¿Qué está pasando con nuestros datos personales en las redes sociales?

11 September, 2023 por Fabricio Rodríguez - Arturo Muente Kunigami
https://blogs.iadb.org/administracion-publica/es/que-esta-pasando-con-nuestros-datos-personales-en-las-redes-sociales/

Un nuevo debate de carácter global se ha generado en torno a la protección de los datos personales, involucrando a una de las redes sociales con mayor crecimiento y popularidad en los últimos años (de acuerdo con Statista). A partir de su creciente éxito, particularmente entre las personas adolescentes y jóvenes, las **autoridades gubernamentales de diversos países han mostrado preocupaciones relacionadas con el tratamiento de los datos personales de las personas usuarias que este tipo de plataformas recopilan**.

Uno de los más recientes capítulos de controversia se vivió en Washington D.C., donde por pedido de las autoridades del Congreso, durante más de cinco horas se discutió, entre otros temas, cómo los datos personales de los **más de 150 millones de ciudadanos y ciudadanas estadounidenses usuarias de una de estas plataformas podrían estar en riesgo**.

Algunos representantes argumentaron que esto pondría en peligro incluso la seguridad nacional del país, lo cual generó solicitudes de prohibición total del uso de esta red social en territorio estadounidense.

En términos generales, es cierto que las redes sociales tienen acceso a datos personales de sus personas usuarias, quienes, **al aceptar los términos del servicio y la política de privacidad, aceptan también el tratamiento que la plataforma brindará a dicha información**. Entre los datos personales más importantes recopilados por algunas redes sociales durante su proceso de registro encontramos:

- Nombre
- Fecha de nacimiento
- Lenguaje (idioma)
- Números de teléfono celular (propios y de los contactos guardados)
- Correo electrónico
- Información de geolocalización de la persona usuaria
- IP del equipo utilizado
- Información biométrica, como huella facial y huella de voz (*faceprint* y *voiceprint*)
- Datos de métodos de pago
- Entre otros

Además de estos datos, debemos contemplar la información que se genera por el uso mismo de las redes sociales y por su potencial interacción con otras plataformas.

Es importante notar que no solo las redes sociales recopilan datos personales de sus personas usuarias, muchas aplicaciones que proveen servicios digitales también lo hacen, en donde, dependiendo de su naturaleza, p**ueden acceder o registrar información incluso aún más sensible, como datos de salud o registros médicos**.

Por lo tanto, actualmente resultaría casi imposible evitar compartir nuestros datos en un entorno virtual. Esto evidencia que su prohibición no constituye una solución sostenible, lo cual nos lleva a preguntarnos: **¿es seguro compartir nuestros datos personales?** Y, tal vez igual de importante, **¿quién está velando por su protección?**

¿Quién vela por la protección de nuestros datos personales?

La coyuntura actual en los Estados Unidos ha despertado interés y este caso evidencia la **necesidad cada vez más imperiosa de los países por contar con una legislación específica y adecuada que regule la protección de los datos personales de la ciudadanía.**

El portal digital Encyclopedia of European History, proyecto digital de la **Universidad Sorbona, Europa**, ha venido observando este problema desde los años sesenta y generando las primeras legislaciones al respecto en los años setenta, convirtiéndose en referente global en materia de protección de datos personales.

En la actualidad, la Unión Europea, mediante el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés), ha generado estándares en torno al adecuado tratamiento de los datos personales de su ciudadanía, que han sido guía y ejemplo a otras naciones del mundo para generar su propia legislación. Por ejemplo, 17 de los 26 países prestatarios del BID ya cuentan con una Ley General de Protección de Datos Personales.

Al igual que la Unión Europea, otros países cuentan con esquemas legales similares como: Canadá con la Ley de Protección de la Información Personal y Documentos Electrónicos (PIPEDA por sus

siglas en inglés); Japón con la Ley de Protección de la Información Personal; y Corea del Sur con la Ley de Protección de la Información Personal, por citar algunos ejemplos. En el caso de Estados Unidos, si bien cuenta con legislación relacionada con la protección de datos personales a nivel federal y estatal, no tiene una legislación específica, con la amplitud e integralidad de los otros ejemplos de los países señalados.

Bajo el funcionamiento de estos marcos legales que determinan la pauta para el uso y tratamiento de datos personales en las plataformas que operen en esos países, se han desarrollado varias demandas por incumplimientos a la norma. Entre las más importantes podemos mencionar el denominado **"escándalo de Cambridge Analytica"** que dio como resultado una de las compensaciones económicas más grandes de la historia relacionada con un proceso legal por el uso de datos personales.

Casos similares, con multas millonarias, han enfrentado plataformas frente a la Unión Europea, por violaciones al GDPR, evidenciando además los retos que varias plataformas enfrentan en el tratamiento brindado a flujos de datos transnacionales, especialmente derivados de la falta de legislación o la incompatibilidad de esta entre los países en donde se están manejando dichos datos.

¿Qué está pasando en América Latina y el Caribe en relación con la protección de datos personales y redes sociales?

A diferencia de otras legislaciones del mundo**, en América Latina y el Caribe, las leyes de protección de datos personales son instrumentos jurídicos relativamente nuevos y con diversos grados de madurez,** según se explica en el portal "Los datos personales y sus leyes".

Al contrastar estas leyes con los estándares iberoamericanos de protección de datos personales, desarrollados por la Red Iberoamericana de Protección de Datos, las legislaciones de **Barbados, Ecuador y México** son las que más se ajustan a dicho modelo.

Bajo este contexto, en la región también se han dado casos donde los gobiernos han utilizado estas leyes para proteger y asegurar el adecuado tratamiento de los datos de sus ciudadanía. Entre otros, podemos mencionar a: **Brasil**, que en el 2022 multó a una plataforma de redes sociales por filtración de datos de 443.000 usuarios brasileños; **Colombia**, cuya Autoridad de Protección de Datos (DPA) ratificó el deber de una red social de fortalecer las medidas de seguridad para proteger mejor los datos personales de más de 31 millones de colombianos, medida que ha sentado bases para casos posteriores en donde la autoridad se ha pronunciado sobre la implementación de medidas acordes con el estándar colombiano en materia de Habeas Data y debido tratamiento de datos personales; o **México**, en donde el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales INAI, resolvió iniciar un proceso de verificación contra una plataforma.

Las múltiples demandas que las plataformas de redes sociales han enfrentado sobre el tratamiento que brindan a los datos personales de sus personas usuarias, son un ejemplo de la **importancia que tiene para los países contar con un marco legal específico y adecuado que asegure la protección de datos personales de su ciudadanía.**

Sin embargo, **garantizar la efectiva aplicación y cumplimiento de estos marcos normativos es también un reto que requiere la creación de capacidades institucionales específicas** para el efecto,

condición particularmente importante en la región en donde **apenas 10 países cuentan con una agencia especializada a cargo de vigilancia y cumplimiento de estas normas**.

Desde el **Banco Interamericano de Desarrollo** trabajamos permanentemente en el apoyo a los gobiernos de la región para la creación, mejora y aplicación de los marcos legales; así como en la generación de la institucionalidad necesaria para lograr una efectiva y adecuada protección de datos personales.

En una sociedad que transita cada vez con mayor velocidad hacia entornos digitales, reconocemos la necesidad de contar con un marco regulatorio no solo para la protección de la ciudadanía, sino también para el impulso a la innovación, la economía digital, la inclusión y el desarrollo de toda la población.