Fundación
Karisma

11 de diciembre de 2017

Comisión de Regulación de Comunicaciones
Calle 59 A bis No. 5- 53
Edificio Link Siete Sesenta, Piso 9
Bogotá, Colombia

Asunto: ***Comentarios a la Resolución de la CRC sobre gestión de seguridad en redes de telecomunicaciones***

Fundación Karisma es una organización de la sociedad civil colombiana que busca responder a las amenazas y oportunidades que plantea la "tecnología para el desarrollo" al ejercicio de los derechos humanos, desde perspectivas que promuevan la libertad de expresión y las equidades de género y social. Trabajamos desde el activismo, incorporando múltiples miradas —legales y tecnológicas— en coaliciones con socios locales, regionales e internacionales.

En el marco del trabajo que adelantamos, hacemos seguimiento a las diferentes iniciativas de política pública del Gobierno colombiano. En esta línea, hemos hecho seguimiento a la política nacional de seguridad digital y ahora presentamos comentarios al proyecto de resolución para la gestión de la seguridad en redes de telecomunicaciones.

Comentarios generales

Globalmente, el proyecto de resolución de la Comisión de Regulación de Comunicaciones (CRC), que modifica el artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones, tiene por objetivo es imponer a los proveedores de redes y servicios de telecomunicaciones normas de gestión de seguridad digital y reporte de incidentes de "afectación significativa" al Estado. Este objetivo tiene sentido, pues los servicios de los operadores de comunicación son vitales para el funcionamiento del Estado y el país.

Sin embargo, la CRC tiene mejores prácticas de solicitud de comentarios que otras entidades del Gobierno en su sector. En particular, dar un plazo de 15 días hábiles (descontando festivos) para el análisis de un documento es más sensible que otras prácticas. Ahora bien, se pueden mejorar otras prácticas: pueden publicar el cronograma del proceso participativo, su metodología y acompañar el documento con un informe técnico que de cuenta del proceso que llevó a que la CRC produjera esta reglamentación —los modelos que usaron, los argumentos que los llevaron a tomar las elecciones que tomaron, etcétera—.

Desafortunadamente vimos este proceso muy tarde y no pudimos hacer un análisis más profundo, aún así presentamos acá la revisión que logramos realizar.

Si bién el texto menciona de manera general los “incidentes de seguridad”, está muy enfocado hacía la “integridad del servicio”. De hecho, suponemos que no se está haciendo un uso adecuado de la palabra “integridad”; en cambio, creemos que lo que se hace referencia en el texto es a la “disponibilidad del servicio”.

De acuerdo al estándar internacional ISO 27000, la seguridad de la información lo que busca es preservar la disponibilidad (propiedad de estar accesible y utilizable a pedido de una entidad autorizada de la información, en los horarios previstos), la confidencialidad (propiedad de que la información no esté disponible o sea divulgada a individuos, entidades o procesos no autorizados) y la integridad (cualidad de exactitud y exhaustividad de la información) de los datos.

En este sentido, creemos que la resolución debería tratar explícitamente estos tres temas y, en particular, la confidencialidad de la información de las personas que es recolectada, almacenada, procesada y transmitida por los proveedores de redes y servicios de telecomunicaciones. Incluso para este tema la definición (cf. tabla) de “afectación significativa" debería ser mucho más estricta en cuanto a la cantidad de personas afectados. Una fuga de datos personales que impacte 1000 personas, no cumpliría necesariamente con el criterio de 1% que establece el proyecto. No obstante, es un incidente grave que puede impactar fuertemente a las personas afectadas.

Se puede hacer un paralelo a lo que existe en la Unión Europea (UE) —Directiva n°2009/136/CE, artículo 3—, que establece los operadores de telecomunicaciones tiene la obligación de notificar a las autoridades de aquellos incidentes de seguridad en donde se ven comprometidos datos personales. Es de notar que en 2018, con la entrada en vigor del Reglamento 2016/679 sobre protección de datos artículo 33), la notificación se ha generalizado a otras entidades y sin que haya ningún criterio de porcentaje de personas afectadas. Solamente existe una obligación de notificación de las brechas de seguridad en donde se afectan datos personales.

Por lo tanto, reiteramos que nos parece fundamental complementar este proyecto de resolución, extendiendo explícitamente la obligación de notificación frente a pérdidas de integridad y de confidencialidad, en particular cuando hay involucrados datos personales. Debería adoptarse una aproximación similar a la europea en la que cualquier brecha de seguridad que comprometa datos personales debe ser notificada a las autoridades competentes del Estado, incluso si concierne a una sola persona.