JOSÉ ALEJANDRO BERMÚDEZ

Director Regional para América Latina, Nymity.

Ex - Superintendente Delegado para la Protección de Datos Personales y uno de los promotores y redactores de la Ley General de Protección de Datos colombiana.

Durante este seminario se han discutido diferentes temas asociados a todas las posibilidades que hay en temas de recolección, cruce de interacción con la información. En ese sentido, el uso de la tecnología nos permite acumular y compartir múltiples datos personales. ¿Cuál diría usted que son las principales ventajas de estos procesos?

Yo creo que, en este tipo de encuentros, es muy importante destacar que uno de los elementos que siempre vemos es cómo los usos de información siempre van mucho más adelante de las normas sobre protección de datos personales, y en esa medida, es muy importante cuando se están diseñando los marcos regulatorios bien sean iberoamericanos, multilaterales o nacionales, que se piense siempre en términos tecnológicamente neutros y de manera que se pueda hacer un tratamiento de la información que tenga 2 componentes fundamentales, primero, un tratamiento de la información que sea benéfico para la sociedad en general, pero segundo, siempre teniendo en cuenta la protección de los derechos fundamentales de los titulares de la información, para eso hay que buscar mecanismos que hagan compatibles esos dos intereses aparentemente contradictorios.

¿Y cuál diría usted que son los princi-

pales riesgos que entrega, frente a esta acumulación de información?

Cuando se hacen más tratamientos de la información, en la medida en que las tecnologías se van desarrollando, lo que vemos es que es posible hacer más cosas con la información, es posible encontrar correlaciones entre los datos personales, entre bases de datos más estructuradas, y eso genera necesariamente, mayores riesgos para los titulares de la información. Si hay más riesgos para los titulares de la información, eso significa que las compañías, que las organizaciones y que los reguladores tienen que pensar en cómo establecer mecanismos objetivos de gobernanza dentro de las organizaciones, para efectos de proteger esos derechos de los titulares de la información.

Y pensando específicamente en el ejercicio de los derechos ARCO, de los derechos de acceso, rectificación, cancelación y oposición, ¿cómo diría usted que se pueden resguardar esos derechos?

Uno de los componentes fundamentales de los programas, o mejor, una de las mejores formas de proteger a los titulares de la información es estableciendo dentro de las compañías y de las organizaciones programas integrales de gestión de datos personales, dentro de los programas inte-

...el Estado tiene que ser doblemente cuidadoso, el Estado puede solamente hacer aquello que la ley le permite, a diferencia de los particulares que tienen un margen de acción un poquito más amplio, las entidades públicas ven limitada su actividad a sus funciones constitucionales y legales, y en esa medida el uso de la información tiene que ser doblemente cuidadoso para una entidad pública, pero, por supuesto, están dentro de sus posibilidades hacerlo, siempre y cuando sea responsable, siempre y cuando, igual que el sector privado, tenga mecanismos de gobernanza.

grales de gestión de datos personales, uno de los componentes fundamentales que tiene que establecer la organización son mecanismos de gobernanza; el segundo, tener políticas que describan sus compromisos en materias de tratamiento de datos personales; y tercero, mecanismos para solucionar potenciales conflictos que se generen con los titulares, esos mecanismos tienen que ser transparentes para los titulares y tienen que ser efectivos. De esa manera, se logra además, una eficiencia

adicional, que es evitar que esas quejas, que esas reclamaciones de los titulares, lleguen a las autoridades de protección de datos personales. Yo cuando estaba en mi rol de Superintendente de protección de datos, siempre le decía a las compañías: en la medida en que ustedes establezcan buenas prácticas de protección de datos, con procedimientos efectivos de resolución de quejas, lo que van a hacer es minimizar el número de quejas que le llegan a la autoridad de protección de datos, es más preventivo, se evitan que la autoridad conozca, o llegue a su conocimiento esa posible reclamación, y eso va a tener correlativamente una disminución del riesgo para la organización y para el titular.

¿Usted cree que se ha avanzado en buena medida en la discusión de los aspectos éticos de la protección de datos personales, o todavía nos falta?

Yo creo que esa es una discusión que se tiene que dar, yo creo que hay que dar el paso a pensar en términos estrictamente de cumplimiento legal, que ese es uno de los posibles enfoques de las compañías, hay compañías que se enfocan únicamente en sus obligaciones de *compliance*, y solamente hacen aquello que la ley les obliga, y hay compañías que van un paso más allá, establecen programas integrales que van un paso más allá del *compliance*, y eso supone pensar en los sucesos éticos de la información, entregar mecanismos para evaluar si los tratamientos de información se están haciendo de conformidad con parámetros éticos y de buenas prácticas, que

vayan más allá del simple *compliance*, que es suficiente para cumplir estrictamente con la ley, pero no es el estándar que debe adoptar una compañía que quiere hacer las cosas de la mejor manera posible.

¿Y pensando en el mundo público, ¿cómo ve usted la inserción del Estado en tema del Big Data? ¿Cree que hay muchas diferencias con el mundo privado? ¿Hay potencialidades?

Hay potencialidades para hacerlas en uno u otro mundo, el avance tecnológico ha hecho que no sean únicamente las grandes compañías quienes tienen la posibilidad de hacer usos de información basados en Big Data, pero por supuesto, cuando se trata del Estado haciendo cursos de información, el Estado tiene que ser doblemente cuidadoso, el Estado puede solamente hacer aquello que la ley le permite, a diferencia de los particulares que tienen un margen de acción un poquito más amplio, las entidades públicas ven limitada su actividad a sus funciones constitucionales y legales, y en esa medida el uso de la información tiene que ser doblemente cuidadoso para una entidad pública, pero, por supuesto, están dentro de sus posibilidades hacerlo, siempre y cuando sea responsable, siempre y cuando, igual que el sector privado, tenga mecanismos de gobernanza.

Para finalizar, hoy en día en Chile se está discutiendo una ley de protección de datos personales, ¿cuáles cree usted que son los principales elementos que debería contemplar esta regulación?

Yo creo que los avances recientes, tecnológicos, hacen necesario que se piense en términos flexibles en algunos aspectos, es decir, por ejemplo, en términos de legitimación del tratamiento, contemplar la posibilidad de tener bases legales diferentes del consentimiento, esto sin decir que el consentimiento haya dejado de ser importante, el consentimiento por cierto, sigue siendo un elemento legitimador importantísimo, pero hay otros elementos

...criterios como el interés legítimo del responsable, donde se haga un balance de intereses, creo que hay que pensar en esos términos, cómo flexibilizar algunos tratamientos de forma que respondan mejor a la realidad tecnológica de hoy en día, y lo segundo, que también está muy en línea con las guías revisadas de la OCDE, y ese es el punto donde apunta el nuevo reglamento europeo, por ejemplo, la implementación de medidas efectivas, por parte de los responsables y encontrar formas de demostrar la implementación de esas medidas efectivas, eso se llama el principio de responsabilidad demostrada...

que deben ser considerados, creo que el más importante que adicionalmente se incluye en los estándares iberoamericanos de protección de datos es acudir a criterios como el interés legítimo del responsable, donde se haga un balance de intereses, creo que hay que pensar en esos términos, cómo flexibilizar algunos tratamientos de forma que respondan mejor a la realidad tecnológica de hoy en día, y lo segundo, que también está muy en línea con las guías revisadas de la OCDE, y ese es el punto donde apunta el nuevo reglamento europeo, por ejemplo, la implementación de medidas efectivas, por

parte de los responsables y encontrar formas de demostrar la implementación de esas medidas efectivas, eso se llama el principio de responsabilidad demostrada, ya la tienen algunas legislaciones en América Latina, y es la manera más efectiva de proteger a los titulares de la información y en la misma medida, pedirle a los responsables en las compañías, mayor rendición de cuentas, que vayan más allá del *compliance* normativo y se comprometan con dar el paso más allá hacia la gestión integral de la protección de datos personales por medio de un programa.