ECIJA GPA
Av. 12 de Octubre N26-97 y Lincoln,
Ed. Torre 1492, 170516. Piso 10 Oficina 1005
Quito - Ecuador
Tel: (+593 2) 2986-528 /29/30
info.ecuador@ecija.com

Derecho a la protección de datos personales en las disposiciones emitidas por las autoridades públicas

Columna de Christian Espinosa Velarde y Jaime Dousdebés Costa, de nuestra área de TMT, Privacidad y Protección de Datos Personales de ECIJA GPA, para The Legal Industry Reviews Ecuador

El artículo 66 numeral 19 de la Constitución reconoce el derecho a la protección de datos personales de la siguiente forma:

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Del referido artículo no se deriva solamente una protección a este derecho, sino una reserva legal creada por mandato de la constitución y que implica que cualquier limitación a este derecho debe darse por una norma de carácter legal.

Luego, la Ley Orgánica de Protección de Datos Personales desarrolla el derecho a la protección de datos personales incorporado en el catálogo de derechos y establece las bases de legitimación que soportan el tratamiento de datos personales, pero si incluso la Superintendencia de Compañías, Seguros y Valores puede aludir el ejercicio de un poder público conferido a esta, de ninguna manera se elimina la obligatoriedad de las entidades del sector público de seguir los principios que se constituyen en reglas a seguir por cada entidad responsable del tratamiento de datos personales.

El Reglamento Sobre los Requisitos que Deben Contener el Nombramiento del Representante Legal y el Poder del Mandatario Mercantil de las Compañías, al ordenar la incorporación del código dactilar, está rebasando el desarrollo constitucional que hace la Ley Orgánica de Protección de Datos Personales, pues como ha quedado establecido anteriormente, la ley regula claramente el tratamiento de los datos, en base a varios principios entre los que destacan, para este caso particular, los de pertinencia y minimización de datos personales y proporcionalidad, mostrando un aparente tratamiento excesivo.

La misma ley incorpora una serie de elementos a considerar dentro de las prácticas de protección de datos personales, esenciales para el cumplimiento del principio de responsabilidad proactiva y demostrada, como lo es la protección de datos personales desde el diseño, misma que obliga a que al responsable del tratamiento a colocar la protección de datos personales en el centro de cualquier desarrollo de producto, servicio, o como es este caso, de una norma.

El tratamiento de datos personales, más allá de considerarse ya haberse definido como un derecho de los titulares, debe estar soportado en una relación de confianza entre el responsable del tratamiento y el titular, siendo que este último entrega al primero sus datos para usarlos para un fin determinado. La Superintendencia, al no transparentar la finalidad que persigue el uso del código dactilar, rompe ese voto de confianza, lo cual impide apreciar con claridad el cumplimiento de los principios de

pertinencia y minimización de datos personales, proporcionalidad y responsabilidad proactiva y demostrada, generando un inoportuno espacio para dudas.

En el mismo sentido, considerando el alto riesgo que puede preverse con la inclusión del código dactilar dentro del nombramiento de representante legal, al ser un dato que suele usarse como verificador para acceder a algunos servicios públicos que se gestionan de manera electrónica, la misma Superintendencia debió realizar una evaluación de impacto del tratamiento de este dato personal, para evaluar de manera anticipada cuáles podrían ser los potenciales riesgos a los que se encontrarían expuestos los datos personales de los titulares en función de la incorporación de este nuevo dato en un instrumento abierto a consulta pública, incluso desde sus propias plataformas.

Hay un deber y una responsabilidad clara de las autoridades, a las que les corresponde, antes de la emisión de una disposición que involucre datos personales, el realizar un análisis previo que le permita identificar si con esta no se está afectando a los titulares de datos o, de manera más clara, vulnerando su derecho constitucional.