Contribución al documento"Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube" de la Red Iberoamericana de Protección de Datos (RIPD)

5 de Marzo de 2021

El Foro de la Sociedad Civil agradece la invitación y desea hacer los siguientes comentarios acerca del proyecto de "Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube" elaborado por la RIPD.

1. Informar al titular del dato acerca de las implicancias de los servicios de computación en la nube: En general, las personas desconocen que grandes volúmenes de datos personales generados por ellos se encuentran almacenados en la nube. Más aún, a veces los titulares del dato pueden tener dificultades para entender el significado de "computación en la nube", su modo de funcionamiento, las consecuencias legales de estos servicios y los lugares en los cuales efectivamente sus datos se encuentran almacenados. Por lo tanto, resulta indispensable que tanto los encargados como los responsables de un tratamiento de datos que se llevará a cabo en la nube comuniquen de manera clara, didáctica y detallada a los titulares del dato todas las características principales de este tipo de tratamiento. De este modo, se cumpliría con el principio de transparencia (art. 16 Estándares Iberoamericanos de Protección de Datos Personales) y el derecho a acceso (art.25 Estándares Iberoamericanos de Protección de Datos Personales).

2. Contratación de servicios de CEN por parte del Estado: En el caso de entidades públicas o gobiernos, la evaluación de la necesidad de contratar servicios de CEN resulta imperiosa. Las bases de datos estatales pueden incluir información particularmente sensible sobre toda la ciudadanía de un país. Por lo tanto, su transferencia a proveedores que estén ubicados en el extranjero puede traer como consecuencia la cesión de control del Estado a otras jurisdicciones sobre datos valiosos no solamente para los titulares sino para asuntos estratégicos de cada país. De esta manera, el documento debería recomendar expresamente a los

Estados que consideren alternativas como la contratación de servicios de nube locales o la creación de servidores propios en donde almacenar los datos personales. Asimismo, los gobiernos deberían adoptar instituciones y procedimientos por el cual actores externos (organizaciones de la sociedad civil, academia, comunidad técnica, etc) y la ciudadanía en general puedan supervisar la forma en que el Estado almacena los datos personales de las personas.

3.Incluir la perspectiva de derechos humanos: El respeto a la normativa local no debe limitarse únicamente a la legislación sobre protección de datos personales. Los tratados internacionales sobre derechos humanos y las Constituciones también deben ser mencionados ya que la protección de datos personales es indispensable para respetar derechos fundamentales como la privacidad o la libertad de expresión. Por otro lado, existe un amplio consenso en que las empresas tienen el deber de prevenir, enfrentar y remediar violaciones a los derechos humanos que aparezcan en el curso de una operación comercial.

4. Acceso a datos por parte de terceros estados: En caso de las transferencias internacionales de datos, debemos tener en cuenta la posibilidad de que las autoridades o fuerzas de seguridad de países extranjeros puedan exigir el acceso a los datos bajo la aplicación de sus leyes internas en materia penal, procesal, de retención de datos, entre otras. Este riesgo debe ser cuidadosamente evaluado por el exportador de datos antes de contratar el servicio. En tal sentido, es indispensable que el acuerdo contemple la prohibición por parte del PSCEN de revelar a terceros países los datos personales exportados salvo que haya una autorización expresa por parte de la legislación del país exportador.

5. Contenido de la evaluación de impacto en protección de datos: Además de las ya mencionadas en el documento, la evaluación de impacto a la protección de datos debería incluir como mínimo lo siguiente: la naturaleza de los datos personales objeto del tratamiento, en particular aquellos que por su sensibilidad puedan ser riesgosos para la vigencia de los derechos fundamentales; el alcance de las operaciones de tratamiento (número de individuos a los cuales puede comprender) y el contexto dentro del cual se llevarán a cabo (categoría de los titulares del dato, ej, si hay niños o trabajadores involucrados); la finalidad para la cual se está proveyendo el servicio. Por otro lado, los riesgos a analizar deberían ser aquellos que son propios de los servicios de CEN en general y los específicos de acuerdo al servicio que se va a brindar en cada caso concreto.

6. Adoptar el marco internacional de derechos humanos como enfoque principal para evaluar los servicios CEN: Si bien compartimos la necesidad de incorporar los principios de privacidad por diseño y por defecto, somos cautelosos en relación a su vínculo con la ética. En este sentido, consideramos que el marco internacional de derechos humanos ofrece un marco y lenguaje común para evaluar la aplicación de estos principios. Adoptar el paradigma de los derechos humanos en lugar del paradigma de la ética brinda diversas ventajas, ya que muchos países poseen legislaciones avanzadas en esta materia, además de que se trata de estándares que han sido desarrollados por los sistemas regionales de protección de los derechos fundamentales.

Manifestamos nuestra disposición para seguir contribuyendo a la redacción del documento, sea a través de la clarificación de los puntos señalados o por medio de otras recomendaciones que forman parte del enfoque general que las organizaciones tienen sobre la implementación de estas tecnologías.

Atte.

Foro de la Sociedad Civil de la Red Iberoamericana de Protección de Datos