

La protección de datos personales es un derecho humano

En esta época de mayor digitalización, las personas se están volviendo más conscientes y preocupadas por la protección de sus datos personales. El procesamiento de datos personales se ha vuelto cada vez más valioso y lucrativo para las empresas. Ofrece oportunidades para el crecimiento económico, el avance social y la investigación. Sin embargo, también puede suponer riesgos para los derechos individuales: sus derechos humanos básicos.

La protección de datos se refiere al procesamiento de datos personales, que conlleva riesgos particulares en términos de cómo se recopilan, almacenan y difunden. Los datos personales pueden revelar quién es una persona, sus relaciones, estado de salud, detalles financieros, preferencias sexuales y creencias. Por lo tanto, su procesamiento puede plantear graves riesgos para el derecho humano básico a la privacidad de una persona.

Las organizaciones tienen más responsabilidad que nunca de utilizar los datos de forma ética, compatible y segura. Con todo, la protección de datos, o más bien la falta de ésta, sigue acaparando los titulares. Cada vez más, la protección de datos y las tecnologías de ciberseguridad emergen como las responsables de proteger la integridad de nuestros derechos humanos, que incluyen el derecho a la libertad de expresión y el derecho a la no discriminación.

El derecho a la libertad de expresión incluye la libertad de buscar, recibir y difundir información, ideas y opiniones. La capacidad de permanecer en el anonimato a veces puede ser fundamental. En sociedades donde ciertas declaraciones pueden dar lugar a represalias o persecución, las personas suelen expresarse libremente de forma anónima. En muchas partes del mundo, sin embargo, esta capacidad está siendo socavada.

El derecho a la no discriminación es fundamental, pues la información sobre una persona podría revelar directa o indirectamente sus características personales que tal vez no desee que se conozcan. Por ejemplo, la privacidad de su religión, orientación sexual, género o estado de salud puede ser fundamental para garantizar la protección contra la discriminación.

Asimismo, el acceso no autorizado a los datos personales de un individuo también puede resultar en discriminación. No es sólo la existencia de datos personales lo que puede dar pie a la discriminación, sino también su procesamiento, particularmente cuando las personas se perfilan sobre la base de sus datos personales. Las empresas y otras instituciones pueden utilizar la elaboración de perfiles para tomar decisiones que afecten a la forma en que se trata a una persona, qué servicios se le ofrecen y en qué condiciones.

¿Hasta dónde llega el papel de la tecnología?

Mucho se ha dicho sobre el rol de la tecnología como facilitadora para difundir desinformación e incitar a una guerra de información cibernética. Pero es vital recordar que la tecnología también es nuestra mayor arma en la lucha contra los ciberdelincuentes, en especial para protegernos de la reciente arma de su elección: el ransomware. Se trata de un malware creado para cifrar los

archivos y el almacenamiento, de manera malintencionada.

El ransomware es una de las amenazas más intratables y comunes que enfrentan las organizaciones en todas las industrias y geografías. Y aún más dañinas son las innumerables violaciones a los derechos humanos, pues los atacantes amenazan cada vez más con filtrar los datos robados.

Para combatir esto, al igual que los crecientes desafíos de los ciberdelincuentes que trabajan en conjunto, es importante que la tecnología forme sus propios ejércitos y alianzas, como las que Veeam ha formado, para la protección contra el ransomware. Pero, por supuesto, los hackers siempre están buscando formas innovadoras de robar datos y, desde el inicio del Covid-19, las empresas no han sido las únicas que aceleran su transformación digital.

Es más crucial que nunca trabajar con socios tecnológicos que no sólo prioricen las necesidades de gestión de datos de hoy, sino que también busquen la nube y las soluciones de seguridad del mañana, mientras permanecen un paso por delante de la ciberdelincuencia. Pero aún así, demasiadas organizaciones, sin darse cuenta, están ayudando a los esfuerzos de los hackers con su enfoque indiferente a la seguridad de los datos.

Las multas y el daño a la reputación son, por supuesto, elementos disuasorios; con todo, seguimos viendo múltiples violaciones a los datos, y las compañías deben hacer más para frenar la difícil situación de la protección de datos. Para este fin, la tecnología es, de nuevo, un factor clave. Sin importar el tamaño de las empresas, es imperativo encontrar una solución que garantice la seguridad de los datos, el cumplimiento y los requisitos de privacidad del cliente; más allá de la palabra de un proveedor de que sus soluciones son seguras, conviene investigar, leer los testimonios de los clientes y buscar organismos de recompensas respetados.

Ante nuevas legislaciones que surgen constantemente, las organizaciones deben asegurar que todos los datos recopilados permanezcan siempre seguros y acorde con el cumplimiento, y que los derechos humanos de las personas están protegidos. Asociarse con un proveedor confiable, como Veeam, es una forma de lograr esto de manera efectiva.