La Visión de América Latina sobre el Reglamento General de Protección de Datos

*Luis Enríquez Álvarez**

Resumen

A partir de la entrada en aplicación del Reglamento General de Protección de Datos de la Unión Europea (RGPD) el 25 de mayo de 2018, casi todos los países latinoamericanos entraron en un proceso de reforma o de creación de nuevas leyes de protección de datos que cumplan con las exigencias del RGPD. La necesidad de cumplir con este nuevo estándar jurídico es indispensable en vista de los procesos de integración y acuerdos de libre comercio que mantienen ambas regiones. Los países de Latinoamérica han seguido casi en su totalidad la visión europea sobre la protección de datos personales, en contraste con otras potencias mundiales con estándares mucho más bajos de protección de la vida privada. Esta influencia de la Unión Europea en Latinoamérica hace que en la actualidad sea indispensable la cooperación entre ambas regiones, para así lograr una alianza estratégica para la transición hacia la cuarta revolución industrial.

Palabras clave: RGPD, protección de datos, gestión de riesgos, vida privada, tecnología, derechos.

Latin America view on the General Data Protection Regulation

Abstract

Since of the EU General Data Protection Regulation (GDPR) was put in practice on May 25, 2018, most Latin American countries started into a process to reform and create new data protection laws that meet the requirements of the GDPR. However, there are some big challenges considering the technical nature of the GDPR based on a risk-based approach and impact assessments. The need to comply with the new GDPR is essential due to the integration processes and trade agreements between both regions. Most Latin American countries have followed the European vision on the protection of personal data, in contrast to other world powers with lower privacy protection standards. This influence of the European Union in Latin America means that cooperation between the two regions is a must and it will help us to achieve a strategic alliance towards the fourth industrial revolution.

Keywords: GDPR; data protection; risk assessment; privacy; technology; law; freedoms.

---

* Profesor, Universidad de Lille y la Foundation pour le Droit Continental, Francia. ‹luis.enriquez@univ-lille.fr›.

Recibido: 19 de junio de 2019 | **Revisado**: 25 de junio de 2019 | **Aceptado**: 6 dejunio de 2020
Para citar este artículo: Enríquez Álvarez, Luis. "La Visión de América Latina sobre el Reglamento General de Protección de Datos". *Comentario Internacional*, n.º 19 (2019): 99-112.
doi: 10.32719/26312549.2019.19.4

Visión comparativa entre la Unión Europea y Latinoamérica

¡El Reglamento General de Protección de datos[1] (RGPD) cambió al mundo! es un decir popular en la actualidad. La verdad es que el RGPD responde a una larga evolución sobre la protección de datos personales en la Unión Europea de más de 40 años, que ha influenciado en otras regiones del mundo, entre ellas Latinoamérica. La aplicación directa del RGPD y su alcance extraterritorial hacen que instituciones públicas y privadas de todo el mundo deban cumplir con las obligaciones en el establecidas, incluidas las latinoamericanas. Pero ¿Cuáles son las innovaciones y cambios establecidos en el RGPD? ¿Qué sucede en Latinoamérica en cuanto a la protección de datos personales? ¿Existen los mecanismos y recursos necesarios para esta transición? ¿Cómo afecta a las leyes latinoamericanas de protección de datos de la era pre-RGPD? ¿Qué estrategias son necesarias para que la Unión Europea y Latinoamérica se conviertan en aliados estratégicos en la protección de datos personales? ¿Cómo impulsar estrategias comunes?

Latinoamérica y el Caribe tienen en conjunto una población aproximada de 670 millones de habitantes distribuidos en 46 países. Varios de ellos como Argentina,[2] Uruguay,[3] México,[4] Perú,[5] Colombia[6] (entre otros) desarrollaron sus leyes de protección de datos personales a partir de los años 2000. Estas leyes fueron muy influenciadas por la visión sobre el derecho a la vida privada de la Unión Europea, plasmadas en la Directiva Europea 95/46/CE. Sin embargo, cabe resaltar que, de aquellos países latinoamericanos con leyes de protección de datos, solo dos eran considerados como países seguros para la transferencia de datos personales, Argentina y Uruguay.[7] Entre los países que no contaban con una ley de protección de datos personales en la época pre-RGPD estaban Ecuador, Venezuela, Bolivia y Brasil.

1. Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.
2. Argentina, *Ley de Protección de los Datos Personales* n.° 25.326, 4 de octubre del 2000.
3. Uruguay, *Ley de Protección de Datos Personales* n.° 18331, el 11 de agosto del 2008.
4. México, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, 5 de julio del 2000.
5. Perú, *Ley de Protección de Datos Personales* n.° 29733, 3 de Julio del 2011.
6. Colombia, Ley Estatutaria 1581, 18 de octubre del 2012.
7. Agencia Española de Protección de Datos, "Transferencias internacionales", *AEPD*, 30 de agosto de 2019.

La idea de crear el RGPD nace en enero del 2012 cuando la Comisión Europea propone una reforma a la Directiva 95/46/CE con dos objetivos:[8] Reforzar la protección del derecho a la protección de datos personales e impulsar la economía digital en la Unión Europea. Considerando los grandes cambios económicos, sociales y culturales que trajeron las tecnologías de la información a partir de 1995, resultó muy coherente el planteamiento. El mayor problema de la Directiva 95/46/CE era la falta de aplicación directa, lo cual conllevaba a una notoria falta de homogenización en las leyes de la Unión. No obstante, es interesante observar que países latinoamericanos como Colombia, promulgaron su ley de protección de datos justo en ese año, al mismo tiempo que la Unión Europea preparaba ya el camino hacia el RGPD.

Entre las implementaciones básicas del RGPD se encuentran las siguientes: 1. Protege los datos de personas físicas (art. 1.1);[9] 2. Se aplica para el tratamiento automatizado, parcialmente automatizado y no automatizado de datos personales (art. 2.1); 3. Establece un ámbito extraterritorial de aplicación (art. 3); 4. Crea el rol del Oficial de protección de datos (art. 37.9); 5. Establece medidas de seguridad en el tratamiento de datos (art. 32); 6. Establece el principio de protección de datos personales desde el diseño y por defecto (art. 25.1); 7. Establece el principio de minimización de datos (art. 5, c); 8. Derecho de acceso (art. 15); 9. Derecho de transparencia (art. 12); 10. Derecho de rectificación (art. 16); 11. Derecho al olvido (art. 17); 12. Derecho de limitación (art. 18); 13. Portabilidad de datos (art. 20); 14. Consentimiento expreso (art. 7.1); 15. Reglas de consentimiento para niños (art. 8); 16. Sanciones administrativas que llegan hasta el 2 o el 4 % del ejercicio económico anual de una empresa (art. 83); 17. Notificación obligatoria a la autoridad de protección de datos sobre incidentes de seguridad en un máximo de 72 horas (art. 33); 18. Comunicación a los interesados sobre violaciones de seguridad de datos (art. 34), entre otras.

A partir de la entrada en vigor del RGPD el 25 de mayo del 2016, casi todos los países latinoamericanos entraron en un proceso de reforma de sus leyes de protección de datos para conformarse con el RGPD. Curiosamen-

8. Comisión Europea, *Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos)*, 25 de enero de 2012.
9. Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*.

te, el primero en desarrollar una ley de protección de datos en sintonía con el RGPD fue Brasil, con la Ley General de Protección de Datos (LGPD).[10] Aquellos países que no tenían una normativa, como Ecuador o Paraguay, están en proceso de desarrollo y aprobación de sus leyes de protección de datos personales. Así, podemos ver que, a nivel regional, todos estos avances convierten a Latinoamérica en un aliado estratégico importante de la Unión Europea en esta área.

En el caso ecuatoriano, ha sido un largo proceso con varios proyectos fallidos.[11] Un análisis jurídico detallado delata que existen normas jurídicas dispersas en varios cuerpos legales e, incluso, la Constitución ecuatoriana. Estas normas intentaban regular la protección de datos personales, sin que siquiera exista en el ordenamiento jurídico una definición legal de datos personales. Sin embargo, cabe mencionar que el nuevo anteproyecto de ley ecuatoriana de protección de datos personales ha sido desarrollado en conformidad a el RGPD, lo cual es muy prometedor.

La gestión de riesgos y el derecho proactivo

El RGPD define a los datos personales de la siguiente manera:

> toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.[12]

Esta definición de datos personales nos da la pauta del enfoque técnico que asume el RGPD, que se fundamenta en la gestión de riesgos, un lenguaje universal utilizado en el sector de la seguridad de la información.

---

10. Brasil, *Lei Geral de Proteção de Dados* n.° 13.709, 14 de agosto de 2018.
11. Para mayor información sobre las falencias del anterior proyecto de ley de protección de datos en el Ecuador ver: Luis Enríquez, "Paradigmas de la protección de datos personales en Ecuador, Análisis del proyecto de Ley Orgánica de Protección de datos". *Foro* 27, n.° 1 (2017): 43-61.
12. Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, art. 4 num. 1.

La pregunta es ¿por qué una rama jurídica adoptó una naturaleza más bien técnica? La respuesta es la necesidad de generar mecanismos efectivos para su cumplimiento en el contexto transnacional de un mundo regido por las tecnologías de la información y comunicación.

La Directiva 95/46/CE introducía ya la noción de la gestión de riesgos, pero de una manera ligera.[13] El RGPD adopta el carácter proactivo del área de la seguridad de la información, constituyéndose en una valiosa normativa de derecho proactivo, desafiando la naturaleza tradicional reactiva del Derecho. El considerando 74 del RGPD establece:

> Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.[14]

Los principios de seguridad de protección en el tratamiento de datos establecidos son: confidencialidad, integridad, disponibilidad, resiliencia y trazabilidad. A continuación, presentamos una breve descripción de cada principio:[15]

Confidencialidad: Es la prevención del acceso, divulgación y uso no autorizado de los datos.
Integridad: Es la prevención de cambios no autorizados a los datos.
Disponibilidad: Consiste en garantizar el acceso a los datos.
Trazabilidad: Consiste en el registro de acciones efectuadas en el tratamiento de datos. Este registro se constituye en prueba para auditorías.
Resiliencia: Es la capacidad de un sistema informático para resistir ataques.

---

13. La Directiva 95/46/CE establece en su artículo 17 numeral 1: "Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados [...].". Esta disposición sugiere una gestión de riesgos y evaluación de impacto, sin mecanismos obligatorios, como lo establece el RGPD.
14. Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, considerando 74.
15. EC-Council, *EC-Council Certified Incident Handler Courseware*. (Consejo Unión Europea: 2015), 13.

Los tres primeros principios han sido y son la base de la gestión de riesgos de ciberseguridad. La resiliencia y trazabilidad son principios aparentemente nuevos, pero que en realidad han sido tradicionalmente sobreentendidos para los especialistas en ciberseguridad. El RGPD establece medidas preventivas de seguridad en su artículo 32 literales a y b:

> Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
> a) la seudonimización y el cifrado de datos personales;
> b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento [...].[16]

El más grande desafío de las leyes latinoamericanas en la actualidad es precisamente el enfoque de la gestión de riesgos, pues ha sido tradicionalmente aplicado por la gran mayoría de las empresas desde el punto de vista de la protección de sus propios activos patrimoniales y no desde el punto de vista de la protección de derechos y libertades. El RGDP establece que el responsable y el encargado del tratamiento de datos, son quienes deben tomar las medidas de seguridad pertinentes. Los responsables y encargados son casi siempre instituciones públicas o privadas.

Por ello, la comprensión del objeto de la gestión de riesgos es esencial y me aventuro a sostener que estamos muy lejos aún de digerirlo como sociedad. Si consideramos que una gran parte del sector productivo en la región son pequeñas y medianas empresas (Pymes), podemos comprender que muchas de ellas no tienen una infraestructura y recursos humanos que les permita implementar las medidas técnicas y organizacionales requeridas para cumplir con lo dispuesto en el RGPD, con una eficiente gestión de riesgos y evaluaciones de impacto.

La mejor forma de comprender lo que es una gestión de riesgos es a través de la analogía. La gestión de riesgos nace a partir de los años setenta y ochenta[17] enfocado a los riesgos financieros y los seguros. Los primeros

16. Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
17. Georges Dionne, "Risk Management: History, Definition and Critique", *Risk Management and Insurance Review* 16, n.° 2 (2013): 147-66.

modelos nacen en los años noventa siendo especialmente notorios el *Risk metrics* y el C*redit metrics*.[18] La gestión de riesgos de ciberseguridad nacen en los años noventa y, muy notoriamente, como consecuencia de los ataques informáticos, adquiriendo tres misiones fundamentales: comprender las capacidades y conocimientos de los atacantes, medir la eficacia de las herramientas de seguridad y comprender y medir las consecuencias de un ataque exitoso.

Uno de los grandes desafíos que asumió la Unión Europea ha sido justamente apostar a una normativa jurídica en concordancia con el estado actual y proyección a futuro de las tecnologías emergentes, que como consecuencia también está ayudando a evolucionar la industria de la ciberseguridad. El paradigma cambia justamente, cuando aplicamos la gestión de riesgos a los derechos y libertades. Si consideramos una rama afín de la seguridad de la información, como la seguridad ocupacional, podemos comprender que los modelos de gestión de riesgos son establecidos en función de precautelar ciertos derechos, como el uso de señales para advertir un riesgo de resbalarse en piso mojado, precautelando el derecho a la vida del interesado.

En la gestión de riesgos de ciberseguridad, la tendencia ha sido más bien considerar los datos personales como un activo más de la empresa, olvidando el derecho de protección a la vida privada del interesado. Es así como la industria de hoy se fundamenta en la explotación de datos, con diversos fines que pueden ser comerciales por parte de empresas, o de vigilancia por parte de Gobiernos. No olvidemos también que el insumo de la próxima cuarta revolución industrial es justamente los datos, pues son estos los que dinamizan la economía digital, siendo fundamentales para cualquier proceso de análisis de datos[19] y aprendizaje automático.[20]

---

18. Ibíd.
19. Es la ciencia que examina datos en bruto con el propósito de sacar conclusiones sobre la información. El análisis de datos se refiere también a las técnicas y procesos cualitativos y cuantitativos utilizados para mejorar la productividad y la ganancia de los negocios. Ver: ‹https://www.tecnologias-informacion.com/analisis.html›.
20. El aprendizaje automático es un tipo de inteligencia artificial (AI) que proporciona a las computadoras la capacidad de aprender, sin ser programadas explícitamente. El aprendizaje automático se centra en el desarrollo de programas informáticos que pueden cambiar cuando se exponen a nuevos datos. Ver: ‹https://searchdatacenter.techtarget.com/es/definicion/Aprendizaje-automatico-machine-learning›.

Solventando el cambio de paradigma

Ante esta situación, las políticas públicas de países de la Unión Europea apuntan a solucionar este paradigma. Es así como la *Comission Nationale de l'Informatique et des Libertés* (CNIL),[21] máxima autoridad de protección de datos francesa ha desarrollado herramientas métricas para medir riesgos e impactos en el tratamiento de datos personales. Entre estos aportes podemos citar las guías de la CNIL para la seguridad de datos personales,[22] y el desarrollo de software de código abierto de asistencia para la gestión de riesgos de derechos y libertades.[23] Así como la CNIL, autoridades de protección de datos de otros países europeos también se encuentran desarrollando herramientas y guías para ayudar a instituciones públicas y privadas a cumplir con el RGPD, lo cual es un ejemplo a seguir por parte de nuestra región y ratifica el compromiso que debe tener una autoridad para emprender una misión común con sus ciudadanos en favor de la protección de sus derechos. No obstante, considero que estas metodologías y herramientas de software están aún en una etapa de desarrollo, y en los próximos meses podremos observar importantes avances.

Otras empresas de software de gestión de riesgos también han implementado métodos para medir riesgos en función de los derechos y libertades de las personas físicas. En la actualidad hay muchas empresas que desarrollan software de gestión de riesgos, evaluaciones de impacto y herramientas de ciberseguridad, que también se encuentran actualizando sus metodologías con el fin de que sus productos sean una herramienta útil para los responsables y encargados del tratamiento de datos.[24] El rol de estas empresas es también fundamental, pues es su responsabilidad empresarial ponerse

21. Ver: ‹https://www.cnil.fr/›.
22. Las guías de la CNIL están desarrolladas a partir de guías y normas comunes en la gestión de riesgos de ciberseguridad, pero con un enfoque a la protección de derechos y libertades. Estas guías pueden ser descargadas desde CNIL. Ver: ‹https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf›.
23. El software Privacy Impact Assesstment (PIA) es de código abierto, y puede ser descargado desde el enlace: ‹https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment›.
24. En la siguiente lista podemos encontrar numerosas herramientas de software que pueden ayudar a cumplir con las obligaciones del RGPD: ‹https://www.capterra.com/gdpr-compliance-software/›.

al día con los requerimientos de seguridad de sus clientes. Así podemos constatar que el RGPD ha obligado a evolucionar también a la industria de la ciberseguridad, siendo el conocimiento y gestión de riesgos de derechos y libertades una de las áreas más demandadas a escala global.[25] Esta fusión entre la protección y la ciberseguridad trae como principal beneficio la de alcanzar un ciberespacio más seguro.

Ahora, si analizamos los resultados del RGPD en este año de aplicación, tenemos cifras bastante novedosas. Han sido reportados alrededor de 5 900 incidentes hasta febrero del 2019 en la Unión Europea.[26] Si bien este incremento responde también al aumento de dispositivos móviles y el apogeo del Internet de las cosas, no cabe duda de que la obligación de notificar a la autoridad ha surtido efectos positivos. Antes del RGPD, las empresas al estar enfocadas en sus propios activos mantenían una confidencialidad respecto a sus incidentes de seguridad, pues ellos pueden ocasionar impactos cualitativos de una empresa, como la falta de credibilidad y mala reputación ante sus clientes. Sin embargo, las instituciones públicas y privadas que no consideraban la seguridad y privacidad de sus clientes ahora están obligadas a mejorar sus procesos institucionales, capacitar de mejor manera a sus funcionarios y utilizar tecnología adecuada para mitigar los riesgos.

Con todas estas nuevas leyes alineadas con el RGPD, América Latina se enfrenta a una fase de ajustes incómodos. Si bien, en algunas áreas de la seguridad de la información, las empresas pueden tener varias dificultades para adaptar sus metodologías para cumplir con las disposiciones del RGPD, también estas pueden ser resueltas a través de programas de capacitación en miras a abordar de mejor manera esta transición. De un lado, podemos tomar como ejemplo la manera como los países de la Unión Europea también proveen de metodologías y hasta herramientas de software a sus instituciones con el fin de proteger derechos y libertades.

Sin embargo, desde otro punto de vista, tomando en cuenta la situación real de Latinoamérica, debemos tener en cuenta que una gran parte de los profesionales latinoamericanos de seguridad de la información han sido capacitados y certificados de acuerdo con las metodologías desarro-

25. La experticia en el RGPD es considerada la más importante en el 2019 para algunos sectores de la ciberseguridad con EC-Council. Ver EC-Council blog, "The hottest cybersecurity skills of 2019", 21 de marzo de 2019: ‹https://blog.eccouncil.org/the-hottest-cybersecurity-skills-of-2019/›.
26. DLA Piper, "DLA Piper GDPR data breach survey: February 2019", 20 de enero de 2020, párr. 1.

lladas en Estados Unidos, como las de EC-Council,[27] el instituto SANS[28] o el ISC2[29]. Del mismo modo, los estándares referentes a la seguridad de la información como la familia ISO/IEC 27000[30] mantienen un enfoque previo a la RGPD que, aunque es muy útil, puede tener actualizaciones en un futuro próximo. Por este motivo, la cooperación de la Unión Europea para desarrollar o adaptar metodologías de evaluación de riesgos basadas en el RGPD que sean adaptables a la ley de los países latinoamericanos es absolutamente necesaria. Además, los países latinoamericanos pueden aprovechar desde ya la experiencia europea en este año de aplicación del RGPD, que les permitan capacitar a sus profesionales, empresas y sobre todo generar conciencia en la población sobre la importancia de la protección de sus datos personales.

Considerando también que en América Latina no existe aún un proceso de integración jurídica en esta área, las disposiciones establecidas en el RGPD pueden tener muchas variantes. Los ejemplos incluyen el principio de protección de la privacidad desde el diseño y por defecto, las certificaciones, las notificaciones de violaciones de datos, el rol del Oficial de Protección de Datos o las sanciones administrativas por incumplimiento. Por ejemplo, en la nueva ley brasilera sobre protección de datos la multa puede ser de hasta el 2 % de la facturación[31] de una empresa en lugar del 4 % previsto en el RGPD. De la misma manera, en el nuevo anteproyecto de ley en Argentina, el consentimiento también puede ser tácito bajo ciertas circunstancias.[32]

Sin embargo, el panorama también es alentador. Si comparamos el desarrollo mundial de la economía digital, encontramos tres grandes protagonistas: Estados Unidos de América, China y la Unión Europea en conjunto. Considerando que Estados Unidos y China son países con estándares mucho más bajos de protección de datos personales, la Unión Europa a través del RGPD juega un rol fundamental para regular tecnologías emer-

27. International Council of Electronic Commerce Consultants. Ver: ‹https://www.eccouncil.org/›.
28. SysAdmin Audit, Network and Security Institute. Ver: ‹https://www.sans.org/›.
29. International Information Systems Security Certification Consortium. Ver: ‹https://www.isc2.org/›.
30. Algunos estándares tales como el ISO /IEC 27005: 2018 han sido actualizados después de la entrada en vigor del RGPD. Ver, International Organization for Standardization: ‹https://www.iso.org/isoiec-27001-information-security.html›.
31. Brasil, *Lei Geral de Proteção de Dados* n.° 13.709, art. 52 num. 2.
32. Argentina, *Ley de Protección de los Datos Personales* n.° 25.326, art. 12 num. 2.

gentes como la inteligencia artificial, la biotecnología, *blockchain* y hasta la computación cuántica. La RGPD se ha convertido en un estándar que ha puesto un freno a las violaciones al derecho a la vida privada por parte de grandes empresas de estos países como *Google*, *Facebook*, *Alibaba*, entre muchas otras. Podemos ver como la obligación de notificar y comunicar incidentes establecidos en el RGPD ha contribuido al aumento de reporte de incidentes en el último año. La consecuencia de la gestión de riesgos enfocada a derechos y libertades es tener un mercado digital más seguro.

Resulta interesante, por ejemplo, analizar las declaraciones de Tim Cook, CEO de la empresa *Apple*, respecto a la necesidad de crear un RGPD en los Estados Unidos de América:

> Las plataformas y los algoritmos que prometieron mejorar nuestras vidas pueden en realidad magnificar nuestras peores tendencias humanas, los actores malintencionados e incluso los gobiernos se han aprovechado de la confianza del usuario para profundizar las divisiones, incitar a la violencia e incluso socavar nuestro sentido compartido de lo que es verdadero y lo que es falso. Esta crisis es real. No es imaginada, exagerada o loca […]. Es hora de que el resto del mundo... siga su ejemplo. En Apple respaldamos plenamente una ley federal de privacidad integral en los Estados Unidos [...].[33]

Desde esta perspectiva, resulta muy interesante ver que Latinoamérica ha ganado tiempo, pues gracias a la influencia de la Unión Europea, cuenta y está en proceso de desarrollar leyes de protección de datos más avanzadas que Estados Unidos. El RGPD se está convirtiendo en un estándar mundial, y en las condiciones actuales, se constituye en el catalizador que regula el derecho a la privacidad de los ciudadanos del mundo entero en el ciberespacio.

Conclusión

En conclusión, cabe señalar que la Unión Europea ha sido un importante inversionista en América Latina y el Caribe en los últimos años, re-

33. Rachel England, "Tim Cook calls for GDPR-style privacy laws in the US", *Engadget*, 24 de octubre de 2018.

presentando alrededor del 39 % de la nueva inversión extranjera directa[34] y alrededor de 26 acuerdos de libre comercio. Por lo tanto, no es una coincidencia que los países latinoamericanos hayan optado por seguir el modelo europeo de protección de datos personales. Considerando que el RGPD se ha convertido en el estándar mundial para frenar la invasión al derecho a la vida privada por parte de corporaciones y Gobiernos, América Latina ha dado ya grandes y firmes avances para alinearse con la normativa de la Unión Europea. Esta sincronía sin duda trae grandes pasos también en función del desarrollo del comercio internacional en un área tan crucial como los mercados digitales.

Sin duda, ha llegado el momento de acciones concretas entre América Latina y la Unión Europea en materia de protección de datos personales. Pero es necesaria la cooperación de todos, especialmente considerando el desfase de reflexión tecnológica que tienen los países de Latinoamérica con relación a los países de la Unión Europea. Latinoamérica tiene muchos usuarios digitales (pero lamentablemente poca comprensión del contexto social de ellas) y una economía que sigue mayoritariamente basándose en la exportación de materias primas. Por ello, es necesario comprender que en esta transición hacia la industria 4.0, no se trata de únicamente de promover conocimientos técnicos sino, sobre todo, que las mentes más brillantes de las Ciencias Sociales comprendan que este nuevo orden mundial debe ser diseñado y regulado desde este campo.

La Unión Europea ha dado grandes saltos en temáticas de tecnologías emergentes tales como la protección de datos personales, la ciberseguridad, *blockchain*, la biotecnología y la inteligencia artificial. He ahí la diferencia entre la Unión Europea y otras potencias mundiales. El desarrollo no solo puede ser concebido desde los ámbitos tecnológicos y económicos, sino sobre todo, desde el desarrollo integral de una sociedad.

34. CEPAL, *La Unión Europea y América Latina y el Caribe: estrategias convergentes y sostenibles ante la coyuntura global* (Santiago: CEPAL, 2018), 100.

Bibliografía

Argentina, "Proyecto de Ley de Protección de Datos Personales primera versión", *Senado y Cámara de Diputados de la Nación Argentina*, 2018. ‹https://www.argentina.gob.ar/sites/default/files/anteproyecto_de_ley_de_proteccion_de_los_datos_personales.pdf ›.

Argentina. *Ley de Protección de los Datos Personales* n.° 25.326, 4 de octubre de 2000.

Agencia Española de Protección de Datos. "Transferencias internacionales". *AEPD*. 30 de agosto de 2019. ‹https://bit.ly/2Xsswj0›.

Antonini Pascal, Bernard Duverneuil y Bertrand Diard. "Enterprises: les clés d'une application réussie du GDPR". *CIGREF, AFAI et TECH in France*. 14 de noviembre de 2017. ‹https://bit.ly/2K5GEXA›.

Banck, Aurélie. RGPD: *La protection des données à caractère personnel*. Francia: Gualino, 2018.

Bennani Younés. "Apprentissage par réseaux de neurones artificiels". *EPAT, France*. 6 de junio de 2014.

Brasil. *Lei Geral de Proteção de Dados* n.° 13.709, 14 de agosto de 2018.

CEPAL. *La Unión Europea y América Latina y el Caribe: Estrategias convergentes y sostenibles ante la coyuntura global*. Santiago: CEPAL, 2018.

Cichonsky Paul, Tom Millar, Tim Grance y Karen Scarfone. "Computer Security Incident Handling Guide". *National Institute of Standards Technology, Special Publication Revision* 2, n.° 800-61 (2012). doi:10.6028/NIST.SP.800-61r2

Colombia. *Ley Estatutaria* 1581, 18 de octubre de 2012.

Comisión Europea. *Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos)*, 25 de enero de 2012. https://bit.ly/2XlTg51

CNIL. "Security of Personal Data". *Commission Nationale de l´Informatique et des Libertés*, 2018.

CNIL. "Privacy Impact Assessment Methodology (PIA)". *Commission Nationale de l´Informatique et des Libertés*, 2018

Desgens-Pasanau, Guillaume. *La protection des données personnelles*. Francia: Lexis Nexis, 2019.

Dionne, Georges. "Risk Management: History, Definition and Critique". *Risk Management and Insurance Review* 16, n.° 2 (2013): 147-66. doi:10.2139/ssrn.2231635

DLA Piper. "DLA Piper GDPR data breach survey: February 2019". 20 de enero de 2020. ‹https://bit.ly/2Vi6Tzz›.

England, Rachel. "Tim Cook calls for GDPR-style privacy laws in the US". *Engadget*. 24 de octubre de 2018. ‹https://engt.co/2y3uMm9›.

Enríquez, Luis. "Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección de datos". *Foro* 27, n.° 1 (2017): 43-61.

Enríquez, Luis, Marcel Moritz, Valentin Gibello, Lorena Naranjo Godoy, Andrea Villalba Fiallos y Claudia Orellana Robalino. "La protección de datos personales en la era digital". *Foro* 27, n.° 1 (2017).

Haas, Gérard. *Le RGPD expiqué à mon boss*. Francia: Kawa, 2017.

Henry, Paul, Jacob Williams y Benjamin Wright. "The SANS Survey of Digital Forensics and Incident Response". *Tech. Rep*. 18 de julio de 2013.

Hildebrant, Mireille. "Data driven intelligence and Data Protection Law". *Global Privacy Assembly*. 17 de octubre de 2016.

Humphreys, Edward. *Implementing the ISO/IEC 27001 ISMS Standard*. Estados Unidos: Artech House Publishers, 2016.

Kriesel, David. *A Brief Introduction to Neural Networks*. Alemania: University of Bonn, 2005. ‹https://bit.ly/2RGioQb›.

Lawrence Öqvist y Filip Johnssén. *Hands-On Guide to GDPR Compliance: Privacy by Design, Privacy by Default*. Estados Unidos: IAPP, 2018.

México. *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, 5 de julio del 2000.

Parlamento Europeo. "Blockchain and the General Data Protection Regulation". *European Parliamentary Research Service, Scientific Foresight Unit (STOA)*. Julio de 2019.

Perú. *Ley de Protección de Datos Personales* n.° 29733, 3 de julio del 2011.

Salomon, David. *Foundations of Computer Security*. Reino Unido: Springer, 2006.

Smith, David. *Preparing for the data protection regulation*. Reino Unido: Allen & Overy, 2018.

Uruguay. *Ley de Protección de Datos Personales* n.°1833, 11 de agosto del 2008.

Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.