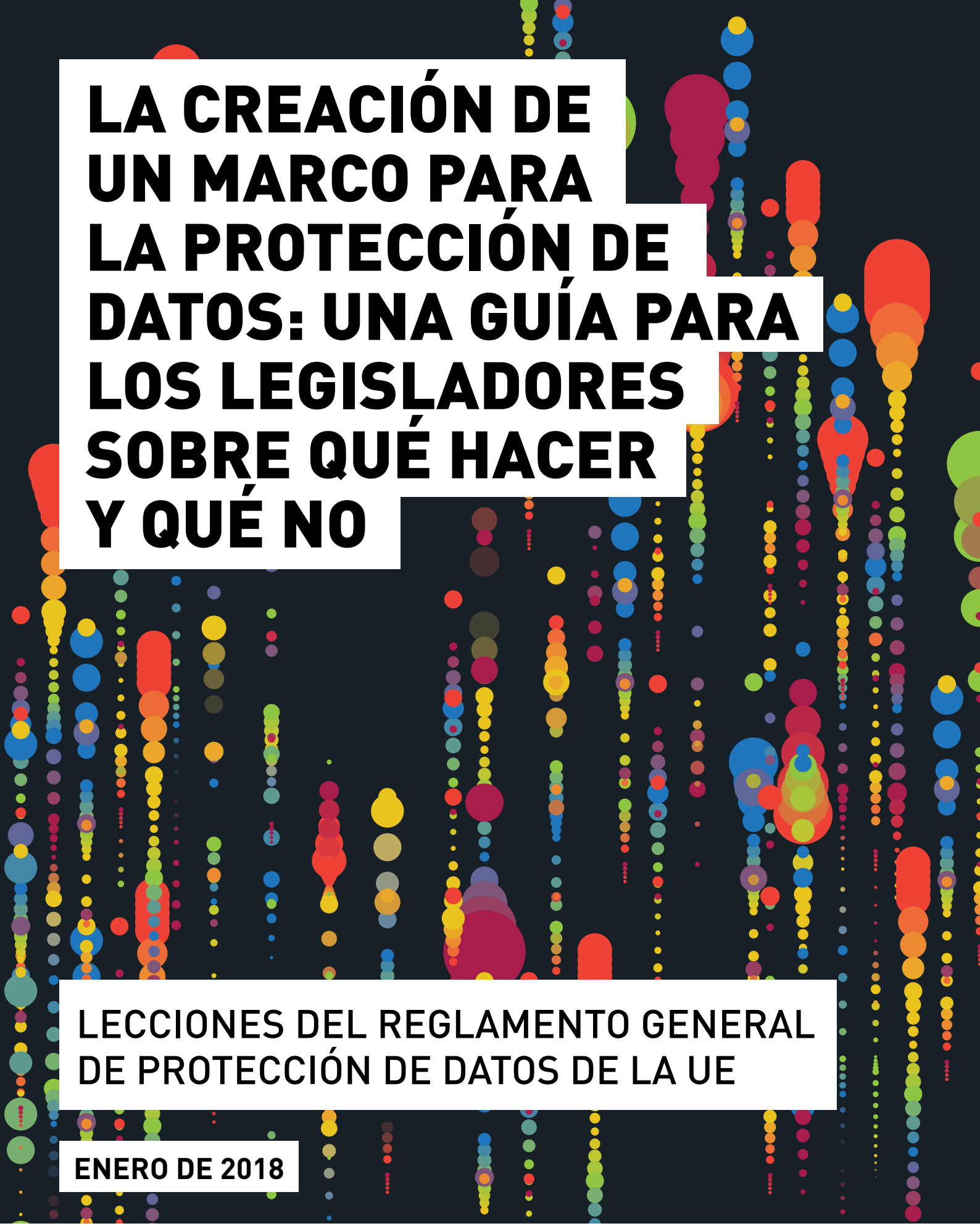


LA CREACIÓN DE UN MARCO PARA LA PROTECCIÓN DE DATOS: UNA GUÍA PARA LOS LEGISLADORES SOBRE QUÉ HACER Y QUÉ NO

LECCIONES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE

ENERO DE 2018

accessnow

accessnow.org

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación del apoyo técnico directo, el compromiso político integral, la defensa global, el otorgamiento de subvenciones para grupos locales emergentes, y las convocatorias como RightsCon, luchamos por los derechos humanos en la era digital.

Este documento es una publicación de Access Now.
Traducción: Justina Diaz Cornejo

Para más información, por favor visite: **https://www.accessnow.org**
Contáctenos: **Estelle Masse** | Senior Policy Analyst | **estelle@accesnow.org**

TABLA DE CONTENIDOS

INTRODUCCIÓN

Access Now presenta *La creación de un marco para la protección de datos: Una guía para los legisladores sobre qué hacer y qué no — Lecciones del Reglamento General de Protección de Datos de la UE* para contribuir al discurso mundial sobre la protección de datos. Este documento en particular propone una reflexión sobre el enfoque de la Unión Europea en cuanto al debate y el nivel de protección de datos personales alrededor del mundo.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea es un marco positivo para proteger a los usuarios y ayudarlos a retomar el control de su información personal. Si bien la ley está actualmente en proceso de implementación, ya ha inspirado a los gobiernos alrededor del mundo a actualizar o desarrollar la legislación relativa a la protección de datos, lo que conlleva enormes oportunidades. Hay importantes lecciones que aprender a partir de las negociaciones del RGPD, muchas de ellas son positivas y algunas, negativas.[1] Según nuestra experiencia, hemos creado una lista de qué se debe hacer y qué no, la cual debería ser tomada en cuenta por los legisladores al momento de desarrollar un marco de protección de datos.

CONTEXTO

¿Alguna vez ha declarado impuestos o realizado una llamada telefónica? ¿Posee un smartphone? ¿Alguna vez ha utilizado la Internet? ¿Tiene una cuenta en redes sociales o utiliza una aplicación para hacer ejercicio físico? Si la respuesta a cualquiera de estas preguntas es «sí», significa que ha estado compartiendo su información personal, ya sea en línea o no, con entidades privadas o públicas, incluso con algunas que quizás nunca haya oído nombrar. Compartir datos es una práctica habitual que se está volviendo cada vez más ubicua a medida que la sociedad se instala en la red. Compartir datos no solo es beneficioso para los usuarios, sino que a menudo es necesario para cumplir con responsabilidades administrativas o involucrarse en la sociedad de hoy en día. Pero esto conlleva riesgos. Nuestra información personal revela mucho sobre nosotros, nuestros pensamientos, y nuestra vida. Es por esto por lo que debemos protegerla.

El derecho a la protección de los datos personales está estrechamente relacionado con el derecho a la privacidad, pero es diferente.

Más de 160 países consagran el derecho a la privacidad en sus constituciones, pero el entendimiento de lo que implica la «privacidad» varía de un país a otro, en base a sus historias, culturas, o influencias filosóficas.[2] Esto explica por qué la manera en la que se protegen los datos difiere de un país a otro, incluso si muchas tradiciones jurídicas centran a la protección de la privacidad en el derecho al respeto de la vida privada y familiar, el hogar, y la correspondencia. La protección de datos, por otro lado, no siempre se considera un derecho en sí mismo. Los 28 estados miembros de la Unión Europea representan una excepción, ya que reconocieron la protección de datos como un derecho fundamental en la Carta de 2001 de la UE.[3] Sin embargo, la protección de datos personales es de una importancia primordial en nuestra sociedad, cada vez más digital. A menudo se la reconoce mediante marcos vinculantes a nivel nacional, regional, e internacional, y en muchos lugares en los que aún no está codificada, los legisladores están en proceso de hacerlo. Creemos que este proceso debería finalizarse con la mayor celeridad posible.

[1] Access Now, General Data Protection Regulation – what tidings do ye bring?
https://www.accessnow.org/general-data-protection-regulation-what-tidings-do-ye-bring/
[2] Vea los resultados provistos por el Constitute Project
https://www.constituteproject.org/search?lang=en&key=privacy
[3] Vea el Artículo 8 de la Carta de Derechos Fundamentales de la UE, 2001.
http://www.europarl.europa.eu/charter/pdf/text_en.pdf

La protección de datos personales, o de información personalmente identificable (IPI), implica establecer reglas que todas las entidades que procesen dicha información deberán cumplir. Este concepto no es nuevo, ya que la protección de datos ha estado vigente en muchos países del mundo por más de 40 años, pero estas leyes se están volviendo más importantes a medida que las personas comparten más datos y la recolección y uso de datos por parte de las compañías aumenta drásticamente. La primera ley de protección de datos fue aprobada en 1970 por el estado federado de Hesse, en Alemania.[4] Algunos años más tarde, los EE. UU. desarrollaron las «prácticas justas de información» que han influenciado las leyes de protección de datos modernas, aunque los EE. UU. no avanzaron hacia la codificación de un marco legal para la protección de datos, sino que adoptaron leyes en sectores específicos.[5] Luego llegaron las leyes de protección de datos a escala nacional, en Suecia, Alemania, y Francia, antes de que las organizaciones internacionales como el Consejo de Europa adoptaran los marcos internacionales. El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal — también conocido como Convenio 108— fue adoptado en 1980 y quedó abierto a la firma de los Estados Miembro en 1981.[6] En 1980, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) también elaboró sus directrices sobre la privacidad.[7] Desde su adopción, el Convenio 108 fue ratificado por los 47 países miembros del Consejo de Europa, y también por la República de Mauricio, Senegal, Uruguay, y recientemente, en 2017, por Túnez.[8] El Convenio 108 jugó un papel decisivo en la adopción de la primera ley europea de protección de datos en 1995.[9] Al día de hoy, cientos de países alrededor del mundo han adoptado leyes de protección de datos de manera sectorial o general.[10]

Además de los marcos vigentes, existen países que actualmente están considerando legislar en materia de protección de datos: Túnez, la India, Japón, Corea del Sur, Brasil, y Argentina, entre muchos otros.[11] Para algunos de estos países, esta sería la primera ley de protección de datos. Access Now trabaja en la legislación de la protección de datos en todo el mundo desde 2009, y particularmente en la reforma de la UE que llevó a la adopción del Reglamento General de Protección de Datos.[12] La UE y sus estados miembros cuentan con una larga tradición en la protección de datos, y a menudo es considerada el órgano normativo en esta área, lo que implica que muchos países están interesados en replicar el RGPD en sus propias jurisdicciones. Hay importantes lecciones que aprender a partir de las negociaciones del RGPD, muchas de ellas son positivas y algunas, negativas. Según nuestra experiencia, hemos creado una lista de qué se debe hacer y qué no, la cual debería ser tomada en cuenta por los legisladores de todo el mundo al momento de desarrollar un marco de protección de datos.

[4] Hessische Datenschutzgesetz, cuya versión original data del 7 de octubre de 1970. (GVBl. I S. 625).
[5] Vea EPIC, el código de prácticas Justas de la información. https://epic.org/privacy/consumer/code_fair_info.html
[6] Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de caracter personal, 1981. http://www.coe.int/web/conventions/full-list/-/conventions/treaty/108
[7] Vea Privacy International, Protección de datos. https://www.privacyinternational.org/node/44
[8] Access Now, Tunisia ratifies Convention 108 and affirms commitment to the protection of personal data https://www.accessnow.org/tunisia-ratifies-convention-108-affirms-commitment-protection-personal-data/
[9] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2015. https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf
[10] Vea Privacy International, Protección de datos. https://www.privacyinternational.org/node/44
[11] Autoridad nacional de Túnez para la protección de datos personales. Projet de loi relative à la protection des données personnelles, 2017. http://www.inpdp.nat.tn/Projet_PDP_2017.pdf
[12] Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

QUÉ HACER

En esta sección encontrará 10 recomendaciones para que sigan los responsables de formular políticas al momento de desarrollar la ley de protección de datos. Estos 10 pasos son necesarios, individual y colectivamente, para asegurar las negociaciones abiertas y la adopción de un marco centrado en el usuario.

1 GARANTIZAR NEGOCIACIONES TRANSPARENTES E INCLUSIVAS

Los gobiernos y los tomadores de decisiones deben garantizar que las negociaciones de los marcos de protección de datos se den de manera abierta, transparente, e inclusiva. Esto implica llevar a cabo consultas públicas y mesas redondas de expertos, publicar los textos de negociación y permitir comentarios de las partes interesadas con fechas límite razonables, y brindar una retroalimentación sobre los comentarios recibidos. En todas las etapas, debe asegurarse la participación significativa de los grupos de la sociedad civil, y todas las reuniones de los tomadores de decisiones con la industria, las ONG, y los grupos de consumidores deben hacerse públicas en un registro fácilmente accesible. El proceso debe estar acompañado por una máxima transparencia en relación con las gestiones. Las contribuciones de la sociedad civil deberán tener un peso razonable para compensar el desequilibrio inevitable con respecto al número de voces en comparación con la industria.

Experiencia de las negociaciones del RGPD

Las negociaciones del RGPD se llevaron a cabo en consonancia con el proceso legislativo de la UE. Este proceso es bastante transparente y, por lo general, asegura la publicación de proyectos de propuestas, opiniones, informes, modificaciones, y asesoramiento jurídico de todas las instituciones de la UE sobre cualquier acto legislativo en debate. Sin embargo, este proceso legislativo podría recibir algunas mejoras. En primer lugar, debería haber una mayor rendición de cuentas en las primeras etapas de elaboración de la legislación. Mediante una solicitud de acceso a la información, Access Now, por ejemplo, recibió un correo electrónico que revela cómo el departamento de Asuntos Internos de la Comisión Europea había estado trabajando a la par de la administración de los EE. UU. durante las primeras etapas del intento de reforma de la normativa sobre la privacidad.[13] Adicionalmente, el diálogo tripartito — la etapa final de las negociaciones entre todas las instituciones de la UE — carece marcadamente de transparencia. Access Now se unió hace años a los esfuerzos liderados por EDRi en el pedido de reformas al proceso.[14] Debido a la falta de transparencia durante esta etapa, el público queda a oscuras en el momento más importante de las negociaciones; es decir, el momento en el que los legisladores se reúnen para acordar en un texto de compromiso final que será vinculante tras el sellado de las instituciones de la UE.

Las partes interesadas externas que buscan influenciar las negociaciones también deben acatar los principios de transparencia y rendición de cuentas. Las negociaciones del RGPD estuvieron sometidas a esfuerzos de cabildeo sin precedentes en los que los representantes de la industria intentaron debilitar los estándares de protección de datos existentes y evitar que las propuestas fortalecieran los derechos de los usuarios. La influencia de ciertas industrias y compañías extranjeras se hizo visible gracias a que los legisladores copiaron y pegaron propuestas de modificación de las propuestas de cabildeo.[15] En esa instancia, los grupos de activistas fueron capaces de ayudar al público a comparar el lenguaje propuesto por los cabilderos con el del texto propuesto por los legisladores.[16] Este proceso permitió que el público realice comentarios pertinentes sobre estas propuestas y ayudó a luchar contra la influencia ejercida mediante negociaciones

[13] Access Now, Big brother's little helper inside the European Commission https://www.accessnow.org/big-brothers-little-helper-inside-the-european-commission/
[14] Access Now, EU "trilogues" consultation: A foot in the door for transparency https://www.accessnow.org/eu-trialogues-consultation-foot-door-transparency/
[15] Access Now, Privacy under siege: Unprecedented lobby efforts against the Regulation are revealed https://www.accessnow.org/privacy-under-siege-unprecedented-lobby-efforts-against-the-regulation-are/
[16] Vea la iniciativa de LobbyPlag http://lobbyplag.eu/compare/overview

secretas tras bastidores. Proponer modificaciones no es en sí una actividad dudosa, pero debe hacerse de una manera transparente. Las personas deben saber de dónde provienen estas propuestas y los cabilderos siempre deben indicar su afiliación en sus propuestas y ponerlas a disposición del público.

2 DEFINIR E INCLUIR EN LA LEY UNA LISTA DE PRINCIPIOS VINCULANTES PARA LA PROTECCIÓN DE DATOS

Cualquier marco dirigido a la protección de información personal debe incluir una clara definición de los datos personales y sensibles. El nivel de protección debe corresponderse con la sensibilidad de cada categoría de datos. Los datos sensibles deben estar definidos de manera que incluyan los datos genéticos y biométricos, así como también el contenido de las comunicaciones y los metadatos, debido a que esta información revela rasgos personales particularmente sensibles. Esto significa que un marco de protección de datos puede también incluir medidas específicas para la protección de datos intercambiados durante comunicaciones y disposiciones de privacidad relacionadas, para garantizar la confidencialidad de las comunicaciones.

Además de definiciones claras, los siguientes ocho principios se encuentran en el centro de los marcos de protección de datos.[17] En conjunto, estos principios interconectados establecen las medidas necesarias que debería incluir cualquier marco de protección de datos que busque proteger de manera efectiva los derechos de los usuarios. La codificación efectiva de estos principios exige el desarrollo de un conjunto de derechos de los usuarios, una base jurídica para el tratamiento de datos, medidas de seguridad de datos, mecanismos de supervisión, obligaciones para las entidades que procesen datos, y medidas que habiliten la transferencia de datos a países terceros.

1. **Lealtad y legalidad:** Los datos personales deben ser procesados de manera justa y legal, lo que implica que la información debe ser procesada en una base jurídica clara, con un propósito claro, y de una manera justa y transparente, para que los usuarios estén informados pertinentemente sobre cómo se recopilarán, usarán o almacenarán sus datos y quién lo hará.

2. **Limitación de la finalidad:** Los datos deberán ser recopilados y procesados solo para fines específicos y legítimos. El propósito debe ser específico, explícito, y de duración limitada. Los datos no deben ser procesados en una manera que sea incompatible con dicho propósito.

3. **Minimización de datos:** Los datos personales recopilados y utilizados deben limitarse a ser suficientes, pertinentes y no excesivos en relación con un propósito específico y definido.

4. **Exactitud:** Los datos personales deben ser precisos y, cuando corresponda, deben ser actualizados. Los usuarios deben tener el derecho a eliminar, rectificar, y corregir su información personal.

5. **Conservación limitada:** Los datos personales procesados por cualquier propósito no deben ser mantenidos por más tiempo del necesario.

6. **Derechos de los usuarios:** Los datos personales deberán ser procesados en consonancia con los derechos de los usuarios, como el derecho al acceso o el derecho a la supresión (vea el punto 4).

7. **Integridad y confidencialidad:** Los datos personales deben ser procesados de manera que se garantice una seguridad de vanguardia para los datos, junto con la protección contra tratamiento no autorizado o ilegítimo y contra la pérdida accidental, destrucción o daños de los datos, utilizando medidas técnicas y organizacionales pertinentes.

8. **Adecuación:** Los datos personales no deben ser transferidos a un país o territorio tercero, a menos que el país o territorio en cuestión garantice un nivel adecuado de protección para los derechos y libertades de los usuarios en relación con el procesamiento de datos personales. Los marcos de protección de datos deben brindar un mecanismo que habilite la libre circulación de datos entre países y garantice un alto nivel de protección de datos.

[17] Vea la Oficina del Comisionado de Información del Reino Unido, Principios de la Protección de Datos https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

Experiencia de las negociaciones del RGPD

Los ocho principios de la protección de datos provienen en gran medida de estándares internacionales, en particular, del Convenio 108 y de las directrices de la OCDE.[18] Estos principios de protección de datos se consideran «estándares mínimos» para la protección de derechos fundamentales para los países que han ratificado los marcos internacionales de protección de datos. Estos principios deben establecer las bases de cualquier marco de protección de datos y se encuentran en una gran cantidad de leyes de protección de datos alrededor del mundo, desde la Directiva de la Protección de Datos de la UE de 1995, y el RGPD, hasta la mayoría de las leyes de protección de datos vigentes en América Latina.

3 DEFINIR LAS BASES JURÍDICAS QUE AUTORIZAN EL PROCESAMIENTO DE DATOS

Toda ley de protección de datos debe definir de manera clara la base jurídica sobre la cual los datos personales de los usuarios pueden ser procesados. Toda entidad, pública o privada, que busque procesar datos personales debe acatar al menos una de las bases jurídicas provistas por ley. Generalmente, estas bases incluyen la celebración de un contrato, el cumplimiento de una obligación legal, y el consentimiento del usuario.

El consentimiento debe estar definido como un pedido activo, informado y explícito del usuario. Debe ser dado de manera libre y el usuario debe tener la capacidad de retirar el consentimiento en cualquier momento. Esto significa, por ejemplo, que las casillas pretildadas no califican como consentimiento válido. Asimismo, las compañías no pueden negar el acceso de los usuarios a un servicio por rehusarse a compartir más datos de los estrictamente necesarios para la funcionalidad de este. De otro modo, el consentimiento no sería dado libremente.

Experiencia de las negociaciones del RGPD

El RGPD contempla seis bases para el procesamiento de datos personales desde el contrato hasta el consentimiento.[19] La definición de consentimiento se fortaleció y aclaró durante las negociaciones en comparación con la definición recogida en su predecesora, la Directiva 95/46. El RGPD indica que el consentimiento debe ser un «claro acto afirmativo que establezca una indicación dada libremente, informada, y carente de ambigüedad» del usuario. Sin embargo, el RGPD también autoriza el procesamiento de datos para los llamados propósitos de «interés legítimo», definidos por la entidad que utiliza la información. Esta disposición limita gravemente el control de los usuarios sobre su información personal debido a que a menudo no son conscientes de las recopilaciones o procesamientos de datos cuando las entidades se valen del interés legítimo (vea más sobre el interés legítimo en el segundo punto de la sección «Qué no hacer»).

4 INCLUIR EN LA LEY UNA LISTA DE DERECHOS DE USUARIO VINCULANTES

Para proteger los datos de los usuarios y garantizar que tengan control sobre su información personal es necesario establecer una serie de derechos vinculantes que ellos puedan ejercer:

[18] Organización para la Cooperación y el Desarrollo Económicos, septiembre de 1980. Directrices que rigen la protección de la intimidad y los flujos transfronterizos de datos personales. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf
[19] Vea el Artículo 6. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

1. **El derecho de acceso** habilita a los usuarios a obtener confirmación de los servicios y compañías con respecto a la posible recopilación y procesamiento de datos personales que los conciernan. Si ese es el caso, los usuarios deben tener acceso a los datos, el propósito del procesamiento, y a quiénes los estén procesando, entre otras cosas.
2. **El derecho de oposición** habilita a los usuarios a rehusarse al procesamiento de su información personal cuando no hayan prestado su consentimiento al procesamiento de sus datos o no hayan firmado un contrato. El derecho de oposición aplica a los mecanismos de toma de decisiones automáticos, incluido el análisis de perfiles, ya que los usuarios tienen derecho a no ser sometidos al uso de estas técnicas.
3. **El derecho de supresión** permite que los usuarios soliciten la eliminación de todos los datos personales vinculados a ellos al momento en que dejan un servicio o aplicación.
4. **El derecho de rectificación** permite que los usuarios soliciten la modificación de información errónea que los concierna.
5. **El derecho a la información** garantiza que los usuarios reciban información clara y entendible por parte de las entidades que procesan sus datos, ya sea que estas entidades los recopilaron de manera directa o a través de terceros. Toda la información provista al usuario debe ser concisa, comprensible, y de fácil acceso, debiendo utilizar lenguaje simple y claro. Esta información debe incluir detalles sobre los datos que están siendo procesados, el propósito por el que se los procesa, y la duración de su almacenamiento, cuando corresponda. Las entidades deben brindar su información de contacto y una dirección de correo electrónico a los usuarios para que estos puedan comunicarse con ellos en caso de que existan problemas.
6. **El derecho a la explicación** motiva a los usuarios a obtener información sobre la lógica que subyace en el tratamiento de datos personales automatizado y sus consecuencias. Este derecho es esencial para la rendición de cuentas y transparencia en el uso de algoritmos para tomar decisiones que tienen un impacto en la vida de los usuarios.
7. **El derecho a la portabilidad** permite que los usuarios movilicen ciertos datos personales que han compartido de una plataforma a otra que ofrezca servicios similares. Para facilitar este proceso, es necesario motivar la interoperabilidad entre los servicios.

Si bien esta lista no es exhaustiva, estos derechos deben estar previstos por ley, y no deben quedar librados a la discreción de las entidades que utilizan los datos. Los usuarios deben ser capaces de ejercer cualquiera de estos derechos sin cargo alguno.

Experiencia de las negociaciones del RGPD

El RGPD brinda a los usuarios todos estos derechos, sin cargo. Las disposiciones que consagran esos derechos establecen obligaciones detalladas para las entidades que procesan los datos para implementar, prever, proteger y respetar estos derechos.[20]

El RGPD es un paso importante para garantizar que los usuarios puedan ejercer su derecho de protección de datos libremente. No obstante, para asegurar que todas las medidas sean efectivas, es necesario que exista una mayor concientización sobre la existencia de la ley y su contenido. Los gobiernos, las autoridades públicas, las compañías y las ONG deberían trabajar en conjunto para lograr ese objetivo.

Finalmente, el ejercicio de ciertos derechos como el derecho a la portabilidad y el derecho a la explicación son especialmente relevantes en la era del big data y la inteligencia artificial. Sin embargo, la realización completa de estos derechos no podrá suceder sin la cooperación de las entidades privadas que desarrollan algoritmos, productos, y servicios. Debemos cerciorarnos de que los ingenieros creen las herramientas necesarias para habilitar la ejecución y el goce de estos derechos. A modo de ejemplo, el derecho a la portabilidad sería inútil si las plataformas no fueran interoperables.[21] En este sentido, el derecho a la explicación solo puede existir si los empleados de las compañías que dependen de algoritmos entienden perfectamente su funcionamiento, y si saben

[20] Vea el Capítulo 3. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[21] Grupo de trabajo sobre la protección de datos del Artículo 29, Directrices sobre el derecho a la portabilidad de los datos. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

por qué se utiliza un determinado algoritmo, qué datos se utilizan en ese algoritmo, qué datos crea el algoritmo, y qué variables utiliza el algoritmo para tomar una decisión. Dado que el RGPD posee un lenguaje limitado sobre ese derecho, muchos académicos están poniendo en tela de juicio hasta la existencia jurídica y la viabilidad de dicho derecho.[22] Queda claro que el RGPD pretendió crear esa posibilidad para los usuarios, pero será necesario obtener más guía por parte de las autoridades de protección de datos y las partes interesadas sobre cómo interpretar el texto en la práctica. En resumen, la creación de estos derechos es un hecho positivo, pero las condiciones para su ejercicio también deben desarrollarse en profundidad.

5 DEFINIR CLARAMENTE EL ALCANCE DE APLICACIÓN

Los derechos y principios establecidos en una ley de protección de datos que vela por la protección de los usuarios deberían ser aplicados en todo momento. Esto significa que, por ejemplo, si una entidad ofrece un servicio público o privado que implique el procesamiento de datos de usuarios en la UE, deberían aplicarse los derechos de usuario consagrados en la ley de la UE.

En la era digital, puede que sea difícil para los legisladores garantizar la suficiente protección de los datos personales y de los derechos de los usuarios sin aplicar el principio de extraterritorialidad. Para entender los beneficios de la extensión del alcance jurisdiccional de la protección de datos, necesitamos abordar la cuestión desde una perspectiva que no se base en el «establecimiento» (¿dónde se sitúa la entidad?), sino desde la perspectiva del usuario (¿dónde está el usuario y de dónde es?). El objetivo de la normativa de los derechos humanos, como los marcos de protección de datos, es, ante todo, proteger a los individuos en todo momento. Por lo tanto, es lógico garantizar que los usuarios sean respetados sin importar dónde están ubicadas las entidades que utilizan los datos de las personas.

Esta aplicación del alcance territorial también tiene el potencial de aumentar el nivel de protección para los usuarios a escala mundial si las compañías y las autoridades comienzan a implementar medidas de protección de datos y privacidad en sus prácticas diarias en todo el mundo. En lo que respecta a la competencia, estas medidas jurisdiccionales pueden evitar una espiral descendente en términos de protección, por la cual ciertas industrias decidirían reubicar sus compañías fuera de un país para evitar la aplicación de medidas que protejan al usuario.

Cabe notar, sin embargo, que extender el alcance jurisdiccional de un instrumento legislativo no viene sin riesgos, y debería ser cuidadosamente debatido por los legisladores. Pueden surgir conflictos entre legislaciones y ciertos estados podrían intentar extender el alcance de medidas que dañen los derechos por fuera de sus fronteras, utilizando la misma jurisdicción. Asimismo, no todas las entidades que procesan datos en el mundo conocen las leyes específicas de otros países. Generalmente, no queda claro de quién es la obligación de informar a los negocios e individuos sobre sus respectivas obligaciones y derechos. Deberán organizarse campañas de concientización para asegurar que las entidades de todo el mundo conozcan sus obligaciones. Para que las leyes de protección de datos funcionen como es debido, es necesario que las autoridades públicas cuenten con las atribuciones y recursos para poder educar al público. La sociedad civil puede y debería cumplir un rol activo en el proceso, en especial para empoderar al público para hacer respetar sus derechos.

Extender el alcance jurisdiccional no es la panacea, y deberán establecerse criterios específicos en las leyes de protección de datos para limitar malas copias o consecuencias dañinas. Los legisladores deberían, por ejemplo, indicar claramente en qué casos la ley aplicaría fuera de sus fronteras, a qué actores específicamente, qué mecanismos de aplicación de la ley estarían vigentes, y brindar a los usuarios, las compañías, y las autoridades claras vías de reparación.

Finalmente, las obligaciones en la ley de protección de datos deben aplicar claramente tanto al sector privado como al sector público. Las autoridades públicas recopilan cada vez más la información de los individuos, obteniendo acceso a bases de datos del sector privado, o bien construyendo grandes bases de datos de datos personales. Este procesamiento debe estar sujeto a obligaciones claras para la protección de la información personal de los individuos, de la misma manera en que se regula el procesamiento llevado a cabo por entidades privadas.

[22] Sandra Wachter, Brent Mittelstadt y Luciano Floridi, Universidad de Oxford, Instituto de Internet de Oxford. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

El RGPD extiende el alcance territorial de la ley, en comparación con la Directiva de Protección de Datos de 1995. El RGPD aplica a todas las compañías y autoridades establecidas en la UE, pero también a las entidades establecidas fuera de la UE si están procesando información personal para la prestación de bienes o servicios a usuarios dentro de la Unión Europea o si están monitoreando el comportamiento de dichos usuarios.[23] Este importante cambio en el alcance de la aplicación de la ley refleja la evolución de la jurisprudencia de la UE. Durante muchos años, los tribunales de la UE lucharon contra grandes compañías tecnológicas que se rehusaban a cumplir con las leyes locales de protección de datos, en base a problemas de jurisdicción. Google y Facebook repetidas veces argumentaron que no están cubiertos por las leyes de protección de datos, por ejemplo, en España o Bélgica, debido a que no estaban formalmente establecidos en dichos países. Tomaron esta posición a pesar de que las compañías estaban minando y monetizando información personal de usuarios en estos países.[24] [25] Al extender el alcance territorial de aplicación, el RGPD buscó responder a estos vacíos legales en la protección de los usuarios y lograr una seguridad jurídica para los usuarios. Este cambio no se produce sin desafíos, ya que no queda claro cómo las autoridades de protección de datos de la UE serán capaces de llevar a cabo medidas de ejecución en relación con las entidades ubicadas fuera de la UE y, así, proteger los derechos como es debido.

Experiencia de las negociaciones del RGPD

6 CREAR MECANISMOS TRANSPARENTES Y VINCULANTES PARA LA TRANSFERENCIA SEGURA DE DATOS A PAÍSES TERCEROS

Los marcos de protección de datos están diseñados para garantizar la libre circulación de datos, estableciendo mecanismos para la transferencia de datos y salvaguardas para los derechos de los usuarios. Estos mecanismos deben estar sometidos a una supervisión estricta y transparente, e incluir medidas de reparación para garantizar que los derechos de los usuarios viajen junto con los datos.

Según el RGPD, la transferencia de datos transfronteriza fuera del Espacio Económico Europeo solo puede llevarse a cabo si la transferencia se realiza hacia un país al que se le ha concedido una situación de adecuación o cuando exista un mecanismo de transferencia legítimo.[26] El RGPD prevé más mecanismos para la transferencia que la Directiva de 1995 mediante códigos de conducta y esquemas de certificación. Este enfoque les confiere a las compañías una mayor flexibilidad. La supervisión y aplicación efectivas de estos mecanismos será primordial para garantizar que los derechos humanos queden protegidos tanto durante como después de la transferencia.

Con respecto a la adecuación, la Comisión Europea tiene el poder de determinar si un país tercero garantiza un nivel adecuado de protección en su derecho nacional o en

Experiencia de las negociaciones del RGPD

[23] Vea el Artículo 3. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[24] Tribunal de Justicia de la Unión Europea, Sentencia dictada en el Asunto C-131/12, Google Spain SL vs Mario Costeja González, 13 de mayo de 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de249578524881c67efe5ec.e34KaxiLc3eQc40LaxqMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=574499
[25] Reuters, Facebook wins privacy case against Belgian data protection authority, junio de 2016. https://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV
[26] Vea el Capítulo 5. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

compromisos internacionales de los que es parte, lo que permitiría que los datos sean exportados a esa jurisdicción. Cualquier país puede postularse para una decisión de adecuación, que lanzará un proceso de revisión llevado a cabo a discreción de la Comisión de la UE. Actualmente, la Unión Europea ha concedido la adecuación a los siguientes países[27]: Andorra, Argentina, Canadá, Suiza, las islas Feroe, Guernsey, el Estado de Israel, la Isla de Man, Jersey, Nueva Zelanda, los Estados Unidos de América, y la República Oriental del Uruguay. La adhesión al Convenio 108 del Consejo de Europa es de especial importancia en este sentido, y es uno de los elementos que se tienen en cuenta al momento de evaluar la concesión de la adecuación.

En 2016, se anuló el acuerdo conocido como Safe Harbour sobre el que estaba basada basada la determinación de la adecuación de los EE. UU., debido a la falta de cumplimiento de la legislación de derechos fundamentales de la UE.[28] La validez de varios elementos de este nuevo acuerdo (llamado EU-US Privacy Shield) continúa bajo escrutinio.[29] Otros países como Australia han solicitado una decisión de adecuación pero, hasta el momento, no han logrado cumplir con los requisitos necesarios.[30] Finalmente, se están llevando a cabo las negociaciones para la revisión y la nueva adecuación con Japón.[31]

7 PROTEGER LA SEGURIDAD Y LA INTEGRIDAD DE LOS DATOS

Para gozar de los beneficios de la economía digital, es necesario que los usuarios puedan confiar en los servicios que usan en línea. Cualquier dato compartido genera un riesgo. Por lo tanto, es cada vez más importante garantizar que la privacidad y la protección de datos sean tomadas en cuenta por los ingenieros en la fase de diseño de productos y servicios, y que estén configurados en el nivel de protección más alto por defecto: este es el concepto de protección de datos por diseño y por defecto. Estas nociones deben estar detalladas en la ley para solicitar que las entidades las adopten.

Experiencia de las negociaciones del RGPD

El RGPD codifica los principios de protección de datos por diseño y por defecto, lo que trae aparejado un gran número de beneficios, como la contribución a la seguridad y la integridad de los datos.[32] Con la privacidad y la protección de datos por diseño y por defecto, las compañías toman una postura positiva para proteger los derechos de los usuarios, ya que se incorporan principios que protegen la privacidad tanto en las políticas tecnológicas como en las organizacionales. La privacidad y la protección de datos se vuelven parte de la cultura y el marco de la rendición de cuentas de la compañía, en

[27] Comisión de la UE, Decisiones de adecuación de la Comisión sobre la protección de datos personales en terceros países http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[28] Access Now, CJEU declares Safe Harbor invalid https://www.accessnow.org/cjeu-declares-safe-harbour-invalid/
[29] Access Now, Comments to EU Commission on Privacy Shield review https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf
[30] Comisión Europea, Estudio comparativo sobre diferentes enfoques de nuevos desafíos de privacidad, en particular a la luz de los desarrollos tecnológicos http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b2_australia.pdf
[31] Comisión Europea, Joint statement by Vice-President Andrus Ansip and Commissioner Věra Jourová on the dialogue on data protection and data flows with Japan, marzo de 2017. http://europa.eu/rapid/press-release_STATEMENT-17-690_en.htm
[32] Vea el Artículo 25. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

lugar de ser un «simple» elemento de cumplimiento. Esto requiere pensar sobre la privacidad y la protección de datos desde el comienzo del proceso de desarrollo de un producto o servicio.[33] Este enfoque puede ayudar a que las compañías ahorren en costos de desarrollo de productos o servicios. Gracias a que los ingenieros y equipos de desarrollo deberán haber tenido en cuenta la privacidad y la protección de datos desde el comienzo de la fase de desarrollo, habría que hacer menos ajustes luego de que el equipo de asesores jurídicos revise el producto. También reduce el riesgo a que la compañía reciba denuncias por violaciones de privacidad o sufra un daño en su reputación por filtración de datos, ya que será capaz de demostrar su compromiso con los derechos de los usuarios. En resumen, pasar de entender la privacidad y la protección de datos como una cuestión de cumplimiento a incorporar privacidad y protección de datos por diseño y por defecto puede ayudar a que las compañías aumenten la confianza en sus servicios.

8 DESARROLLAR MECANISMOS DE NOTIFICACIÓN Y DE PREVENCIÓN DE VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS

A pesar de que los marcos de protección de datos deberían impulsar medidas que promuevan la seguridad y la integridad de los datos, las violaciones de datos pueden, aun así, suceder. Por lo tanto, deberán existir medidas de solución, reparación, y notificación al usuario por tales problemas. Las violaciones de datos han recibido una atención generalizada debido a que negocios de todos los tamaños están dependiendo cada vez más en la computación en la nube y los servicios en línea. Debido a que los datos personales y sensibles se encuentran almacenados en dispositivos locales y servidores en la nube, la violación de la seguridad de la red y la información se ha hecho más atractiva para aquellos que intentan exponer o explotar información privada o pedir un rescate. Las violaciones de datos suceden desde que existe la preservación y el almacenamiento de los registros privados de los individuos. Antes de la era digital, una violación de datos podía ser algo tan simple como ver el archivo de un individuo sin autorización, o encontrar documentos que no habían sido descartados de manera correcta.[34] Con la digitalización de los registros y la creciente recopilación de datos personales, la magnitud de las violaciones de datos ha aumentado drásticamente, poniendo en mayor riesgo la información personal de los usuarios.

Para prevenir y mitigar estos riesgos, deben desarrollarse mecanismos para la notificación y prevención de tales violaciones, ya sea dentro del marco de protección de datos o en legislación complementaria. Los incidentes de más resonancia en relación con la pérdida o el robo de datos en todo el mundo impulsaron un amplio debate sobre el nivel de seguridad concedido a la información personal compartida, procesada, almacenada y transmitida electrónicamente. En este sentido, ganar y mantener la confianza de los usuarios en que sus datos están seguros y protegidos representa un desafío clave para las organizaciones. La ONG Privacy Rights Clearinghouse registró 7.619 violaciones de datos que se hicieron públicos a partir de 2005 solamente en los EE. UU.[35] Esto significa que por lo menos 926.686.928 registro privados han sido violados en los EE. UU. desde entonces. IBM y Ponemon Institute informan que en 2017 el costo promedio mundial de una violación de datos fue de $ 3,62 millones de dólares.[36] Aunque este costo se redujo un poco en comparación con el año anterior, el estudio muestra que las compañías están sufriendo violaciones más grandes. Otros estudios estiman que el costo promedio de una violación de datos excederá los $150 millones de dólares en 2020, con una estimación de costo anual de $2,1 billones.[37] Esto significa que prevenir y mitigar las violaciones de datos no solo es beneficioso para los usuarios, sino que también lo es para los negocios, ya que se ahorrarían gastos.

[33] Para más información sobre la Privacidad por Diseño, vea Ann Cavoukian, Privacy by Design, the 7 Foundational Principles https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
[34] Nate Lord, The history of data breaches, julio de 2017. https://digitalguardian.com/blog/history-data-breaches
[35] Privacy Rights Clearinghouse, Data Breaches. https://www.privacyrights.org/data-breaches
[36] Ponemon Institute for IBM, 2017 Cost of Data Breach Study: Global Overview https://www.ibm.com/security/data-breach/
[37] The Experian, Data Breach Industry Forecast, 2015. https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf

Experiencia de las negociaciones del RGPD

Los requisitos de notificación de violación de datos fueron incorporados a la Unión Europea para el sector de comunicaciones electrónicas en 2002.[38] Se desarrollaron reglas más específicas por sector desde ese momento, hasta que las medidas se armonicen bajo el RGPD para facilitar el cumplimiento de las organizaciones.

Las medidas adoptadas por el RGPD exigen que una organización informe sobre una violación de datos «sin dilación indebida» y, de ser factible, dentro de las 72 de haberse notado el incidente.[39] A pesar de que queda claro que el objetivo de la medida es asegurar que las violaciones de datos se reporten tan pronto como sea posible, el lenguaje es impreciso. El RGPD luego describe los pasos que debe seguir cualquier organización que se enfrenta a una violación y prevé la posibilidad de notificar a los usuarios. Dichas notificaciones son positivas desde el punto de vista de la rendición de cuentas y la transparencia, y también son esenciales para asegurar que los usuarios puedan tomar las acciones correspondientes para proteger su información y obtener resarcimiento cuando sea necesario. Sin embargo, el RGPD deja en manos de las organizaciones decidir si se notifica a los usuarios sobre una violación en base a su propia evaluación de riesgos de los derechos y libertades de los usuarios. La notificación a los usuarios debería ser un requisito para cualquier violación de datos personales, lo que incluye no solo información de subscripción, sino también otros datos personales, como fotografías. La notificación debe ser oportuna, fácil de comprender, y exhaustiva, y las opciones de resarcimiento deben ser claramente indicadas y accesibles. Al dejar mucho a discreción de las organizaciones, esta disposición se queda corta en el empoderamiento de los usuarios para que ellos tomen control de su información. Las organizaciones que sufren una violación de datos tienen un obvio interés económico en restar importancia a los riesgos asociados con el incidente y que no se notifique a los usuarios, lo que puede resultar en violaciones de protección de datos sin resolver. Instamos a los legisladores de todo el mundo a evitar estos inconvenientes y a desarrollar claros mecanismos de prevención y notificación de violación de datos.

9 ESTABLECER AUTORIDADES INDEPENDIENTES Y MECANISMOS ROBUSTOS DE APLICACIÓN

Ningún marco de protección de datos puede estar completo sin un mecanismo robusto de aplicación de la ley, que incluye la creación de una autoridad de supervisión independiente (autoridad o comisión de protección de datos — DPA, por sus siglas en inglés —). Hasta la mejor ley de protección de datos del mundo sería deficiente si no existiera una autoridad que tenga los poderes y recursos para monitorear su implementación, llevar a cabo investigaciones, y sancionar a las entidades en caso de violaciones de protección de datos (repetidas, por negligencia o intencionales).

Las sanciones deberían ser proporcionadas a las violaciones y pueden darse en forma de notificaciones o hasta acciones legales. Las autoridades pueden, por ejemplo, solicitar que una compañía detenga ciertas prácticas que violan los derechos de protección de datos de los usuarios, como la falta de provisión de políticas de privacidad o la venta de información sensible de los usuarios sin su conocimiento o consentimiento.

Si bien es necesario que exista el pago de multas, las autoridades de protección de datos deben aplicar multas limitadas a las compañías, en especial a las pequeñas y medianas empresas, que no se involucran en un procesamiento de datos

[38] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
[39] Vea los Artículos 33 y 34. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

significativo, no tienen los medios para comprender sus obligaciones para respetar la ley de protección de datos, y han cometido errores por su ignorancia, y no tanto por malas intenciones. El gobierno debe también tener iniciativas de concientización para evitar situaciones en las que las compañías ignoren la existencia y relevancia de las leyes de protección de datos. Túnez, que se encuentra debatiendo su primera ley de protección de datos de su historia, está proponiendo un enfoque gradual e innovador con respecto a las sanciones, que incluye multas más altas en los casos de reincidencia.[40] Consecuentemente, si una compañía se encuentra culpable de cometer violaciones de protección de datos por las que ya ha sido sancionada, la multa que recibiría luego será mucho más elevada.

Las sanciones y multas, sin embargo, representan solo una pequeña parte del trabajo de las DPA. El rol de las autoridades de protección de datos es, por supuesto, hacer cumplir las leyes de protección de datos y supervisar, pero también deben asistir a las organizaciones en el cumplimiento de sus tareas. Esto implica que las compañías, las autoridades públicas, y las ONG deben trabajar en conjunto con las autoridades de protección de datos para entender las responsabilidades y obligaciones de cada uno. Las organizaciones no deben dudar en establecer contacto con sus DPA, ya que pueden brindarles recursos y materiales para ayudarlas a implementar la ley.

Por último, las DPA tienen el poder de impulsar investigaciones independientes en las organizaciones y tener audiencias presentadas por individuos u ONG. En ese sentido, las DPA actúan como guardianas de los derechos de los usuarios y pueden ayudar a proteger sus derechos fundamentales. No obstante, muchos de los usuarios alrededor del mundo desconocen la existencia de estas autoridades. Para proteger aún más los derechos de los usuarios, las ONG deberían estar empoderadas para representar a los usuarios y presentar, de manera independiente, casos ante las DPA o tribunales. Los gobiernos deben también promover el trabajo de las DPA, explicar sus roles, y brindarles un presupuesto adecuado para garantizar que cumplan con sus responsabilidades.

Experiencia de las negociaciones del RGPD

La Unión Europea y sus estados miembros han contado con leyes de protección de datos por casi 30 años. A pesar de esto, muchas compañías las ignoraban debido a la carencia de poderes de ejecución de las autoridades de protección de datos y las multas relativamente bajas (hasta €150.000).[41] Durante años, en Europa los asesores jurídicos a menudo recomendaban a las compañías que no cumplieran con la ley de protección de datos de la UE, ya que el riesgo de recibir una multa era tan bajo como el precio que tendrían que pagar.[42] Este flagrante incumplimiento de los derechos fundamentales fue abordado por el RGPD mediante el aumento de multas hasta un máximo del 4% de los ingresos mundiales de la compañía.[43] Los poderes de aplicación y el funcionamiento de las DPA también se aclararon y armonizaron. Las DPA ahora se reunirán en una Junta Europea de Protección de Datos, que les permite, por ejemplo, realizar investigaciones conjuntas en diferentes países de la UE.

10 CONTINUAR PROTEGIENDO LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS

Contar con una ley exhaustiva es un gran hito, pero no implica que los gobiernos dejen de avanzar con respecto a la protección de datos personales y la privacidad. Es posible que surjan nuevos desafíos con respecto a la privacidad y la

[40] Autoridad nacional de Túnez para la protección de datos personales. Artículo 211. Projet de loi relative à la protection des données personnelles, 2017. http://www.inpdp.nat.tn/Projet_PDP_2017.pdf
[41] Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
[42] Vea el Panel de debate: Computer, Privacy and Data Protection, Bruselas, 2015.
https://www.youtube.com/watch?v=sikwHfoiylg
[43] Vea los Capítulos 7 y 8. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

protección de datos durante las fases de implementación, incluso si los gobiernos apuntan a que las leyes sean «a prueba del futuro». Esto significa que posiblemente sea necesario un proceso de revisión, el cual es una gran oportunidad para actualizar la ley, abordar cualquier potencial problema de cumplimiento, y arrojar una mayor claridad y certeza legal donde sea necesario.

También es importante entender que la ley de protección de datos actúa como base y no como techo en la protección de los derechos de los usuarios. Esto quiere decir que las organizaciones deben cumplir con la ley, como mínimo, pero deberían también estar motivadas a ir más allá y tomar más medidas para proteger la privacidad de las personas. Asimismo, dependiendo de la estructura y la forma de gobierno de un determinado país, se pueden tener en cuenta distintos enfoques con respecto a la protección de datos y la privacidad. A modo de ejemplo, en los EE. UU., el gobierno federal no debería evitar que los gobiernos y estados locales contemplen protecciones a los usuarios, además de las medidas limitadas brindadas por el nivel federal, y abstenerse de usar sus poderes para prevenir leyes regionales y locales.[44] Sin embargo, en el caso de la Unión Europea, los estados miembros deben evitar crear reglas adicionales, ya que esto podría fragmentar el alto y armonizado nivel de protección de los usuarios, acordado en el RGPD.

Experiencia de las negociaciones del RGPD

Desde 1995, los estados miembros de la UE habían adoptado diferentes leyes locales de protección de datos teniendo como referencia la Directiva de Protección de Datos de la UE. Esta ley de la UE se completó en un momento en el que solo el 1% de la población estaba en línea, y urgía modernizarla cuando la Comisión de la UE propuso el Reglamento General de Protección de Datos en 2012.[45] Llevó casi cinco años de negociaciones que los legisladores concordaran en las nuevas medidas en la ley, que se aplicarán de manera directa a partir de mayo de 2018 (a diferencia de una Directiva, que necesita incorporarse a la ley nacional, un Reglamento es aplicable de manera directa). Las 28 leyes nacionales de protección de datos serán remplazadas por esta única ley que recoge derechos y reglas armonizadas para toda la UE. Si bien este sistema funciona en el ordenamiento jurídico de la UE, puede que no sea el panorama ideal en otras regiones o países. Puede llegar a ser muy difícil ponerse de acuerdo en las leyes supranacionales y puede que no sea el mejor instrumento para proteger a los usuarios. Por lo tanto, no existe un modelo de ley ideal, sino que todas las leyes de protección de datos deberían tener en cuenta todos los puntos mencionados en este documento.

QUÉ NO HACER

En esta sección encontrará cinco recomendaciones para que sigan los responsables de formular políticas al momento de desarrollar una ley de protección de datos. Advertimos que, si son ignorados, estos cinco elementos podrían limitar los beneficios de la ley propuesta y dañar los derechos de los individuos.

1 BUSCAR AMPLIAS LIMITACIONES DE PROTECCIÓN DE DATOS Y DE PRIVACIDAD POR RAZONES DE SEGURIDAD NACIONAL

Los gobiernos no solo tienen la obligación sino también un interés de seguridad al proteger los datos personales, en especial cuando la información es retenida por agencias del gobierno. En 2015, como resultado de un incidente de ciberseguridad en los EE. UU., robaron 21,5 millones de registros de empleados federales y miembros familiares almacenados en la Oficina de Administración de Personal.[46] A causa de que estos tipos de incidentes y ataques van en aumento en el mundo, los países deben tomar medidas para proteger mejor la información de los individuos.

[44] EPIC, Privacy preemption watch. https://epic.org/privacy/preemption/
[45] Comisión Europea, reforma de la UE de las reglas de protección de datos, 2012. http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[46] Patricia Zengerle, Megan Cassella, Millions more Americans hit by government personnel data hack, Reuters, 2015. https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709

A pesar de esto, los gobiernos a menudo buscan limitaciones a la protección de datos y los derechos de privacidad para su propio uso de datos personales a través del uso de excepciones amplias. Estas excepciones deben evitarse y estar limitadas a medidas claramente definidas, necesarias, y proporcionadas que incluyan mecanismos de supervisión judicial y reparación accesible. La legislación no debería conceder a los gobiernos y entidades públicas la capacidad de escudarse de la obligación de proteger los derechos de los usuarios a la protección de sus datos. Los países tienen un interés de seguridad en salvaguardar los datos personales mediante agencias gubernamentales.

Experiencia de las negociaciones del RGPD

El RGPD aporta una lista de razones a las que pueden recurrir los estados miembros para restringir los derechos y libertades de los usuarios protegidos bajo la ley, como la seguridad o defensa nacional.[47] Aunque es común encontrar disposiciones que permiten a los estados restringir derechos en todos los instrumentos de la UE y la legislación nacional, el lenguaje de estas disposiciones es, generalmente, deliberadamente impreciso y puede llegar a cubrir un gran rango de actividades estatales. El RGPD, por ejemplo, permite la restricción de derechos, amplia e indefinidamente, a causa de «otros objetivos importantes de interés público general de la Unión o de un Estado miembro». Dado el impacto de tales restricciones a los derechos y libertades de los usuarios, estas deberían estar claramente definidas y limitadas en la ley, y sometidas a criterios de transparencia y supervisión estrictos, y ser medidas necesarias y proporcionadas en una sociedad democrática.

2 AUTORIZAR EL PROCESAMIENTO DE DATOS PERSONALES EN BASE AL INTERÉS LEGÍTIMO DE LAS COMPAÑÍAS SIN LIMITACIONES ESTRICTAS

Las compañías a menudo argumentan que deberían tener el derecho a recopilar y procesar los datos de los usuarios, cuando este es su «interés legítimo», sin tener que notificar a los usuarios. A menos que esas excepciones estén definidas como tal (lo que no sucede en el caso del RGPD o la Directiva de 1995) y estén estrechamente delimitadas (lo que se logró mejor en el RGPD), eso no debería estar permitido. De otro modo, esto se contradice intrínsecamente con el objetivo de protección de datos, que es darles a los usuarios el control de su información. Deben evitarse estos intentos de limitar los derechos de los usuarios.

Experiencia de las negociaciones del RGPD

El interés legítimo de las organizaciones es una de las bases jurídicas que puede utilizarse para procesar datos personales bajo el RGPD.[48] La esencia de la protección de datos es el control en manos de los usuarios y la predictibilidad del uso de sus datos. La disposición del interés legítimo va en contra de estos principios. Respaldada por el «interés legítimo», una organización está autorizada a recopilar y utilizar información personal sin tener que notificar a los usuarios en cuestión. Si no sabemos que una entidad retiene nuestros datos, ¿cómo podemos ejercer nuestro derecho de acceso de datos o nuestro derecho de oposición?

Esta disposición fue una de las más debatidas durante las negociaciones del RGPD. Las compañías defendían una disposición amplia y definida de manera imprecisa para el interés legítimo, y la sociedad civil intentaba eliminarla o limitar su alcance significativamente. Los legisladores intentaron limitar el impacto de la disposición durante los últimos meses de negociaciones mediante la incorporación de un requisito

[47] Vea el Artículo 23. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[48] Vea el Artículo 6. 1. (f). Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

por el que las compañías equilibren su interés legítimo y los derechos fundamentales. Si bien la intención es loable, las compañías llevarán a cabo esa evaluación a discreción propia y los usuarios quedarán a ciegas. El resultado final no fue satisfactorio para ninguna de las partes, ya que los negocios querían más flexibilidad que la acordada en el texto y sus correspondientes considerandos, y las ONG querían limitaciones claras. Entendemos la necesidad de brindar a las compañías medidas que les permitan dirigir sus negocios, pero las medidas que evitan que los usuarios tomen control de su información personal deben quedar excluidas, debido a que contradicen el espíritu y el objetivo de la ley de protección de datos.

3 DESARROLLAR UN «DERECHO AL OLVIDO»

El «derecho al olvido» emerge de la ley de protección de datos de la UE incluyendo el fallo de «Google Spain».[49] Este derecho permite que los usuarios, en ciertas circunstancias, soliciten que los motores de búsqueda no presenten ciertas direcciones web en los resultados cuando se realiza una búsqueda de sus nombres, sin que esas direcciones se quiten de los índices de los motores de búsqueda. Este derecho no debe confundirse con el derecho a la supresión, que permite a los individuos eliminar todos los datos personales referidos a ellos al dejar un servicio o aplicación. El derecho a la supresión es esencial para garantizar el control del usuario sobre su información personal. Tampoco debe ser comparado con cualquier medida de eliminación, ya que el derecho al olvido desarrollado en la jurisprudencia de la UE no exige o pone como requisito que cualquier contenido en línea sea eliminado de la web o de los índices de los motores de búsqueda.

Una importante amenaza para los derechos humanos es la manera en que varios gobiernos han malinterpretado —accidentalmente o no— a escala internacional el «derecho al olvido» o han buscado extender su alcance para limitar las libertades de expresión o de información de los individuos. Tribunales y legisladores alrededor del mundo mostraron un gran interés en desarrollar medidas para establecer un «derecho al olvido» ordenando la eliminación de contenido, lo que se desvía significativamente del enfoque desarrollado por los tribunales de la UE.[50] [51] [52] Cualquier medida del llamado derecho al olvido que lleve a la supresión de contenido en línea es una malinterpretación grave del derecho. Bajo ninguna circunstancia debe aplicarse este derecho para habilitar la remoción de contenido en línea. Asimismo, las autoridades de protección de datos no deberán estar autorizadas a solicitar la eliminación de información en línea sin la supervisión de un juez que pueda garantizar que todos los derechos fundamentales, incluidos el derecho a la libre expresión y la libertad de acceso a la información, sean respetados.

Access Now se opone a cualquier desarrollo de semejante «derecho al olvido». No obstante, si los legisladores fueran a tener en cuenta un derecho similar al vigente en la UE, Access Now ha identificado una serie de salvaguardas legales que deberían entrar en vigor para poder seguir mitigando los riesgos de abuso y daños de los derechos humanos.[53]

[49] Tribunal de Justicia de la Unión Europea, Sentencia dictada en el Asunto C-131/12, Google Spain SL vs Mario Costeja González, 13 de mayo de 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de249578524881c67efe5ec.e34KaxiLc3eQc40LaxqMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=574499
[50] Access Now, O direito ao esquecimento no Brasil: quais os riscos para os direitos humanos? https://www.accessnow.org/o-direito-ao-esquecimento-no-brasil-quais-os-riscos-para-os-direitos-humanos/
[51] Access Now, Documento de posición: El "derecho al olvido" y su impacto en la protección de los Derechos Humanos https://www.accessnow.org/documento-de-posicion-el-derecho-al-olvido-y-su-impacto-en-la-proteccion-de-los-derechos-humanos/
[52] Access Now, In India, the "right to be forgotten" is in the hands of the Delhi High Court https://www.accessnow.org/india-right-forgotten-hands-delhi-high-court/
[53] Access Now, Understanding the right to be forgotten globally, September 2016 https://www.accessnow.org/cms/assets/uploads/2016/09/Access-Not-paper-the-Right-to-be-forgotten.pdf

El derecho al olvido se añadió al derecho a la supresión en el RGPD.[54] El derecho al olvido codifica la jurisprudencia del Tribunal de Justicia de la UE en el caso «Google Spain».[55] El Tribunal desarrolló un conjunto de criterios para que los motores de búsqueda tengan en cuenta al momento de recibir una solicitud de no presentación de resultados. Los motores de búsqueda deben satisfacer una solicitud de no presentación únicamente si la información personal incluida en la dirección web designada es «inadecuada, irrelevante, ha dejado de ser relevante, o es excesiva», y solo si la información no concierne a una figura pública o no es de interés público. Sin embargo, la información o los enlaces no deberán ser removidos de los índices de búsqueda. Deben ser accesibles al momento que los usuarios realicen búsquedas utilizando términos distintos al nombre del individuo que ha hecho la solicitud de no presentación. Cabe señalar que es importante que el RGPD aclara que la información debe ser presentada si es necesaria para el ejercicio del derecho a la libertad de expresión e información.

A pesar de esas salvaguardas, es necesario que exista una guía más profunda por parte de la UE y sus estados miembros para garantizar que los motores de búsqueda no se excedan ni se queden cortos en el cumplimiento de la ley y la sentencia. La incertidumbre respecto al alcance geográfico de la aplicación del derecho al olvido, por ejemplo, ha provocado nuevas procedimientos judiciales.[56] Por su parte, los motores de búsqueda deberían ser más transparentes con respecto a los criterios que han estado utilizando internamente para lidiar con estas solicitudes.

Finalmente, en la implementación actual de este derecho en la UE, el acceso a reparación es limitado. La única forma de recurso con la que cuenta un usuario es la oportunidad de impugnar una decisión del motor de búsqueda a la negación de la solicitud de no presentación. Debería quedar claro cuáles son las vías de reparación, y deberían ser extendidas.

Experiencia de las negociaciones del RGPD

4 AUTORIZAR A QUE LAS COMPAÑÍAS RECOPILEN DATOS SENSIBLES SIN CONSENTIMIENTO

Dada la importancia de los datos sensibles, es necesario brindarles un nivel de protección más alto que al resto de los datos personales para garantizar un nivel adecuado de control para los individuos. Por lo tanto, la recopilación y el procesamiento de datos personales sensibles solo deberán ser autorizados si los individuos prestan su consentimiento explícito e informado y si tienen el derecho a retirar ese consentimiento subsecuentemente.

Los datos sensibles representan un amplio rango de información personal, como el origen étnico o racial, la opinión política, las creencias religiosas o de otra índole, las afiliaciones, los detalles de salud mental o física, los datos genéticos o biométricos, información sobre vida sexual o sexualidad, o sobre delitos civiles o criminales. La naturaleza y relevancia especial de esta información implica que los usuarios deben siempre ser capaces de controlar quién tiene acceso y quién utiliza esta información. Consecuentemente, el tratamiento de datos sensibles debería únicamente estar autorizado si los usuarios han prestado libremente su consentimiento explícito e informado. Con el objetivo de proteger la esencia de los derechos fundamentales de los usuarios a la privacidad y a la protección de datos, no deberán permitirse excepciones a estas reglas.

[54] Vea el Artículo 17. Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[55] Access Now, FAQ on the right to be forgotten, 2014. https://www.accessnow.org/cms/assets/uploads/archive/docs/GoogleSpainFAQRtbF.pdf
[56] Access Now, Only a year until the GDPR becomes applicable: Is Europe ready? https://www.accessnow.org/year-gdpr-becomes-applicable-europe-ready/

Experiencia de las negociaciones del RGPD

El RGPD exige que las organizaciones obtengan el consentimiento explícito del usuario para la recopilación de datos sensibles como regla general. Si bien esto es extremadamente positivo, la ley también autoriza la recopilación y el uso de datos sensibles sin el consentimiento de los usuarios para cumplir algunos objetivos específicos, incluyendo «fines de investigación científica e histórica o fines estadísticos».[57] Esta amplia excepción priva a los usuarios de controlar su información más íntima y es aún más problemática en el contexto de la creciente industria de los servicios de salud en línea, el análisis a gran escala de puntos de vista políticos, entre otros. Si no se limita, las compañías podrían retener millones de datos sensibles por los próximos años, inicialmente para llevar a cabo investigaciones y elaborar estadísticas sobre sus productos. En la práctica, sería complejo supervisar cómo las organizaciones usan estos datos, ya que los usuarios no estarían informados sobre ello. Los usuarios deben ser capaces de controlar qué organización tiene acceso a sus registros de salud o votación. Deben evitarse estos tipos de vacío legal, o por lo menos deben estar estrictamente limitados mediante la restricción del uso de estos datos para la investigación, y la investigación estadística debe llevarse a cabo en el interés público bajo estricta supervisión.

5 FAVORECER LOS MECANISMOS DE AUTORREGULACIÓN Y CORREGULACIÓN

Durante muchos años, las compañías y entidades que recopilan datos pidieron que la regulación de la privacidad y la protección de datos no se diera a través de marcos vinculantes, sino mediante mecanismos de auto- o corregulación que ofrezcan mayor flexibilidad. Pese a varios intentos, no existen ejemplos de regímenes no vinculantes que hayan tenido éxito en proteger los datos personales o la privacidad y que hayan sido positivos para los derechos de los usuarios o, de hecho, para el negocio en sí.

Gracias a que se comparten más datos tanto en línea como fuera de línea, ya es hora de que se desarrollen marcos obligatorios para la protección de datos y la privacidad en todo el mundo, para evitar o terminar con estos comportamientos y devolverles el control de su información a los usuarios. Esto también habilitará el desarrollo de innovación que respete la privacidad, que actualmente se encuentra limitada a un pequeño número de compañías que han tomado un compromiso a largo plazo para proteger a sus usuarios, en lugar de basar sus modelos de negocio en la monetización de la información privada de sus usuarios.

Los modelos de negocio construidos sobre la privacidad pueden funcionar como una ventaja competitiva. En países que no cuentan con leyes de protección de datos generales, las compañías podrían innovar mediante sus prácticas internas, a través del desarrollo voluntario de salvaguardas y directrices que mejoren la confianza de las personas en la economía digital. A pesar de que la autorregulación no es adecuada como mecanismo de aplicación y no es sostenible para la protección de los derechos de los individuos, puede ser beneficiosa en ciertas circunstancias tanto para las compañías como para los individuos que adoptan voluntariamente un marco en esos países. No se puede confiar plenamente en ellos, ya sea desde la perspectiva de los individuos o de los negocios, debido al riesgo de un aprovechamiento indebido por parte de actores maliciosos que socaven la privacidad, la confianza, la innovación y la implementación de productos nuevos.

Experiencia de las negociaciones del RGPD

La Unión Europea tiene una larga historia de intentos fallidos en auto- o corregulación en el área de la libertad de expresión.[58] En el campo de la privacidad y la protección de datos, sin embargo, la UE ha sido pionera en el desarrollo de una protección de alto nivel para los usuarios. El RGPD es otro de los ejemplos de ese éxito. Aunque dista

[57] Vea el Artículo 9.2 (j). Unión Europea, Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[58] EDRi, Human rights and privatised enforcement https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf

mucho de la perfección, el RGPD es un instrumento clave para la protección de derechos fundamentales en la UE, y refleja años de experiencia ganada a través de la implementación de leyes y jurisprudencia previas desarrolladas por los tribunales. El RGPD crea obligaciones claras y fuertes para las organizaciones pero también incorpora varias herramientas de rendición de cuentas para promover los derechos de protección de datos, como los principios de protección de datos por diseño y por defecto y las nuevas disposiciones para los esquemas de certificación de las compañías y los códigos de conductas para toda la industria. Estas herramientas apuntan a desarrollar una visión de la protección de datos que va más allá del mero cumplimiento con la ley y motiva la innovación en este campo.

CONCLUSIÓN

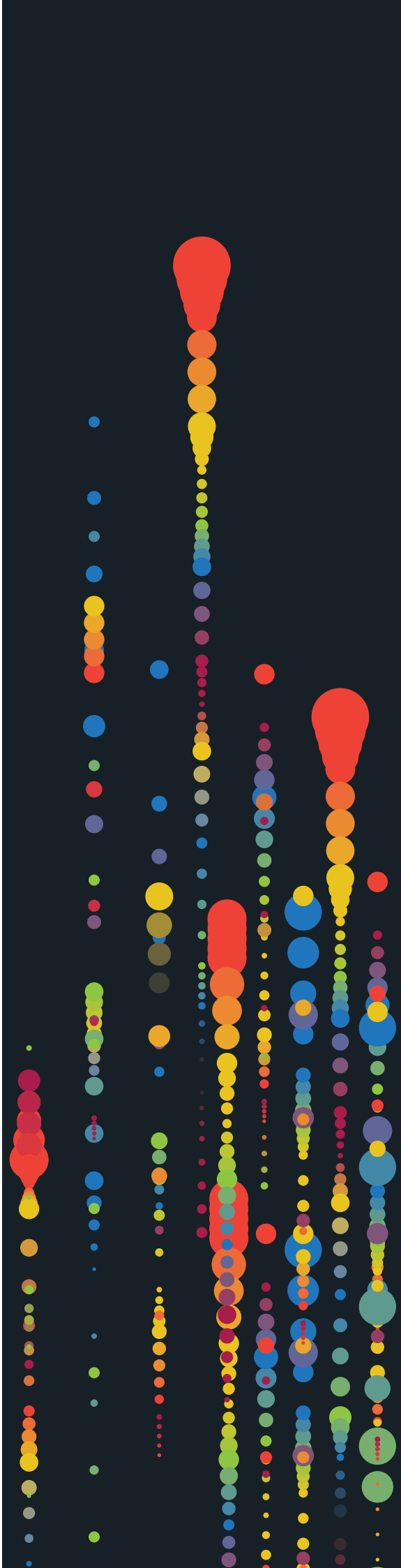
Access Now apoya con entusiasmo el desarrollo de marcos locales, regionales e internacionales para la protección de datos personales. Estos marcos deben estar centrados en el usuario y enfocarse en amparar y fortalecer los derechos, al tiempo que proporcionen reglas claras y predecibles para que las cumplan las entidades públicas y privadas. Por último, pero no por ello menos importante, cabe remarcar la importancia de los mecanismos de aplicación robustos e integrales, supervisados por una autoridad independiente para garantizar que las protecciones propuestas sean totalmente funcionales.

Proteger los datos a escala mundial ha sido el foco de Access Now durante un largo tiempo, y sigue siendo una de nuestras máximas prioridades. Entre otras cuestiones, nuestro equipo está involucrado de manera activa en la implementación del RGPD, la reforma de la legislación de protección de datos de Argentina, y las negociaciones en la India y Túnez para el desarrollo de una primera ley de protección de datos.

LA CREACIÓN DE UN MARCO PARA LA PROTECCIÓN DE DATOS:
UNA GUÍA PARA LOS LEGISLADORES SOBRE QUÉ HACER Y QUÉ NO

Este documento es una publicación de Access Now.

Para más información, por favor visite: **https://www.accessnow.org**
Contáctenos: **Estelle Masse** | Senior Policy Analyst | **estelle@accesnow.org**



accessnow

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación del apoyo técnico directo, el compromiso político integral, la defensa global, el otorgamiento de subvenciones para grupos locales emergentes, y las convocatorias como RightsCon, luchamos por los derechos humanos en la era digital.

https://www.accessnow.org