combatting the Financing of Terrorism handbook",* en https://www.sannegroup.com/our-thinking/insights/2021/mauritius-updates-to-the-anti-money-laundering-and-combatting-the-financing-of-terrorism-handbook/.

El caso de Somalia también es muy relevante. En la conferencia online "Reformas económicas de Estados frágiles: perspectivas desde Somalia" tuvimos ocasión de trasladarle nuestras preguntas acerca de las problemáticas que afrontaba su país, al Ministro de Finanzas Dr. Abdirahman Dualeh Beileh. En su respuesta, nombró la posibilidad de utilizar tecnologías, como la creación de identidades digitales, para mejorar el acceso a los servicios financieros[142]. Este hecho es preocupante, dada la nula legislación respecto a la protección de datos y, como hemos comentado anteriormente, su baja calificación del Estado de derecho.

En algunos casos, como India y Kenia, la decisión del gobierno de crear un sistema de identificación nacional ha provocado preocupaciones sobre la privacidad[143] que llevaron a casos judiciales o debates políticos que impulsaron a los legisladores a crear una ley nacional de protección de datos[144]. En Kenia, aunque el artículo 51 de su Ley de Protección de Datos crea exoneraciones para los organismos públicos en asuntos que son difíciles para la seguridad nacional, el comisionado de datos debería establecer unos principios rectores claros para los organismos públicos, ya que la privacidad es fácilmente quebrantable.

Los datos personales también se utilizaron para afectar las elecciones en Kenia y Nigeria. Además, Kenia debe implementar su ley de protección de datos antes de las elecciones presidenciales de 2022[145]. En muchos países en desarrollo, el encargado de proteger los datos estaría a cargo de evitar que los partidos políticos

[142] OLOFSGÅRD, A. & STRÖMBERG, S., "*The Role of Partnerships in Economic Reforms of Fragile States : Perspectives from Somalia | Summary*", Free Network, 2020, en https://freepolicybriefs.org/2020/11/30/economic-reforms-somalia/.

[143] GILL, M., *"Explained: In Kenya's digital ID system, echoes of India's Aadhaar*", en https://indianexpress.com/article/explained/in-kenyas-digital-id-system-echoes-of-indias-aadhaar-6244643/.

[144] Supra nota 95, pp. 698-700.

[145] WANGARI, N., "*Kenya must implement data protection law before 2022 presidential election*", en https://globalvoices.org/2021/01/16/kenya-must-implement-data-protection-law-before-2022-presidential-election/ (Fecha de consulta: 07/01/2021).

usen los datos para manipular al electorado o, peor aún, que incite a la tensión y la violencia étnica. También velaría por impedir el uso discriminatorio de estas leyes.

En 2017, por ejemplo, Hungría aprobó una ley sobre la transparencia de las organizaciones no gubernamentales (Ley de Financiamiento Extranjero), que reciben apoyo del extranjero y restringió su financiamiento[146]. El 18 de junio de 2020, el Tribunal de Justicia de la Unión Europea (TJUE) dictaminó que la ley violaba la legislación de la Unión Europea al "introducir restricciones discriminatorias e injustificadas", violando la libre circulación de capitales y otros derechos garantizados[147].

Lamentablemente, este tipo de legislaciones han proliferado en múltiples continentes de todo el mundo, donde tal vez no existan tribunales como el TJUE para hacerle frente. Así, encontramos ejemplos en países en desarrollo como Kenia en 2013, donde la legislatura rechazó una ley que habría impuesto un límite a la financiación extranjera. Sin embargo, en 2014, el presidente Uhuru Kenyatta declaró que no permitiría que "organizaciones que promueven intereses extranjeros desestabilicen al gobierno"[148].

Etiopía, Nigeria, Malawai, Zimbabwe y Congo han tenido proyectos similares. Otros como Egipto, Túnez, Ruanda o Tanzania, tienen medidas similares o buscan introducirlas. Esto lleva a pensar que es posible que el riesgo de abusar de una ley de protección de datos sea elevado[149]. Sin tribunales que aseguren el respeto

[146] FRANZ, V., HAYES, B. & HANNAH, L., "*Civil Society Organizations and General Data Protection Regulation Compliance: Challenges, Opportunities, and Best Practices*", 2020, pp. 24-25.

[147] Id

[148] Pueden verse las declaraciones del presidente Uhuru Kenyatta en el siguiente enlace: https://www.youtube.com/watch?v=TWfTsMz7LVU.

[149] MUSILA, G., "*The Spread of Anti-NGO Measures in Africa: Freedoms Under Threat*", en https://freedomhouse.org/report/special-report/2019/spread-anti-ngo-measures-africa-freedoms-under-threat

a la normativa de protección de datos, pueden convertirse en herramientas de control.

También resulta muy interesante el caso de India, que recientemente ha desarrollado su legislación de protección de datos tomando al RGPD como referencia. Aquí, la Ley de Regulación de Contribuciones Extranjeras de la India de 2010 fue declarada inconstitucional por la Corte Suprema de la India el pasado 2020[150]. Dados estos movimientos, los países en desarrollo que aspiren a una decisión de adecuación lo deberían tener muy complicado.

En la contestación que UNCTAD nos ofreció, a la pregunta de si los países en desarrollo que habían iniciado un proceso de alineación con el RGPD tenían posibilidades reales, relató que los países en desarrollo están implementando leyes de protección de datos al estilo del RGPD, ya que lo ven como el enfoque regulatorio más reciente y desarrollado. Sin embargo, necesitan establecer autoridades de supervisión independientes, lo que constituye un desafío sustancial para gran multitud de estas naciones (y citaron a los países africanos como ejemplo).

Además, predicen que, si bien las leyes a menudo están alineadas con el RGPD de la UE, es probable que sea insuficiente para cumplir con el estándar de adecuación requerido por la UE, por lo que continuará confiando en otros mecanismos de transferencia de datos, como las cláusulas contractuales estándar. Estos elementos, si bien siguen siendo válidos tras Schrems II, tienen debilidades.

Si la legislación nacional de un país no pasa la prueba de idoneidad de la UE, las empresas deben utilizar Reglas corporativas vinculantes (BCR), diseñadas para que las empresas multinacionales muevan datos a nivel mundial, o Cláusulas contractuales estándar (SCC) para cada una de ellas. Ambas rutas son costosas y requieren de mucho tiempo y esfuerzo (económico, social…).

[150] RAUTRAY, S., "*NGOs can't be denied foreign funds, rules Supreme Court*", en https://economictimes.indiatimes.com/news/politics-and-nation/ngos-cant-be-denied-foreign-funds-rules-sc/articleshow/74519274.cms?from=mdr.

1.4. Falta de armonización normativa: fragmentación regional

El RGPD tenía como uno de sus objetivos primordiales armonizar las legislaciones de los Estados miembros. Si el enfoque de los países en desarrollo se centra en perspectivas ajenas, olvidando su desarrollo regional, podría provocar un caos normativo, que fue precisamente lo que Europa quiso corregir.

La mayoría de países en desarrollo carecen de un enfoque normativo unificado para la protección de datos personales. Más de la mitad de los cincuenta y cuatro países de África[151], por ejemplo, carecen de leyes de privacidad o protección de datos a pesar de haber experimentado el mayor crecimiento en el uso de internet de la década.

Se han realizado esfuerzos para adoptar una legislación integral de protección de datos en algunas regiones en desarrollo[152]. Por ejemplo, la Unión Africana (UA) aprobó en 2014 el Convenio sobre seguridad cibernética y protección de datos personales, que tenía como objetivo establecer marcos regulatorios en los niveles nacional y regional. Sin embargo, a diferencia de la aplicabilidad automática del RGPD, la convención de la UA carece de fuerza legal hasta que los países africanos adopten las disposiciones en su legislación nacional.

1.4.1. Infravaloración de iniciativas regionales

La República de Mauricio se encuentra entre los primeros países de África en promulgar una legislación integral de protección de datos. Mauricio se ha inspirado en el régimen de protección de datos de la UE, así como en el Convenio 108 del Consejo de Europa y su Protocolo adicional (que lo actualiza). Mauricio

[151] GREENLEAF, G. & COTTIER, B., *"Comparing African Data Privacy Laws: International, African and Regional Commitments"*, University of New South Wales Law Research Series, 2020, pp. 8.

[152] Id, pp. 13 y ss.

adoptó una ley de privacidad de datos para atraer inversión extranjera de la Unión Europea y por temor a la pérdida de relaciones comerciales con ella[153].

Mauricio es parte de las Naciones Unidas (ONU), la Unión Africana (UA) y la Comunidad de Desarrollo de África Meridional (SADC). En consecuencia, los tratados de derechos humanos y las políticas de privacidad de datos a nivel de la ONU, la UA y la SADC son relevantes para el sistema de protección de datos de Mauricio o, al menos, deberían serlo[154].

El instrumento de derechos humanos más importante de las Naciones Unidas que aborda la privacidad es el Pacto Internacional de Derechos Civiles y Políticos de 1966. En África, hay dos instrumentos principales que son relevantes para la protección de la privacidad: la Carta Africana de Derechos Humanos y de los Pueblos (Carta Africana) de 1981 y la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales de 2014 (Convención de Malabo)[155].

Ninguna de las anteriores bases regionales ha aparecido citada a lo largo del desarrollo legislativo de la normativa de protección de datos en Mauricio. De hecho, Mauricio ratificó el Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales el 6 de marzo de 2018, mucho después de que aprobara su nueva Ley de Protección de Datos el 8 de diciembre de 2017[156].

Este patrón es idéntico en las múltiples legislaciones que se han ido desarrollando en África. Así, en noviembre de 2019, Kenia promulgó la Ley de

---

[153] MAKULILO, A. B., "*The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius"*, International Journal of Human Rights, Volumen 24, Nº 1, 2020, pp. 117-146. (Alex B. Makulilo es profesor de derecho y tecnología en la Universidad Abierta de Tanzania. Es codirector y presidente del Instituto Africano de Derecho y Tecnología. Sus publicaciones sobre las leyes de privacidad en África son pioneras y ha estudiado los efectos e influencia que el RGPD ha tenido en el continente africano).

[154] Id

[155] Id

[156] Id

Protección de Datos. “Kenia se ha unido a la comunidad global en términos de estándares de protección de datos”, declaró Joe Mucheru, actual secretario del Gabinete de Kenia en el Ministerio de Información y Comunicaciones.

Se ha mencionado escasamente la influencia de la Convención de la UA. Desde asuntos relacionados con la clasificación de datos, los derechos de los interesados, las obligaciones legales de los controladores y procesadores de datos, el procesamiento legítimo de datos, la seudonimización y anonimización, la notificación de infracciones y las disposiciones de ejecución, entre otros, tienen un fuerte matiz del RGPD.

Esto puede traer consigo una fragmentación de legislaciones, al no basarse en acuerdos regionales, dificultando a largo plazo el comercio interno de países vecinos. El desarrollo a nivel regional no presenta incentivos suficientes para las economías en desarrollo para dejar de lado diferencias políticas o culturales, pero recordemos que ese tipo de iniciativas son valoradas en el requisito de adecuación.

1.4.2. Divergencia en modelos de privacidad

Un problema importante son las divergentes visiones de privacidad. De esta forma, China, Rusia[157] o India extraen más datos de sus ciudadanos que cualquier otro país del mundo. Como resultado, es poco probable que países vecinos con un elevado grado de relación, como es el caso de Pakistán[158] o India[159] con China, adopten una visión muy alejada de estos en la práctica real.

---

[157] SOLDATOV, A. & BOROGAN, I., “*Putin Trolls Facebook: Privacy and Moscow’s New Data Laws”*, Foreign Affairs, en https://www.foreignaffairs.com/ articles/russian-federation/2015-11-03/putin-trolls-facebook (Fecha de consulta: 05/03/2021).

[158] LATIF HAMDANI, Y., *“GDPR and the Pakistani context*”, en https://www.thenews.com.pk/tns/detail/568766-gdpr-pakistani-context (Fecha de consulta: 23/02/2021).

[159] DIXON, P., “*A Failure to B Do No Harm – India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.”,* Health Technol (Berl), Volumen 7, Nº 4, 2017, pp. 565.

La gobernanza de datos de China se deriva del interés nacional en utilizar los datos personales como un recurso valioso para desarrollar la industria de los datos y mantener la estabilidad social.[160] La presencia china en África, por ejemplo, es una constante desde hace años. La importancia que tiene para China el continente y sus recursos la sitúa en un punto clave de la expansión del modelo llamado "*Belt and Road Initiative"* (BRI).

No es un secreto que el continente africano es una importante y decisiva extensión de BRI. De acuerdo con los datos disponibles, existen más de diez mil empresas chinas en África, de las que aproximadamente el 90% son de capital privado, con planes a futuro. El número de ciudadanos chinos viviendo en el continente excede los dos millones y el interés chino continua en ascenso[161]. Restricciones importantes del flujo de datos podrían suponer un conflicto a largo plazo[162].

En los EEUU se valora más de manera generalizada la libertad de expresión[163]. Cuando Filipinas redactó una legislación nacional sobre privacidad para garantizar el acceso continuo al mercado de procesamiento de datos de la UE, las empresas estadounidenses con sede en ese país suspendieron los planes de inversión porque los costes operativos aumentaban demasiado[164].

El enfoque europeo para regular los flujos de datos transfronterizos se basa claramente en la intención de mantener un alto nivel de salvaguardias para los

---

[160] PERNOT-LEPLAY, E., *"China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?",* Penn State Journal of Law & International Affairs, 2020, pp. 68

[161] MARTINEZ GONZALEZ, C., *"Necesidad de protección de los intereses chinos en África, ¿una oportunidad para las empresas de seguridad españolas?*", en Estudios Estratégicos - Universidad de Granada (global-strategy.org) (Fecha de consulta: 25/02/2021).

[162] JOHNSTON, L. A*., "The Belt and Road Initiative: What is in it for China?",* Asia and the Pacific Policy Studies, Volumen 6, Nº 1, 2018, pp. 46 y ss.

[163] KOENIG, T. H. & RUSTAD, M. L., "*Towards Global Data Privacy Standard*", Florida Law Review, Volumen 71, Nº 2, 2019, pp. 387-410.

[164] Supra nota 90.

derechos y libertades de la ciudadanía, como lo demuestran las tensiones con los EEUU y el predominio de las decisiones judiciales sobre los intereses económicos. Por el contrario, las restricciones a los flujos de datos y las políticas para defender la soberanía digital introducidas por países como China, están orientadas a la vigilancia y el control (aunque replica cada vez más al RGPD en la relación consumidor/empresas).

2. ENFOQUE REGULATORIO PARA PAÍSES EN DESARROLLO

Los países de Asia, África y América Latina han experimentado un rápido crecimiento de empresas emergentes de tecnología, junto con el desarrollo de legislaciones inspiradas en el RGPD. Por lo tanto, un nuevo estándar global que regule los datos debe garantizar necesariamente que no haya impactos económicos adversos para estos países.

La UE debería considerar formas de mitigar estos impactos adversos, así como aumentar los incentivos económicos para los signatarios del Convenio 108+ (C108+). Uno de esos intereses evidentes es, por supuesto, el acceso al propio mercado único digital de la UE.

Para la UE, la protección de datos siempre ha estado íntimamente ligada al objetivo de promover la realización del mercado interior, además del objetivo de salvaguardar los derechos humanos fundamentales de los interesados[165]. Por el contrario, la agenda del C108+ se ocupa predominantemente de la promoción de los derechos humanos.

2.1. El Convenio 108+: una perspectiva humanista y global

Si bien en la Unión Europea se elaboró en su día una Directiva sobre Protección de Datos Personales (95/46/CE), ya derogada por el Reglamento (UE) 2016/679, en vigor desde mayo de 2016, fue el Consejo de Europa el que, teniendo ya garantizado en el artículo 8 CEDH el tratamiento de datos personales, elaboró

[165] Supra nota 8, pp. 100.

una serie de normas con objeto de regular la protección de datos y poder hacer frente a las amenazas que se pudieran derivar del tratamiento de datos personales.

La más importante es el Convenio 108 de 28 de enero de 1981. Como bien expone Cazurro, uno de los principales motivos por los que se decidió redactar un convenio y no un protocolo, fue el deseo de que la norma resultante no se limitara al ámbito del Consejo de Europa, sino que existiera la posibilidad de que se adhirieran al Convenio países que no fueran miembros de tal organización. De ahí que la rúbrica no incluyera el adjetivo "europeo"[166].

El C108 es el único tratado multilateral de este tipo. No en vano, el día de la Protección de Datos (a nivel mundial) es el 28 de enero, día de su firma hace 40 años. Podemos observar, en la adhesión de Uruguay al C108 en 2013, como el Consejo declaró que, al estar abierto a la firma de cualquier país, es el único estándar vinculante que tiene el potencial de ser aplicado en todo el mundo, proporcionando seguridad jurídica y previsibilidad en relaciones internacionales[167].

Por último, no podemos dejar de señalar que, de la misma manera que ha ocurrido en la Unión Europea, por parte del Consejo de Europa se ha trabajado de manera intensa en la actualización y modernización de la normativa para adaptarla a los nuevos cambios tecnológicos existentes[168]. Ello se ha llevado a cabo a través de un modernizado Convenio 108, denominado Convenio 108+, aprobado en 2018[169].

---

[166] Supra nota 8, pp. 85.

[167] CoE, "*Personal data protection: Uruguay becomes first non-European state to accede to "Convention 108*"", en https://www.coe.int/en/web/portal/news-2013/-/asset_publisher/TEHtOeUO1Ozc/content/personal-data-protection-uruguay-becomes-first-non-european-state-to-accede-to-convention-108- (Fecha de consulta: 27/02/2021).

[168] El Convenio 108 tiene un protocolo adicional que lo actualiza y que han bautizado con el nombre de Convenio 108+. Este nuevo Convenio está siendo ratificado por los distintos países interesados. España lo ratificó en su aniversario de este año, el 28 de enero de 2021.

[169] El Consejo de Europa ha elaborado un cuadro con las diferencias entre el Convenio 108 y su modernización 108+, que puede encontrarse en el siguiente enlace https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958.

El artículo 4 del C108+ declara que quien desee adherirse debe tomar las medidas necesarias para brindar niveles efectivos de protección de datos. Los requisitos de acceso son más asequibles que los del RGPD. Es probable que un país pueda acceder al C108 + incluso si está motivado principalmente por el deseo de alcanzar un respeto internacional, siempre que demuestre la capacidad de proteger los datos personales de acuerdo con las reglas básicas del C108+[170].

Esto es así, por el enfoque multilateral del Consejo de Europa, con múltiples países miembros distintos entre sí, fomentando la convergencia entre diferentes contextos culturales, marcos legales e intereses económicos. En este sentido, Cazurro considera que al tener unos principios que van más allá de las barreras comunitarias, propicia la adhesión de terceros Estados y, por lo tanto, favorece un intercambio de información que enriquece el comercio internacional.

La adhesión al C108+ no será una opción realista para los Estados no europeos que no compartan ese compromiso, ya que puede que no respeten elementos como la insistencia en la completa independencia de las autoridades de protección de datos[171]. En este sentido, los países en desarrollo siguen teniendo obstáculos que superar.

Pauletto[172] y Greenleaf[173] señalan acertadamente una multiplicidad de beneficios que pueden derivarse de la adhesión al C108+[174], incluida una mayor estabilidad en la gestión de los flujos de datos transfronterizos, el reconocimiento

[170] Supra nota 28, pp. 9 y ss.

[171] Artículo 15.5 del Convenio 108+.

[172] Christian Pauletto es profesor en la Universidad Internacional de Ginebra. Ha ejercido como representante de Suiza en foros multilaterales y relaciones bilaterales. Además, ha elaborado publicaciones centradas en el Convenio 108 y los estándares de privacidad. Puede verse más en https://www.iun.ch/en-en/faculty-research/faculty

[173] Graham Greenleaf es profesor de Derecho y Sistemas de la Información en la Universidad de Nueva Gales del Sur en Australia. Su trabajo ha estado muy vinculado al estudio de la privacidad y la protección de datos. En la respuesta obtenida por el Consejo de Europa, fue uno de los autores recomendados. Para verse más en https://www.law.unsw.edu.au/staff/graham-greenleaf

[174] Supra nota 28, pp. 10-11.

de cumplimiento de los estándares internacionales, la asistencia de los Europa y el requisito de solo estándares de protección moderados (a diferencia del RGPD)[175].

Sin embargo, la adhesión no garantiza la recompensa más atractiva: la adecuación por parte de la Comisión Europea. Como indican tanto el considerando 105 como el artículo 45.2 RGPD en el apartado c), la Comisión debería valorar la adhesión al Convenio al determinar la adecuación, pero la adhesión por sí sola no basta. Aun así, es el mejor pilar sobre el que construir un proyecto válido de protección de datos para países en desarrollo.

No obstante, encontramos casos como el de India que, siendo el país más grande del mundo, ha mostrado interés en la adopción de normas de protección de datos alineadas con Europa. Sin embargo, el CoE apenas figura en su proyecto, mientras que el RGPD ocupa un lugar destacado[176]. Esta hoja de ruta debería ser corregida, pues los beneficios de pertenecer al C108+ son considerables.

La Comisión ha manifestado su apoyo afirmando que la adhesión a dicho Convenio es un factor importante que la Comisión Europea tendrá en cuenta en su evaluación de adecuación[177]. Además, la Comisión reconoce el papel que el C108 ha desempeñado en la difusión del modelo europeo de protección de datos a nivel global y predice que el impacto práctico del C108+ puede ser mucho mayor.

Debido a este hecho, ha afirmado que promoverá la adhesión de terceros países al Convenio. Junto con esto declaró que "reflejará los mismos principios que los consagrados en las nuevas normas de protección de datos de la UE y, por tanto,

---

[175] GREENLEAF, G., "*Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe*", UNSW Law Research Paper, Nº 16-52, 2016.

[176] White Paper of the Committee of Experts on a Data Protection Framework for India, 2017, en https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf (Fecha de consulta: 19/02/2021).

[177] Comunicación de la Comisión al Parlamento Europeo y al Consejo, *"Intercambio y protección de los datos personales en un mundo globalizado"*, 2017, en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

contribuirá a la convergencia hacia un conjunto de altos estándares de protección de datos"[178].

Una de las Conferencias del Convenio 108+ en enero de 2021, muestra la influencia de esta regulación[179]. En Costa Rica lo defienden como una herramienta para lograr superar su Asamblea legislativa, muy dividida políticamente y, de esta forma, poder exigirse unas reformas serias en esta materia con una justificación que supere el debate a nivel interno. Uruguay, afirma que, aunque parezca lejana geográficamente ha marcado un camino en la forma de encarar la regulación en Latino América y colaboran con la Red Iberoamericana en su difusión[180].

El CoE dio respuesta a nuestras dudas sobre el Convenio 108+ y su influencia global y nos recordó que el derecho a la privacidad es un derecho humano universal previsto en primer lugar por el UNDHR en su artículo 12 (pero también por otros instrumentos regionales de derechos humanos como el Convenio Europeo de Derechos Humanos), por lo tanto, los Estados (y otras partes interesadas) tienen la obligación positiva de defender y garantizar este derecho a todas las personas.

En este sentido el Consejo de Europa no abandona a los países en desarrollo y, a través de sus programas de asistencia técnica, está ayudando a los países en su esfuerzo por adoptar una legislación nacional para la protección de la privacidad y los datos personales basada en el Convenio 108+ para responder a estas obligaciones, como fue el caso de Kenia en 2019.

Una de las cuestiones más debatidas y cuestionadas es la división que pueda crear como barrera comercial. En este sentido, el CoE nos respondió que la protección de la privacidad y los datos personales no es de ninguna manera un

[178] Id

[179] CoE, "*Data Protection Day 2021 in Latin-America 40th Anniversary of data protection Convention 108*", en https://www.coe.int/en/web/data-protection/dpd2021-in-latin-america (Fecha de consulta: 03/03/2021).

[180] Se puede ver más información sobre las iniciativas de cooperación en https://ec.europa.eu/fpi/sites/fpi/files/ann8_international_digital_cooperation_personal_data_protection_and_flow.pdf (Fecha de consulta: 03/03/2021).

impedimento para el comercio, pues favorece la seguridad jurídica. No obstante, afirman ser conscientes de que no siempre será así para todos.

Según afirma el Consejo, aquellos países que no tienen un marco legal con un nivel de protección de datos personales comparable al de sus vecinos (o de otra parte de su región o del mundo) con los que desean interactuar, podrían afrontar algunas dificultades en áreas que supongan la transferencia de datos personales, no solo en asuntos comerciales, sino en otras áreas, como el intercambio de datos relacionados con la salud, la cooperación en materia de justicia penal, la banca móvil o las redes sociales.

Para remediar esto, el CoE nos recuerda el caso de Gambia[181]. El país con el apoyo del CoE ha adoptado una política de privacidad completa y un proyecto de ley de privacidad en aproximadamente 1 año. Estos desarrollos para Gambia seguramente tendrán un impacto en sus relaciones con su país vecino, Senegal, que es parte del Convenio 108, pero también con otros en África, Europa y América Latina.

Además, considera que EEUU y China están en "conversaciones estables" para desarrollar una legislación nacional en línea con el RGPD y el Convenio 108+, por lo que asumir una posición europea, podría ser el camino a seguir para los países en desarrollo que luchan por tener un papel en el comercio global. Al ver como obtienen el visto bueno de un convenio internacional vinculante, la inversión extranjera los vería más seguros, con gran potencial y pioneros en su campo.

Al mismo tiempo, estas economías en desarrollo podrían establecer conversaciones a nivel regional fomentadas por esos principios, dándole más importancia a la armonización y aumentando el comercio entre ellas. Las bases más laxas hacen posible regular por etapas la legislación, teniendo, tal vez, al mercado de la UE como objetivo final.

[181] Puede verse más información en https://www.coe.int/en/web/data-protection/newsroom/-/asset_publisher/7oll6Oj8pbV8/content/privacy-policy-in-the-gambia (Fecha de consulta: 05/03/2021).

2.2. Cooperación internacional en el ámbito de la protección de datos

Fomentar la convergencia entre diferentes sistemas de privacidad también significa aprender unos de otros mediante el intercambio de conocimientos, experiencias y mejores prácticas. Por ello, la Comisión ha intensificado su diálogo sobre protección de datos y flujos de datos con una amplia gama de actores y en diferentes foros, a nivel bilateral, regional y multilateral.

2.2.1. La dimensión bilateral

Tras la adopción del RGPD, ha habido un interés creciente en la experiencia de la UE en el diseño, negociación e implementación de reglas de privacidad actualizadas. El diálogo con países que atraviesan procesos similares ha adoptado varias formas que mostraremos a continuación y que deberían responder completamente a la cuestión sobre el interés que tiene Europa en los países en desarrollo[182].

Los servicios de la Comisión han realizado presentaciones a una serie de consultas públicas organizadas por gobiernos extranjeros que consideran la legislación en el área de la privacidad, por ejemplo, India, Malasia y Etiopía. En algunos países, los servicios de la Comisión tuvieron oportunidad de testificar ante los órganos parlamentarios competentes, por ejemplo, en Brasil, Chile, Ecuador y Túnez.

Además, en el contexto de las reformas en curso de las leyes de protección de datos, se llevaron a cabo reuniones específicas con representantes gubernamentales o delegaciones parlamentarias de muchas regiones del mundo (como Georgia, Kenia, Taiwán, Tailandia y Marruecos). Esto brindó oportunidades

[182] Comunicación de la Comisión al Parlamento Europeo y al *Consejo "La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos"*, en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0264 (Fecha de consulta: 13/02/2021).

para aclarar conceptos importantes del RGPD e ilustrar los beneficios de la convergencia.

Alexandre Baron, Jefe de Sección del departamento de Gobernanza y Macroeconomía de la Delegación de la Unión Europea en Kenia nos trasladó que la UE ha identificado la protección de datos como un área prioritaria para la cooperación con Kenia en los próximos años. De hecho, en el contexto de dicha cooperación bilateral con Kenia, actualmente se están desarrollando asociaciones con la Comisión de Protección de Datos de Kenia, junto con los Estados miembros de la UE.

Así nos mostró que "el interés es garantizar que, a medida que se desarrollen nuevas legislaciones secundarias para implementar el DPA, estas sigan alineadas con el RGPD, en la medida de lo posible, como ya es el caso del propio DPA. Por lo tanto, la UE tendrá como objetivo apoyar a la Comisión de Protección de Datos (autoridad nacional competente requerida por ley) recientemente establecida, para que esté capacitada para implementar su mandato y hacer cumplir el DPA en Kenia.

La brecha digital en el mundo en desarrollo es amplia y, por lo tanto, este consentimiento no tendrá sentido si no se realizan esfuerzos concentrados para cerrar la brecha digital. De hecho, entre muchas otras propuestas, la estrategia "*Digital4Development*"[183] de la Comisión Europea, ejemplifica la promoción de la alfabetización digital como una de sus áreas prioritarias en países en desarrollo.

La UE ofrece apoyo para integrar las habilidades digitales, así como en la mejora de la infraestructura digital, la realización de reformas regulatorias, el fomento del espíritu empresarial digital y la promoción del uso de tecnologías digitales. La Comisión Europea publicó en 2020 diversos proyectos con múltiples iniciativas en Asia, África y Latino América, donde la protección de datos tenía un

[183] Puede verse más información sobre esta iniciativa en https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-157-F1-EN-MAIN-PART-1.PDF.

papel central[184]. África será una pieza primordial en la estrategia de digitalización europea de los próximos años[185].

2.2.2. Dimensión multilateral

Más allá de los intercambios bilaterales, la Comisión también participa activamente en varios foros multilaterales para promover valores compartidos y construir la convergencia a nivel regional y mundial, como el Convenio 108+.

Durante la reciente conferencia sobre privacidad de datos del Consejo de Europa en 2021, se discutieron algunos de los cambios recientes en distintos continentes. Los asistentes africanos resaltaron la importancia que había tenido poder aplicar una ley de protección de datos después del RGPD.

Aún con ello, se comentó la evidente dificultad de lograr esa decisión de adecuación por parte de la Comisión, pero mostraron mucho optimismo respecto al interés mostrado por Europa en ofrecerles apoyo (como hemos podido observar en las iniciativas comentadas en el apartado anterior).

La encargada de la protección de datos en Mauricio, Drudeisha Madhub, comentó el programa del Grupo de Trabajo de Economía Digital UE-AU en el contexto de la Nueva Asociación de Economía Digital África-Europa[186] (PRIDA). Este proyecto europeo sirve para estandarizar reglas y principios para la transferencia de datos africana, dado el escaso éxito de las iniciativas regionales (véase Malabo como referencia).

---

[184] Pueden consultarse en profundida las últimas iniciativas de 2020 en https://ec.europa.eu/fpi/sites/fpi/files/ann8_international_digital_cooperation_personal_data_protection_and_flow.pdf.

[185] Joint communication to the European Parliament and the Council, *"Towards a comprehensive strategy with Africa"*, en https://reliefweb.int/report/world/joint-communication-european-parliament-and-council-towards-comprehensive-strategy (Fecha de Consulta: 27/02/2021).

[186] COMISIÓN EUROPEA, "*New Africa-Europe Digital Economy Partnership Accelerating the Achievement of the Sustainable Development Goals"*, AU-EU Digital Economy Task Force (AU-EU DETF, 2019.

Esto indica que los beneficios de una armonización tendrían efectos muy positivos para la economía africana. Los asistentes comentaron que espera que la Unión Africana (políticamente) presione para que se apliquen esos principios en ausencia de un RGPD africano.

Esto se traduciría en que los países en desarrollo de regiones donde la UE muestre un interés especialmente elevado, como se ha mostrado en África, podrían acertar a la hora de establecer legislaciones cercanas al modelo europeo, aprovechando sus ganas de extender el RGPD a la vez que armonizando el continente con una base centrada en los derechos humanos.

Con el tiempo, los principios extendidos con ayuda europea pueden modernizar las iniciativas regionales actuales y lograr mayor consenso político en estos territorios. La falta de iniciativa política parece ceder cuando se tiene como recompensa un posible acceso al mercado de la UE. Así se está viendo en África.

Mauricio ha facilitado la transferencia de datos en su ley, algo que el RGPD no ha hecho en el mismo sentido, porque la adecuación es clave para Europa. Mauricio asume moralmente esa misma preocupación, pero prefiere velar por el balance adecuado entre que los negocios florezcan y que se restrinjan oportunidades.

En este sentido y como refleja una de las respuestas obtenidas de la mano de las Naciones Unidas (UNCTAD), las posibilidades de la mayoría de países en desarrollo para obtener la decisión de adecuación por parte de la Comisión es muy baja. Sin embargo, un modelo basado en fases podría resultar mucha más efectiva que establecer una legislación estricta de golpe.

Así, un modelo como el de Mauricio, que a nivel estratégico no asume todas las provisiones del RGPD, dejando margen para su crecimiento empresarial, será un ejemplo para el resto. Mauricio pertenece al Convenio por lo que demuestra que una legislación como la suya puede ser apta como estándar de mejores prácticas.

Con el tiempo es muy posible que logre la adecuación a la UE, pero mientras tanto, se beneficia de estar incluido en las iniciativas de desarrollo de la Comisión Europea, a la par que ya está adherido al Convenio de Europa (y su protocolo adicional) y puede construir su propio sistema de protección de datos que no parece ahuyentar en absoluto la inversión extranjera[187].

En definitiva, considero que disponer de un marco moderno de protección de datos que fomente inversiones y la competitividad, al tiempo que contribuye al respeto de los derechos humanos y el Estado de derecho, es una meta alcanzable y deseable para países en desarrollo. Además, considero que es una inquietud que compartimos y donde una cooperación sería enriquecedora para ambas partes.

CONCLUSIONES

El RGPD está destinado a establecer estándares dorados para la protección de datos. Como comprobamos en las teorías difusión, el efecto Bruselas ha trasladado al RGPD a múltiples países, inspirando legislaciones similares y que siguen sus principios fundamentales, incluso en jurisdicciones donde prevalecen otras visiones de privacidad (CCPA de California).

La falta de una línea ideológica única y global en materia de protección de datos es un problema latente para el comercio internacional. No obstante, también ha permitido a la UE, gracias a su influencia económica significativa, una oportunidad para influir en los valores, las identidades y las culturas en la era del internet sin fronteras.

El supuesto de extraterritorialidad incluido en su art. 3 RGPD, supone una evolución loable en cuanto a su ámbito espacial de aplicación y la victoria de la Unión Europea respecto al valor de sus derechos fundamentales en cualquier lugar

[187] El 1 de enero de 2021, entró en vigor el Tratado de Libre Comercio entre el Gobierno de la República Popular China y el Gobierno de la República de Mauricio, en http://spanish.mofcom.gov.cn/article/ultimasniticias/202101/20210103029475.shtml (Fecha de consulta: 6/03/2021).

del mundo. Disponen así de tribunales de control capaces de hacer estos derechos efectivos globalmente en la práctica diaria.

Como defendían los autores que hemos citado, los costes derivados del RGPD, u otras políticas estrictas de privacidad, pueden ser vistos como un activo inmaterial que aporte una diferenciación competitiva o como una carga económica improductiva. Como también hemos comprobado, esto no está exento de dificultades para pequeñas y medianas empresas y las instituciones deberían velar por asegurar el menor impacto negativo.

Además, es muy posible que las empresas obligadas a utilizar el RGPD cambien sus políticas de datos extendiendo los derechos fundamentales de la UE a países donde este derecho carezca del mismo valor. La difusión de estos derechos puede ser replicado por otras empresas, bien sea para poder acceder al mercado europeo o, simplemente, por sentirse obligados por la competencia. También es posible que los consumidores que perciban una diferenciación de trato exijan los mismos derechos, amplificando esta tendencia.

Los últimos avances los encontramos en la Decisión de adecuación con Japón, que consolida un camino distinto a los modelos de EEUU y China. Además, demuestra que un camino intermedio entre preservar los valores y cultura nacionales y lograr armonizar distintas visiones es posible. El modelo japonés permite a una de las partes cosechar los beneficios financieros de una Decisión de adecuación al mismo tiempo que ajusta el alcance de las reformas a su marco y cultura de privacidad nacional.

Como hemos analizado a lo largo del presente trabajo, el RGPD no supone un mero trámite ni la decisión de adecuación es sencilla de conseguir. No basta con establecer unas normas similares. Las exigencias requieren de un profundo análisis político, económico y social, para evaluar el estado de cada país en contraposición con lo que desde Europa se considera unos principios fundamentales ineludibles.

Al realizar la lectura del artículo 45.2 RGPD que establece los elementos que tendrá en consideración la Comisión, se prevé que no será sencillo lograr un acuerdo. Manteniendo esta perspectiva, Schrems II la confirma. El fracaso del

nuevo pacto entre EEUU-UE pone de manifiesto que el rigor que se exige para lograr una adecuación solo se conseguirá de dos formas, (1) considerando la protección de datos como un derecho fundamental y que se priorice sobre otros derechos (véase la seguridad nacional en EEUU) o, (2) que se desarrolle un sistema como el modelo japonés.

Los países más avanzados, pueden establecer una normativa adecuada y equivalente preservando sus valores, pero los países en desarrollo necesitarían una reforma profunda de sus sistemas para lograr la transparencia demandada. También tendrían que reformar su sistema para asegurar la independencia de las autoridades. En definitiva, el RGPD no es una mera norma de protección de datos. El cierre del mercado europeo a países que no cumplan con el estándar puede ser una de las contribuciones a la promoción de los derechos humanos más grandes y silenciosas.

La UE pondría en peligro su rigurosa regulación si suspendiera su responsabilidad frente a economías en desarrollo. Acuerdos especiales para este tipo de países provocarían conflictos y daños a los derechos de los consumidores y haría que el esfuerzo de las reformas no fuese tan intenso. Por estas razones, una exención exclusiva probablemente no sea la solución óptima para ninguna de las partes. De esta forma, un "*Privacy Shield"* para estos países es improbable.

Lograr la adecuación supone todo un reto atendiendo a lo expuesto anteriormente y tomando como base los elementos principales que la Comisión tendrá en cuenta en su evaluación. Tras la Decisión de adecuación a Japón, se prevé una mayor participación del resto de órganos políticos de la Unión Europea, pues en el Considerando 190 el Parlamento Europeo emitió una resolución sobre la idoneidad de las garantías ofrecidas por Japón.

Ese hecho es un hito procedimental porque no está previsto en la norma, así que es posible que, si no se vuelve habitual, se dé en situaciones delicadas o de especial importancia. En países en desarrollo, probablemente su mayor ventaja resultará en ser pioneros en el campo de la protección de datos. Es posible que como ocurrió en el caso de Argentina, que no estuvo libre de críticas al ser considerada

adecuada, estos órganos políticos de la UE exijan máximo rigor en el análisis de los principios requeridos.

No obstante, debemos ser conscientes de que los países en desarrollo es muy posible que hayan requerido de reformas profundas y, con ellos, el marco de revisión cada 4 años (art. 45.4 RGPD) debería adaptarse. Esto significa que no siempre se contará con un plazo relativamente extenso de tiempo para equilibrar el sistema normativo impuesto y corregir sus defectos a tiempo. Se arriesgan los países que quebranten los elementos esenciales a perder ese mecanismo de transmisión de datos, con un rechazo unilateral de la UE (art. 45.5 RGPD).

En respuesta al planteamiento de Koen Lenaerts, Europa debería sentirse orgullosa de las consecuencias que ha traído consigo el RGPD. Las ambiciosas disposiciones del RGPD pueden ser valiosas para estimular la difusión de derechos fundamentales, materializados en la regulación de protección de datos. No obstante, los países en desarrollo deben diseñar cuidadosamente reglas más flexibles y, en algunos casos, menos estrictas, para crear un terreno común a nivel regional que permita construir su propio recorrido.

En este sentido, considero que Europa no debe ser ajena a lo que el mundo haga con estos estándares exigidos por el RGPD, pues los efectos negativos pueden traer la exclusión de muchos países al comercio y diálogo internacional. Promover los valores de la dignidad humana debe incluir, como considero probado a lo largo de este trabajo, un interés profundo de Europa en solventar estos efectos. La construcción de infraestructuras y compartir conocimiento, es crucial para el éxito.

De esta forma, tanto en el ámbito de la Unión Europea como en el marco del Consejo de Europa, existen programas de asistencia y un historial de conversaciones con países de todos los continentes. Además, sus proyectos de digitalización en estos territorios fomentarán aún más las conversaciones bilaterales con los gobiernos nacionales y desde una perspectiva multilateral, con autoridades regionales, que pueden desarrollar marcos comunes de protección de datos con una base centrada en valores compatibles con la UE (como está sucediendo en África).

En el contexto de la privacidad de datos en economías frágiles, tener políticas más amplias que fomenten la innovación, tendría un beneficio mayor que las leyes estrictas de protección de datos. Deben elaborarse de forma incremental, implementándose en fases hasta el objetivo final, como está haciendo Mauricio. Debería haber un equilibrio dinámico entre los nuevos modelos comerciales, las nuevas normas digitales aceptadas por la comunidad internacional y las auténticas preocupaciones nacionales de cada país.

En este sentido, hay varios motivos por los que los países en desarrollo deberían considerar que le conviene adherirse a la Convención 108+. Para muchos países con recursos disponibles limitados y experiencia en el campo de la privacidad, el apoyo recibido para evaluar, desarrollar e implementar su legislación es una motivación clave. La Convención ya cuenta con una cartera considerable de programas y actividades de cooperación, especialmente en América Latina y África.

Dada la creciente priorización de la protección de datos tanto en el sector público como en el privado, el cumplimiento de la Convención es un activo que tiene valor para cualquier jurisdicción. Además, la Convención constituye un atractivo foro multicultural que permite el intercambio de información y experiencias. Esta particularidad es importante, en especial, para países en desarrollo sin base legal previa para embarcarse en un proceso bilateralmente.

Desde la perspectiva del tercer país, la adhesión al Convenio 108+ tiene, por tanto, un doble objetivo: 1) Obtienen un reconocimiento internacional de su ley de privacidad nacional, acceso a un foro global e intercambio de información y experiencias; 2) En materia de derechos humanos, el CoE ostenta una trayectoria que muestra el más alto nivel de compromiso con uno de los derechos humanos fundamentales recogidos en la DUDH.

Los países que obtuvieron una decisión de adecuación del RGPD nunca deben olvidar, como hemos comentado, que la adecuación es una decisión unilateral autónoma de la Comisión que puede revertirse en revisiones posteriores. Este hecho favorece iniciar los planes de desarrollo de protección de datos en el marco de la

Convención, para asegurar que en caso de fallar en la adecuación o de ser reevaluados negativamente, siguen disponiendo de una referencia de calidad que no les perjudique reputacionalmente.

Además, la Convención es el mejor primer paso hacia una decisión de adecuación. Como hemos analizado en el presente trabajo, se tendrá en cuenta la adhesión a tratados internacionales o regionales (especialmente el C108+). Incluso si no se plantea una adecuación, es razonable presumir que la participación en la Convención facilitaría el desarrollo de salvaguardas adecuadas con un Estado miembro de la UE, a la par que reduciría el riesgo para la inversión extranjera.

Se necesita un enfoque que tenga en cuenta las diversas cuestiones políticas y el contexto de la economía digital de cada país. Las diferentes culturas de protección de datos y niveles de desarrollo hacen inevitable que el RGPD sea un estándar demasiado ambicioso para ser aceptado en todas partes. El Convenio 108+ es atractivo porque es legalmente vinculante y una armonización desde la base de unos principios sobre los que cada país puede regular más ampliamente en su cultura y realidad del momento.

De esta forma, los países en desarrollo que han iniciado reformas profundas inspiradas en el RGPD, considero que no han tomado un rumbo equivocado, pues el interés de Europa es profundo. No obstante, deberían considerar la vía del Convenio 108+, pues está siendo muy infravalorado y lograría mejores resultados que una legislación tan estricta, que no obtendría, igualmente, acceso al mercado de la UE. En el contexto regulatorio y geopolítico de países en desarrollo, es más importante definir un estándar Global que uno Dorado.

El RGPD ha puesto la conversación de la privacidad en el foco mundial, pero el C108+ puede servir como vínculo entre naciones distintas, cultural y económicamente. Extendiendo los valores humanistas europeos por distintas jurisdicciones, incluidos los países en desarrollo, favoreciendo la construcción de sistemas regionales extranjeros en base a estos. El C108+ se alza como una herramienta clave para que nos parezcamos más, en beneficio del respeto a la dignidad humana.

BIBLIOGRAFÍA

ABERASTURI GORRIÑO, U., "*Movimiento internacional de datos. Especial referencia a la transferencia internacional de datos sanitarios*", Revista de administración pública, Nº 186, 2011, pp. 333-340.

ALBRECHT, J. P., "*How the GDPR Will Change the World*", European Data Protection Law Review, Volumen 2, Nº 3, 2016, pp. 287-238.

ÁLVAREZ RIGAUDIAS, C., "*Condiciones para las transferencias internacionales de datos personales en servicios de cloud*", MARTÍNEZ MARTÍNEZ, R. (Editor), Derecho y Cloud Computing, Aranzadi, Navarra, 2012, pp. 5-6.

APARICIO VAQUERO, J. P., *"La protección de datos que viene: el nuevo Reglamento General europeo*", Ars Iuris Salmanticensis, 2016, pp. 33.

BAUER, M., ERIXON, F., KROL, M., LEE-MAKIYAMA, H. & VERSCHELDE, B., "*The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce"*, European Center for International Political Economy, 2013.

BAUER, M., LEE-MAKIYAMA, H., VAN DER MAREL, E. & VERSCHELDE, B., "*The Costs of Data Localisation: Friendly Fire on Economic Recovery*", ECIPE Occasional Paper, Nº 3, 2014.

BEEHAREE, Y., "*Mauritius updates to the Anti-Money Laundering and Combatting the Financing of Terrorism handbook*", en https://www.sannegroup.com/our-thinking/insights/2021/mauritius-updates-to-the-anti-money-laundering-and-combatting-the-financing-of-terrorism-handbook/.

BRADFORD, A., *"The Brussels Effect: How the European Union Rules the World"*, Oxford University Press, Nueva York, 2020, pp. 3-170.

BRIGHT, J. & HRUBY, A., *"The Rise Of Silicon Savannah And Africa's Tech Movement"*, TECH CRUNCH, en https://techcrunch.com/2015/07/23/therise-of-silicon-savannah-and-africas-tech-movement (Fecha de consulta: 21/01/2021).

BYGRAVE, L. A., *"The* '*Strasbourg Effect' on data protection in light of the Brussels Effect: Logic, mechanics and prospects",* Computer Law & Security Review, Volumen 40, 2021.

CAMPBELL, J., GOLDFARB, A. & TUCKER, C., *"Privacy regulation and market structure"*, Journal of Economics & Management Strategy, Volumen 24, Nº 1, 2015, pp. 47-73.

CANNATACI, J., "*Report of the Special Rapporteur on the Right to Privacy*", en https://undocs.org/A/73/438 (Fecha de consulta: 28/04/2021).

CAZURRO BARAHONA, V., *"Antecedentes y fundamentos del Derecho a la protección de datos",* J.M. BOSCH, 2020, pp. 125.

CHRISTENSEN, L., COLCIAGO, A., ETRO, F. & RAFERT, G., *"The Impact of the Data Protection Regulation in the EU*", Intertic Policy Paper, 2013, pp. 42-43.

COMISIÓN EUROPEA, "*Digital Single Market. Big data*". Big data (grandes datos o volúmenes de datos) es un término que se refiere a grandes cantidades de datos generados rápidamente y procedentes de diversas fuentes, pudiendo ser generados por personas o de manera automatizada. En https://ec.europa.eu/ (fecha de consulta: 27/04/2021).

COMISIÓN EUROPEA, "Informe de la Comisión: las normas de protección de datos de la UE empoderan a los ciudadanos y están adaptadas a la era digital", en https://ec.europa.eu/commission/presscorner/detail/es/ip_20_1163 (Fecha de consulta 28/04/2021).

COMISIÓN EUROPEA, "*Memo/17/15, Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers*", en http://europa.eu/rapid/press-release_MEMO-17-15_en.htm (Fecha de consulta: 25/02/2021)

COMISIÓN EUROPEA, "*New Africa-Europe Digital Economy Partnership Accelerating the Achievement of the Sustainable Development Goals",* AU-EU Digital Economy Task Force, 2019.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL *CONSEJO, "La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos"*, en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0264 (Fecha de consulta: 13/02/2021).

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL *CONSEJO, "Intercambio y protección de los datos personales en un mundo globalizado"*, 2017, en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=EN (Fecha de consulta: 13/02/2021).

CUNNINGHAM, M., "*Diminishing sovereignty: how European privacy law became international norm",* Santa Clara Journal of International Law, Volumen 11, Nº 2, 2013, pp. 421-430 & 449-552.

CURTISS, T., "*Privacy Harmonization and The Developing World: The Impact of The EU's GDPR on Developing Economic*", Washington Journal of Law, Technology & Arts, Volumen 12, Nº 1, 2016.

DE MIGUEL ASENSIO, P. A., *"Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea*", Revista Española de Derecho Internacional (REDI), Nº 1, 2017, pp. 7-8.

DÍAZ DÍAZ, E., "*El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*", Revista Aranzadi Doctrinal, Nº 6, 2016, pp. 13.

DIXON, P., "*A Failure to B Do No Harm – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.",* Health Technol (Berl), Volumen 7, Nº 4, 2017, pp. 565.

DODANI, S. & LAPORTE, R. E., *"Brain drain from developing countries: how can brain drain be converted into wisdom gain?"*, Journal of the Royal Society of Medicine, Nº 98, 2005, pp. 487–490.

DOWERS, A., "*The transnational reach of GDPR : a comprehensive framework that can regulate data privacy internationally , or is that unrealistic?",* UGA UFR Droit, 2019.

DURAN CARDO, B., *"La figura del responsable en el derecho a la protección de datos",* 2015, pp. 97-98 y 538-539.

FRANZ, V., HAYES, B. & HANNAH, L., "*Civil Society Organizations and General Data Protection Regulation Compliance: Challenges, Opportunities, and Best Practices*", 2020, pp. 24-25.

FRIZELL, S., "*How Kenya's New Data Privacy Bill Could Hurt Its Economy*", Council on Foreign Relations, en https://www.cfr.org/blog/howkenyas-new-data-privacy-bill-could-hurt-its-economy (Fecha de consulta: 23/01/2021).

GARCÍA MICÓ, T. G. & GARCÍA-PERROTE, I., "*Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II",* Revista para el Análisis del Derecho, 3, 2020, pp. 551-555.

GAY, C., "*The GDPR's Effect on Transatlantic Relations*", International Program Papers (Chicago Unbound), Nº 105, 2019.

GILL, M., "*Explained: In Kenya's digital ID system, echoes of India's Aadhaar*", en https://indianexpress.com/article/explained/in-kenyas-digital-id-system-echoes-of-indias-aadhaar-6244643/.

GOLDSMITH, J. & WU, T., "*Who Controls the Internet? Illusions of a Borderless World*", Oxford University Press, Nueva York, 2006, pp. 176.

GONZALO DOMENECH, J. J., *"Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros",* Cuadernos De Derecho Transnacional, Volumen 11, Nº1, 2019, pp. 350-371.

GREENLEAF, G. & COTTIER, B., *"Comparing African Data Privacy Laws: International, African and Regional Commitments"*, University of New South Wales Law Research Series, 2020, pp. 8.

GREENLEAF, G. & COTTIER, B., "*Data Privacy Laws and Bills: Growth in Africa, GDPR Influence*", Privacy Laws & Business International Report, Nº 18-52, 2018.

GREENLEAF, G., *"Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe*", UNSW Law Research, Nº 16-52, 2016.

GREENLEAF, G., *"European Data Privacy Standards Implemented in Laws Outside Europe",* Privacy Laws & Business International Report, Nº18-2, 2017.

GREENLEAF, G., *"Global Data Privacy Laws 2019: New Eras for International Standards"*, Privacy Laws & Business International, Nº 19-20, 2019.

GREENLEAF, G., *"How far can Convention 108+ 'globalise'? Prospects for Asian accessions"*, Computer Law & Security Review, Volume 40, 2021.

GREENLEAF, G., *"Modernised' Data Protection Convention 108 and the GDPR*" Privacy Laws & Business International Report, Nº 19-3, 2019.

HUANG, J., "*Applicable law to transnational personal data: Trends and dynamics",* German Law Journal, Volumen 21, Nº 6, 2020, pp. 1287-1292.

ISLAM, T. & ERSHADUL KARIM, M., *"Extraterritorial Application of the Eu General Data Protection Regulation: an International Law Perspective*", IIUM Law Journal, Volumen 28, Nº 2, 2020, pp. 537-548.

JABLONKA, I., "*The Origins of Mass Surveillance Interview with Sophie Cœuré*", en http://www.booksandideas.net/The-Origins-of- Mass-Surveillance.html (Fecha de Consulta : 06/03/2021).

JERKER SVANTESSON, D., "*The CJEU's Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, Yet So Very Important*", Maastricht Journal of European and Comparative Law, 2016, pp. 332-341. Para más información:

STJUE de 1 de octubre de 2015, asunto C-230/14, Weltimmo, ECLI:EU:C:2015:639.

JIA, J., ZHE JIN, G. & WAGMAN, L., *"The short-run effects of GDPR on technology venture investment",* National Bureau of Economic Research, 2018, pp. 6-10.

JOHNSTON, L. A., "*The Belt and Road Initiative: What is in it for China*?", Asia and the Pacific Policy Studies, Volumen 6, Nº 1, 2019, pp. 40-58.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, *"Towards a comprehensive strategy with Africa"*, en https://reliefweb.int/report/world/joint-communication-european-parliament-and-council-towards-comprehensive-strategy (Fecha de Consulta: 27/02/2021).

KITCHENMAN, W. F., "*U.S. Credit Reporting:Perceivid Benefits Outweigh Privacy Concerns*", The Tower Group, 1999.

KLOTH, A., "*One law to rule them all – On the extraterritorial applicability of the new EU General Data Protection Regulation*", Völkerrechtsblog, 2018, en https://voelkerrechtsblog.org/one-law-to-rule-them-all/.

KOENIG, T. H. & RUSTAD, M. L., "*Towards Global Data Privacy Standard*", Florida Law Review, Volumen 71, Nº 2, 2019.

KRASTEVA, S., SHARMA, P. & WAGMAN, L., "*The 80/20 rule: Corporate support for innovation by employees*", International Journal of Industrial Organization, 2015, pp. 5–10.

KUNER, C., "*Symposium on the GDPR and international law. The GDPR and international organizations"*, Cambridge University Press, 2020, pp. 15-19.

KUNER, C., "*Reality and Illusion in EU Data Transfer Regulation Post Schrems*", German Law Journal, Volumen 18, Nº 4, 2017, pp. 904.

KWASNY, S., MANTELERO, A. & STALLA-BOURDILLON, S., *"The role of the Council of Europe on the 40th anniversary of Convention 108*", Computer Law & Security Review, Volume 40, 2021.

LATIF HAMDANI, Y., "*GDPR and the Pakistani context*", en https://www.thenews.com.pk/tns/detail/568766-gdpr-pakistani-context (Fecha de consulta: 23/02/2021).

LOMAS, N., *"Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement With U.S."*, TechCrunch, en https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s (Fecha de consulta: 23/01/2021).

LÓPEZ-LAPUENTE, L., "*La aplicación extraterritorial del Reglamento General de Protección de Datos"*, Actualidad Jurídica Uría Menéndez, 2019.

MAKULILO, A. B., "*The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius"*, International Journal of Human Rights, Volumen 24, Nº 1, pp. 117-146, 2020.

MAKULILO, A. B., *"African accession to Council of Europe Privacy Convention 108*", Datenschutz Datensich, Volumen 41, 2017, pp. 364-367.

MAKULILO, A. B., *"One size fits all: Does Europe impose its data protection regime on Africa?"*, Datenschutz Datensich, Volumen 37, 2013, pp. 447-451.

MANNION, C., "*Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets*", Vanderbilt Journal of Transnational Law, Volumen 53, Nº 2, 2020, pp. 685-712.

MARTINEZ GONZALEZ, C., *"Necesidad de protección de los intereses chinos en África, ¿una oportunidad para las empresas de seguridad españolas?*", en Estudios Estratégicos - Universidad de Granada (global-strategy.org) (Fecha de consulta: 25/02/2021).

MARTÍNEZ MARTÍNEZ, R., "*Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos*", pp. 160. Y MARTÍNEZ MARTÍNEZ, R., *"La protección de datos no puede ser un freno a la innovación*", en https://confilegal.com/20150611-ricard-martinez-proteccion-datos-freno-innovacion-11062015-2104/ (Fecha de Consulta: 28/04/2021).

MARTÍNEZ MARTÍNEZ, R., "*Schrems II. Una breve reflexión desde los derechos fundamentales*", en https://diariolaley.laleynext.es (Fecha de consulta: 28/04/2021).

MATOO, A. & MELTZER, J., "*Resolving the conflict between privacy and digital trade*", Center for Economic and Policy Research, en https://voxeu.org/article/resolving-conflict-between-privacy-and-digital-trade (Fecha de consulta: 13/01/2021).

MELTZER, J., "*Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-Sized Enterprises and Developing Countries*", Global Economy & Development at Brookings, 2014.

MELTZER, J. P. & LOVELOCK, P., "*Regulating for a digital economy: Understanding the Importance of Cross-Border Data Flows in Asia*", Global Economy and Development at Brookings, 2018, pp. 19 y 20.

MUSILA, G., "*The Spread of Anti-NGO Measures in Africa: Freedoms Under Threat*", en https://freedomhouse.org/report/special-report/2019/spread-anti-ngo-measures-africa-freedoms-under-threat.

NISELOW, T., *"Five massive data breaches affecting South Africans*", Mail & Guardian, en https://mg.co.za/article/2018-06-19-five-massivedata-breaches-affecting-south-africans (Fecha de consulta: 03/03/2021).

ORTEGA GIMÉNEZ, A., *"La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español",* Tesis doctoral: Universidad de Alicante, 2014, pp. 42 y 45.

ORTEGA GIMÉNEZ, A., "*Transferencias Internacionales de Datos de Carácter Personal Ilícitas*", Aranzadi, Navarra, 2017, pp. 55-59.

PADÍN, A., *"El Tribunal de Justicia de la Unión Europea anula el Escudo de Privacidad*", en https://www.garrigues.com/es_ES/noticia/tribunal-justicia-union-europea-anula-escudo-privacidad-privacy-shield (Fecha de consulta: 02/02/2021).

PERNOT-LEPLAY, E., "*China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?"*, Penn State Journal of Law & International, Volumen 8, Nº 1, 2020, pp. 107-110.

PHILLIPS, T., KIRA, B., TARTAKOWSKY, A., DOLAN, J. & NATIH, P., "*Digital technology governance: developing countries priorities and concerns*". Digital Pathways at Oxford Paper Series; no. 3., 2020.

PIÑAR MAÑAS, J. L., "*Transferencias de datos personales a terceros países u organizaciones internacionales"*, ÁLVAREZ CARO, M. / RECIO GAYO, M. (Coordinador), Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Edición I, Reus, Madrid, 2016, pp. 428-429.

PIÑAR MAÑAS, J. L., "*Introducción*", ÁLVAREZ CARO, M. / RECIO GAYO, M. (Coordinador), Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Edición I, Reus, Madrid, 2016, pp. 15.

PIÑAR MAÑAS, J. L., *"El Tribunal de Justicia anula de nuevo las transferencias de datos entre la Unión Europea y Estados Unidos*", en https://www.eleconomista.es/opinion-legal/noticias/10702030/08/20/El-Tribunal-de-Justicia-anula-de-nuevo-las-transferencias-de-datos-entre-la-union-europea-y-estados-unidos.html (Fecha de consulta: 28/04/2021).

PIÑAR MAÑAS, J. L., "*El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades*

Europeas", Cuadernos de Derecho Público, Nº 19-20, 2013, pp. 58-60. Y ORTEGA GIMÉNEZ, A., "*Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE "Lindqvist", de 6 de noviembre de 2013*", Revista de derecho de Extremadura, Nº 7, 2010, pp. 101-105.

PISA, M., DIXON, P., NDULU, B. & NWANKWO, U., "*Governing Data for Development: Trends, Challenges, and Opportunities*", CGD Policy Paper 190. Washington, DC: Center for Global Development, 2020.

POP, V., "*ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust*", en https://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/ (Fecha consulta: 06/03/2021).

PRAMESTI, I. & AFRIANSYAH, A., *"Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia*", Advances in Economics, Business and Management Research (Atlantis Press), Volumen 130, 2020, pp. 84-90.

RAUTRAY, S., "*NGOs can't be denied foreign funds, rules Supreme Court"*, en https://economictimes.indiatimes.com/news/politics-and-nation/ngos-cant-be-denied-foreign-funds-rules-sc/articleshow/74519274.cms?from=mdr.

RECIO GAYO, M., "*Nivel adecuado para transferencias internacionales de datos*", Revista de la Facultad de *Derecho PUCP*, Nº 83, 2019, 207-240.

RECIO GAYO, M., "*Protección de datos e innovación: ¿(in)compatibles?",* Reus, Madrid, 2016, pp. 31-32.

RULE OF LAW INDEX, WORLD BANK, en https://tcdata360.worldbank.org/indicators/hf5cdd4dc?indicator=370&viz =choropleth&y ears=2017&compareBy=region / (Fecha de consulta: 25/01/2021).

SAFARI, B., *"Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection"*, Seton Hall Law Review, Volumen 47, Nº 3, 2017, pp. 809-836.

SCHWARTZ, P. M., "*Global Data Privacy : The EU Way*", New York University Law Review, Volumen 93, Nº 4, 2019, pp. 772-817.

SOLDATOV, A. & BOROGAN, I., "*Putin Trolls Facebook: Privacy and Moscow's New Data Laws"*, Foreign Affairs, en https://www.foreignaffairs.com/ articles/russian-federation/2015-11-03/putin-trolls-facebook (Fecha de consulta: 05/03/2021).

TORRE DE SILVA, J., LUIS PIÑAR, J. & RECIO, M., "*Guía sobre transferencias internacionales de datos*", CEMS ESPAÑA, 2020.

TRONCOSO REIGADA, A., "*Autoridades de control independientes*"**,** ÁLVAREZ CARO, M. / RECIO GAYO, M. (Coordinador), Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Edición I, Reus, Madrid, 2016, pp. 428-429.

TRONCOSO REIGADA, A., "*Hacia un nuevo marco jurídico europeo de la protección de datos personales*", Revista española de derecho europeo, Nº 43, 2012, pp. 48-47.

UNCTAD, "*Data Protection and Privacy Legislation Worldwide",* en https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Fecha de consulta: 16/01/2021).

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *"Data Protection Regulations and International Data Flows: Implications for Trade and Development"*, 2016, en https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

URÍA GAVILÁN, E., "*Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems*", Revista de Derecho Comunitario Europeo, Nº 53, 2016, pp. 267 y ss .

WANG, F. Y., *"Cooperative Data Privacy: The Japanese Model of Data Privacy and the Eu-Japan Gdpr Adequacy Agreement*", Harvard Journal of Law & Technology, Volumen 33, Nº 2, 2020, pp. 661-690.

WANGARI, N., "*Kenya must implement data protection law before 2022 presidential election*", en https://globalvoices.org/2021/01/16/kenya-must-implement-data-protection-law-before-2022-presidential-election/ (Fecha de consulta: 07/01/2021).

NORMATIVA, JURISPRUDENCIA Y OTRA DOCUMENTACIÓN

Article 29 Data Protection Working Party, "*Adequacy Referential (WP 254 rev.01)"*, 2018, en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, 28 de enero de 1981 (también su protocolo adicional C108+).

Maximillian Schrems c. Data Protection Commissioner. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 6 de octubre de 2015. Asunto C-362/14. ECLI:EU:C:2015:650.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (CEPD), "*Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)"*, en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf (Fecha de consulta: 04/03/2021).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE, Diario Oficial de la Unión Europea, serie L, Nº 119, 2016.

CoE, "*TRADUCCIÓN N° 058/2019 - Informe Explicativo de Convenio*" en https://rm.coe.int/informe-explicativo-de-convenio/1680968479 (Fecha de Consulta: 13/03/2021).

WEBINAR

CONSEJO DE EUROPA , *"Data Privacy Day 2021: Asia Pacific Region event 40th Anniversary of data protection Convention 108*", 2021, en https://www.coe.int/en/web/data-protection/dpd2021-asia-pacific-region-event

CONSEJO DE EUROPA , "*Data Protection Day 2021 in Latin-America 40th Anniversary of data protection Convention 108*", 2021, en https://www.coe.int/en/web/data-protection/dpd2021-in-latin-america

CONSEJO DE EUROPA, *"Conference on "Transborder transfers - Challenges of international data transfer from the perspective of the Convention 108+ and GDPR",* 2021, en https://www.bmi.bund.de/SharedDocs/videos/EN/european-data-protection-day.html

CONSEJO DE EUROPA, *"Data Protection Day 2021 in Africa 40th Anniversary of data protection Convention 108*", 2021, en https://www.coe.int/en/web/data-protection/dpd2021-african-region-event

STOCKHOLM INSTITUTE OF TRANSITION ECONOMICS & MISTRA CENTER FOR SUSTAINABLE MARKETS, *"Economic reforms of fragile states – Perspectives from Somalia",* 2020, en https://www.hhs.se/en/about-us/calendar/misum-events/2020/the-role-of-partnerships-in-economic-reforms-of-fragile-states/

PETICIONES DE INFORMACIÓN PÚBLICA

Destinatario: Consejo de Europa.

Objeto: Contactamos con la Unidad de Protección de Datos del Consejo de Europa para solicitar su valoración acerca de la tendencia de los países en desarrollo de inspirar sus legislaciones de protección de datos en el modelo europeo. También se pidió información sobre la existencia de programas de apoyo y asistencia que tuviesen con estas naciones en el ámbito de este derecho fundamental.

Destinatario: Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD).

Objeto: Dado que los objetivos de la organización son maximizar las oportunidades comerciales y de inversión de los países en vías de desarrollo, solicitamos su opinión respecto a las reformas que estaban teniendo lugar en materia de protección de datos en países considerados subdesarrollados. En concreto, sobre las posibilidades de obtener una decisión de adecuación positiva por parte de la UE.

Destinatario: Delegación de la Unión Europea en Kenia.

Objeto: Contactamos con el Jefe de Gobernanza y Macroeconomía, Alexandre Baron, para solicitar su valoración de la ley que el país africano desarrolló recientemente, inspirada en el RGPD. También se preguntó acerca del interés de Europa en este tipo de iniciativas, con tal de valorar si habría apoyo por parte de la UE para continuar con las reformas y conversaciones pertinentes.