LITORALPRESS

Fecha: 21-09-2020
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Actualidad
Título: Implementación del 5G representa un desafío de cara a proteger la privacidad de los datos personales

Pág. : 7
Cm2: 763,0
VPE: $ 10.022.543

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

ADVIERTEN MAYOR RIESGO DE UBICACIÓN EXACTA DE LAS PERSONAS:

Implementación del 5G representa un desafío de cara a proteger la privacidad de los datos personales

RAMÓN RIVERA NOTARIO

Especialistas señalan que la mayor cantidad de aparatos "inteligentes" y densidad de antenas que conlleva la nueva tecnología celular generará enormes cantidades de datos y facilitará la identificación de sus usuarios, algo para lo que la legislación debe prepararse.

La quinta generación de telefonía móvil, conocida como 5G, promete revolucionar las comunicaciones y alentar la conexión de gran cantidad de aparatos a internet, al ofrecer una mayor velocidad de transmisión de datos que las redes actuales, mayor densidad de conexiones y una menor latencia, todo lo que conlleva una mayor factibilidad de realizar acciones a distancia en tiempo real, facilitando, por ejemplo, la implementación de inteligencia artificial.

Pero existe una preocupación expresada por instituciones como la Agencia Española de Protección de Datos (AEPD) y Privacy Internacional, quienes advierten que las redes 5G podrían significar un mayor riesgo para la privacidad de los datos personales de quienes las usen.

Lo anterior, según la AEPD, ocurre —entre otras cosas— debido a que la adopción del 5G favorecerá la expansión del denominado Internet de las Cosas (IoT) —proliferación de aparatos "inteligentes" conectados a internet, muchas veces, sin mayor intervención del usuario—, que ya no necesitarán conectarse a un *wifi* doméstico para alcanzar buenas velocidades de descarga de datos, pudiendo hacerlo directamente al 5G. Esto generará también un aumento "exponencial" de la superficie de exposición a ciberataques, explica la AEPD, es decir, puntos de entrada para potenciales accesos no autorizados a redes y aparatos, que puedan producir brechas de información.

Juan Carlos Lara, director de Investigación y Políticas Públicas de Derechos Digitales, aclara que si bien "todas las formas de comunicación tienen riesgos", con el nuevo estándar tecnológico de las redes celulares 5G crecerán las amenazas a la privacidad "porque aumenta la cantidad y la precisión de la información que puede recogerse".

Además del IoT, "los riesgos a la privacidad se ven extendidos por el 5G porque aumenta el volumen de datos almacenados en cada estación de base (las antenas de las firmas proveedoras del servicio)", dice Jessica Matus, fundadora de Datos Protegidos y *of counsel* de Tecnologías en Ferrada Nehme.

La experta explica que "las amenazas a la privacidad se relacionan con el múltiple registro de los datos del usuario". Esto, ya que al incremento en el volumen de datos y el aumento del uso de la red por parte de los dispositivos, se suma el que estos "deben identificarse en más lugares y veces", ya que "las microceldas o estaciones base registran a los usuarios que pasan por su área de cobertura, incluso si no le dan permiso de geolocalización a sus *apps*".

Georreferenciación

La gestión de una mayor cantidad de datos facilita individualizar a las personas, indica Pedro Huichalaf, docente del Centro de Investigación en Ciberseguridad de la Universidad Mayor y exsubsecretario de Telecomunicaciones. Esto significa poder "definir sus perfiles y comportamientos, o su condición socioeconómica en base al precio de los dispositivos que use".

"Imagínate, drones que van a estar conectados entre sí para la seguridad pública, rastreando y sacando imágenes en forma constante. Cámaras interconectadas y dispositivos que posibilitan el rastreo de cosas y personas", ejemplifica Huichalaf.

Matus agrega que "es muy fácil inferir información de los usuarios, aun cuando estos decidan limitar qué datos y a quiénes se los entregan". Además, indica, existe con el 5G mayor "coparticipación" en el manejo de la información, porque "son más los operadores, fabricantes y proveedores que intervienen en el tratamiento de los datos y eso puede generar ambigüedad en la responsabilidad" sobre su uso adecuado y con respeto a la privacidad.

"Es posible que se recoja más información y más precisa", concuerda Lara, ya que "con el crecimiento del IoT, la existencia de más dispositivos conectados generará más información. Al usar frecuencias de transmisión más altas del espectro radiofónico, cada antena usada para el 5G tiene una menor cobertura. Eso significa que se necesitarán más antenas, por lo que se podrá identificar con más precisión la ubicación de cada usuario, explica la AEPD, con resoluciones de localización "inferiores a un metro".

No todos concuerdan. Christian Oberli, académico de Ingeniería Eléctrica de la UC y especialista en telecomunicaciones, considera que el cambio tecnológico no representa una mayor amenaza para la privacidad de la gente: "No me parece que haya un cambio relevante del 4G al 5G. Los operadores siempre han sabido dónde está cada uno".

Cuestión de legislación

"Más que un peligro, esto lo veo como un desafío", dice Huichalaf, ya que Chile debería adecuar su legislación para dificultar que la información que generará esta mayor conectividad no sea mal usada. "Una Ley de Datos Personales actualizada se está debatiendo en el Congreso, pero tomará tiempo", indica.

Lara emite un diagnóstico similar. "A Chile le falta preparación ante los riesgos de la seguridad de la información, ya que aunque hay una Política Nacional de Ciberseguridad robusta, su implementación está incompleta" y la protección de datos personales "es todavía deficiente".

Con todo, indica que la Subtel emitió en agosto una resolución que incorpora "aspectos clave de la ciberseguridad" para operadores de servicios de telecomunicaciones. Lo que está por verse, dice, es si estas y otras exigencias que se adopten serán, en la práctica fiscalizadas.

Sobre si la privacidad de los datos de los usuarios está siendo considerada en la implementación del 5G en Chile, Jozsef Markovits, jefe de la División Jurídica y encargado de Ciberseguridad de la Subsecretaría de Telecomunicaciones (Subtel), destaca que "el grupo internacional 3GPP ha establecido estándares de seguridad para las redes 5G, lo que ha sido incorporado al texto de las bases del concurso que se encuentra impulsando Subtel", y que dichas especificaciones "incluyen nuevos protocolos para, por ejemplo, cifrado autenticación y privacidad del usuario".

Fernando Saiz, director de Regulación y Asuntos Públicos de Movistar Chile, asegura que en la empresa se da un uso "ético y legal" de la información personal de sus clientes, "resguardando siempre su privacidad y anonimización". En ese sentido, también llama a implementar lo que denomina una "carta de derechos digitales", donde el mundo público y privado defina los derechos de las personas en el contexto digital, y la forma en que se asegurarían.

"Chile no está preparado para contrarrestar los riesgos en la implementación de 5G en materia de privacidad", sentencia Matus, ya que la evaluación del impacto de los marcos regulatorios sobre el derecho a la privacidad y la protección de datos debería ser realizada por una autoridad de datos distinta de entes como el Sernac y la Subtel, indica.

El 5G aumenta el volumen de datos almacenados en cada estación de base:las antenas de las firmas proveedoras del servicio.