Hablemos de Protección de Datos

Hemos estado viviendo en la era de la información hace un tiempo y hoy, la data es el recurso más valioso. Es vital comprender que cada acción, decisión y movimiento que hacemos genera data, se ha vuelto inevitable. Es a través de esta que se construyen negocios, se toman decisiones y se establecen relaciones. Dada su relevancia, es imperativo hablar sobre la protección de datos, que se ha vuelto una inquietud recurrente entre gobiernos, organizaciones e individuos. Buscamos dar un enfoque tanto desde la perspectiva en la República Dominicana como en el panorama internacional, centrándonos en los aspectos regulatorios y los casos más significativos recientes.

La protección de datos personales es un pilar fundamental en el contexto internacional, las empresas se toman muy en serio el tema y es evidente que es una consecuencia directa de la globalización y la creciente digitalización de la sociedad. Esta relevancia viene dada en muchos casos por la ética corporativa que muchas empresas aplican, y en otros casos por las cuantiosas sanciones que las legislaciones en muchos países imponen a violaciones que implican la exposición de datos personales protegidos de sus ciudadanos.

Si bien cada región tiene su particular enfoque y regulaciones específicas, existen principios comunes que buscan garantizar la privacidad y seguridad de la información personal. Conversemos para entender comparando las diferentes legislaciones con la propia, cómo se enfoca una adecuada protección de datos en el marco de la ley y las recomendaciones prudenciales más socorridas de la materia.

1. Legislación Base

República Dominicana: La norma principal es la Ley No. 172-13 para la Protección de Datos de Carácter Personal.

Europa: El marco normativo clave es el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés), que se aplica en todos los Estados miembros de la Unión Europea.

Estados Unidos: A diferencia de Europa, Estados Unidos no posee una legislación federal única sobre protección de datos. Sin embargo, leyes como el California Consumer Privacy Act (CCPA) en California y el Health Insurance Portability and Accountability Act (HIPAA) para el sector salud, entre otras, regulan aspectos específicos de relevancia de la protección de datos.

2. Principios Rectores

República Dominicana y Europa: Ambas legislaciones coinciden en principios como la licitud, lealtad, limitación de la finalidad, exactitud y limitación de conservación.

Av. John F. Kennedy 64, Santo Domingo, D.N. 10512, República Dominicana • 809.566.7111 • www.ulisescabrera.com • info@ulisescabrera.com • RNC 1-01-88634-1

Estados Unidos: Si bien no existe una normativa unificada, la transparencia, la finalidad, y la minimización de datos son principios que emergen recurrentemente en diferentes leyes estatales y federales.

3. Derechos del Titular
República Dominicana: Se reconocen derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

Europa (GDPR): Se amplían los derechos de los ciudadanos, incluyendo el derecho al olvido, la portabilidad de datos y el derecho a ser informado sobre violaciones de datos.

Estados Unidos: Depende de la jurisdicción y la ley específica, pero, por ejemplo, el CCPA otorga derechos similares al GDPR, como acceso, oposición a la venta de datos y eliminación.

4. Responsabilidades de las Organizaciones
República Dominicana: Las entidades deben informar, mantener confidencialidad, asegurar datos y registrar archivos en el órgano de control.

Europa (GDPR): Las organizaciones deben garantizar el cumplimiento de los principios del GDPR, realizar Evaluaciones de Impacto de Protección de Datos en ciertos casos y designar un Delegado de Protección de Datos cuando sea necesario.

Estados Unidos: Las responsabilidades varían, pero muchas legislaciones exigen transparencia, consentimiento informado y medidas de seguridad adecuadas.

5. Transferencia Internacional de Datos
República Dominicana: Se permite la transferencia internacional de datos bajo ciertas condiciones, resguardando la protección adecuada de los datos.

Europa (GDPR): Las transferencias fuera de la UE están sujetas a requisitos estrictos para garantizar un nivel adecuado de protección.

Estados Unidos: Las transferencias se basan más en acuerdos bilaterales o sectoriales. Un ejemplo clave fue el "Escudo de Privacidad" entre la UE y los EE.UU., aunque fue invalidado por el Tribunal de Justicia de la UE en 2020.

6. Enfoque Regulatorio y Sanciones
República Dominicana: La ley establece sanciones que incluyen multas pecuniarias y la posibilidad de suspensión de actividades relacionadas con el tratamiento de datos.

Europa (GDPR): El enfoque es altamente regulatorio, con sanciones que pueden alcanzar hasta el 4% del volumen de negocios anual global de la empresa o 20 millones de euros, lo que sea mayor.

Estados Unidos: El enfoque varía según el estado y el sector, pero en general, hay una combinación de sanciones civiles, requerimientos de notificación y, en algunos casos, acciones colectivas por parte de los consumidores.

Av. John F. Kennedy 64, Santo Domingo, D.N. 10512, República Dominicana • 809.566.7111 • www.ulisescabrera.com • info@ulisescabrera.com • RNC 1-01-88634-1

7. EU GDPR Casebook

La Unión Europa basa su enfoque en algunos pilares esenciales:

Derechos de los individuos: La GDPR refuerza los derechos individuales, incluido el derecho a ser informado, el derecho de acceso, el derecho de rectificación, el derecho de supresión (derecho al olvido), entre otros.

Consentimiento: El consentimiento debe ser libre, específico, informado e inequívoco. Las organizaciones ya no pueden usar términos y condiciones largos y difíciles de entender.

Violaciones de datos: Las organizaciones están obligadas a informar a las autoridades de protección de datos sobre las violaciones de datos en un plazo de 72 horas después de haber tenido conocimiento de ello.

Responsabilidad y gestión de riesgos: Las empresas deben adoptar un enfoque de "protección de datos desde el diseño y por defecto", lo que significa que deben considerar la privacidad desde las primeras etapas de cualquier proyecto.

Transferencias internacionales: Las transferencias de datos personales fuera del EEE (Espacio Económico Europeo) solo están permitidas bajo ciertas condiciones.

Designación de DPO (Oficial de Protección de Datos): Algunas organizaciones están obligadas a designar un DPO.

Mecanismos de responsabilidad: Las organizaciones deben implementar políticas internas, medidas y procedimientos que cumplan con los principios de la GDPR.

Sanciones: Las violaciones de la GDPR pueden resultar en sanciones significativas, que pueden alcanzar hasta el 4% del volumen de negocios anual global de una empresa.

Opiniones del Comité Europeo de Protección de Datos (EDPB): El EDPB ha emitido varias opiniones y guías sobre diferentes aspectos de la GDPR, las cuales han sido esenciales para la interpretación y aplicación del reglamento.

8. Casos específicos

A lo largo de los años, han surgido varios casos judiciales que han ayudado a interpretar y aplicar la GDPR. Por ejemplo, casos relacionados con plataformas de redes sociales, motores de búsqueda y otros actores clave en la economía digital.

Desde la implementación del Reglamento General de Protección de Datos (GDPR) en la UE en mayo de 2018, ha habido varias sanciones notables impuestas a empresas por violaciones:

Francia: Google. En 2019 La Comisión Nacional de Informática y Libertades de Francia (CNIL) impuso una multa de 50 millones de euros a Google. La razón fue a criterio de la CNIL, Google no proporcionó una información clara y comprensible a sus usuarios sobre cómo procesa sus datos, y no obtuvo un consentimiento válido para la personalización de sus anuncios.

Reino Unido: Marriott International. La ICO también anunció en 2019 una multa propuesta de 110 millones de euros para Marriott International debido a una violación de datos que expuso información personal de hasta 339 millones de huéspedes. Al igual que con British Airways, la multa se redujo más tarde a 20 millones de euros en 2020.

Italia: TIM. En 2020 la Autoridad Italiana de Protección de Datos impuso una multa de 27,8 millones de euros a TIM, una de las principales compañías de telecomunicaciones de Italia, por varias infracciones, que incluyen marketing no solicitado y fallas en el procesamiento de datos.

Alemania: H&M. En 2020 la autoridad de protección de datos de Hamburgo impuso una multa de 35,3 millones de euros a la filial alemana de la marca de moda H&M. La compañía había almacenado información privada sobre sus empleados en un archivo accesible a cientos de gerentes.

Irlanda: WhatsApp. En 2021 WhatsApp fue multado con 225 millones de euros por la Comisión de Protección de Datos de Irlanda debido a la falta de transparencia en torno a cómo comparte datos con otras empresas de Facebook.

En latitudes más cercanas:
Colombia: Uber. En 2019, la Superintendencia de Industria y Comercio (SIC) sancionó a Uber con una multa cercana a los 2,128 millones de pesos colombianos (aproximadamente 600.000 dólares) debido a una violación de datos que afectó a 267.000 colombianos en 2016.

México: Banco Mercantil del Norte (Banorte). En 2013, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) impuso una multa de 32 millones de pesos mexicanos (aproximadamente 1,6 millones de dólares) a Banorte por no proteger adecuadamente los datos de sus clientes.

Argentina: Telefónica Móviles Argentina. En 2017, la Dirección Nacional de Protección de Datos Personales impuso una multa de 110.000 pesos argentinos (aproximadamente 1.200 dólares) por no actualizar correctamente la base de datos del sistema "No llame", permitiendo que los usuarios continuaran recibiendo publicidad no deseada.

Chile: Retail Financiero (CMR Falabella). En 2019, la Superintendencia de Bancos e Instituciones Financieras impuso una multa de 6.000 UF (aproximadamente 170.000 dólares) a CMR Falabella por no notificar oportunamente una filtración de datos que afectó a más de 14.000 tarjetas de crédito.

Perú: Supermercados Peruanos (Plaza Vea). En 2018, la Autoridad Nacional de Protección de Datos Personales sancionó a la empresa con una multa de 183.000 soles (aproximadamente 55.000 dólares) por no contar con el consentimiento expreso de sus clientes para el tratamiento de sus datos personales en acciones de marketing.

Estos son solo algunos ejemplos de las sanciones relacionadas con el EU GDPR y otras jurisdicciones. Es importante destacar que cada caso es único y las circunstancias específicas, el alcance de la violación y otros factores determinan la severidad de las sanciones. Además, muchas de estas sanciones pueden ser objeto de apelación o negociación. Para Latinoamérica es clara la voluntad de las autoridades de garantizar la privacidad y seguridad de la información personal de los ciudadanos. Es esencial que las empresas en la región estén al tanto de sus obligaciones y actúen de manera proactiva para evitar sanciones y garantizar la confianza de sus clientes y usuarios.

Av. John F. Kennedy 64, Santo Domingo, D.N. 10512, República Dominicana • 809.566.7111 • www.ulisescabrera.com • info@ulisescabrera.com • RNC 1-01-88634-1

En nuestro patio, la República Dominicana ha trabajado en el fortalecimiento de su marco legal relacionado con la protección de datos personales, especialmente a través de la Ley No. 172-13 para la Protección de Datos de Carácter Personal. Sin embargo, a pesar de que ha habido discusiones y actividades de sensibilización en torno a esta ley, la aplicación de sanciones específicas no ha sido prominente como en otras jurisdicciones.

9. Reflexiones finales

Si bien existen diferencias en la forma en que la República Dominicana, Europa y Estados Unidos abordan la protección de datos, todas reconocen la importancia fundamental de proteger los derechos de los individuos en relación con su información personal. En un mundo cada vez más interconectado, la armonización y el entendimiento de estas regulaciones se vuelven esenciales para las organizaciones que operan a nivel global.

En nuestra era digital, la información, o "data", se ha convertido en el recurso más valioso. Somos generadores de data, consumidores de ella, la comercializamos y, a menudo, somos vulnerables a su mal uso. Su relevancia creciente nos impulsa a entender y discutir el panorama de la protección de datos, tanto en el contexto dominicano como en el internacional.

Este breve artículo ha buscado ofrecer más que una simple opinión; su objetivo ha sido presentar una visión regulatoria, resaltando casos significativos y aspectos críticos en el ámbito de la protección de datos. Con la esperanza de haber proporcionado claridad y entendimiento sobre este tema complejo y en constante evolución, invitamos a los lectores a reflexionar sobre la importancia de estas regulaciones en nuestra sociedad digital actual.

Autora:
MÓNICA VILLAFAÑA
Socia