EDITORIAL ASTREA

*Interceptación de comunicaciones**

Por Claudio Causarano

1. Introducción

El derecho a la intimidad o a la privacidad de las personas es un derecho moderno, que se originó con las primeras manifestaciones de los mass media, cuando la presión social sobre la esfera privada de las personas comenzó a verse alterada.

Es un derecho fundamental, sin el cual la persona quedaría reducida a nivel de objeto o cosa, pues brinda una protección jurídica al ámbito individual, conformado por ideología política, religiosa, costumbres, situación económica, orientación sexual, es decir, todo aquello que esté reservado a la vida normal del individuo.

Ello representa la libertad individual que hace que una persona tenga el derecho de controlarse a sí mismo y que se resguarde de las intromisiones de otras personas en su vida privada, que no vulneren áreas de su actividad que no estén destinadas o autorizadas a ser difundidas.

La violación a este derecho se establece cuando existe publicación, anuncio o se pone en conocimiento de terceros, elementos propios de la esfera privada de la persona que también incluye a las comunicaciones.

En muchos casos los gobiernos estiman necesario escuchar conversaciones telefónicas con el propósito de investigar el delito organizado, entonces, definir cuándo un gobierno tiene derecho a espiar las conversaciones de otros y cuándo no, puede resultar un tanto subjetivo, nadie considerará válido espiar a los rivales políticos, aunque sea una práctica frecuente en muchos países; pero sin lugar a dudas habrá consenso en la pertinencia de escuchar las conversaciones para identificar los próximos movimientos delictivos de quien pueda resultar ser un narcotraficante o terrorista.

Por ende, cuando en materia de comunicaciones se refiere a “interceptar”, es equivalente a hacerse con una comunicación, captarla, tomar conocimiento de la existencia, destino, contenido, aprehenderla de alguna manera, grabarla y reproducirla.

Para realizar una “interceptación de comunicación”, la misma deberá proceder únicamente con orden judicial, pues las comunicaciones en la República Argentina están protegidas por los Tratados Internacionales, por la Constitución Nacional, por la Ley de Telecomunicaciones, por la Ley de Inteligencia Nacional, por la Ley de Tecnologías de la Información y las Comunicaciones y por los principios rectores en materia de interceptación de la Corte Suprema de Justicia de la Nación.

Por último, el término “escuchas telefónicas”, debe utilizarse cuando ésta se realiza como una práctica ilegal, es decir, sin autorización judicial y el fruto de ello carece de legalidad como medio probatorio, sería pues, una prueba viciada, ésta se distingue de la “interceptación”, que es técnicamente y legalmente realizada con autorización judicial y cuya prueba es considerada válida.

---

* Bibliografía recomendada.

2. Inviolabilidad de las comunicaciones

La convergencia entre los distintos sistemas de comunicaciones que existen en la actualidad, permite la interactividad de la información entre los usuarios, llegando de esta manera a las sociedades de la información, donde los mercados se vuelven cada vez más competitivos.

Los avances tecnológicos en materia de comunicaciones, también son aprovechados por personas con fines delictivos para atentar contra la sociedad, los gobiernos y los valores democráticos, donde el nuevo entorno de seguridad es cada vez más abierto y sin fronteras, por lo tanto, las nuevas amenazas se caracterizan por ser asimétricas, multidimensionales, difíciles de predecir y afectan a la seguridad pública de un Estado.

Es por estos y otros motivos, que los gobiernos recurren a la medida de interceptación de comunicaciones como método de investigación procesal y prueba en el proceso penal para la investigación de delitos complejos, pero también prevén en su legislación la privacidad de las comunicaciones.

En la República Argentina, la Ley de Telecomunicaciones 19.798 y más precisamente en sus arts. 18 y 19, expresa que la correspondencia de telecomunicaciones es inviolable y su interceptación solo procede a requerimiento judicial, siendo el término “correspondencia” en esta materia, toda comunicación establecida entre dos puntos o extremos mediante un proceso de doble vía de comunicación o también “una comunicación de ideas, sentimientos, propósitos o noticias enviadas por correo oficial o particular, por un remitente a un destinatario. Es decir, de elementos netamente inmateriales que una persona hace a otra por un medio apto para fijar, transmitir o recibir la expresión del pensamiento” (CNCasPen, Sala II, 29/8/96, Registro 1049, causa 781).

También en la ley de las TIC’s 27.078, se garantiza a los usuarios la confidencialidad de los mensajes transmitidos y el secreto de las comunicaciones.

Por otra parte, en la Ley de Inteligencia Nacional 25.520, está previsto el tema en tratamiento en su Título VI, art. 18 y ss., con especificación de procedimientos, autorizaciones, plazos procesales, etcétera.

Por último, la CSJN como cabeza del Poder Judicial de la Nación y como supremo custodio y último garante del goce de las garantías individuales, expresa en su acordada 17/2019, todo lo referente a los derechos de la privacidad e intimidad como así también a la interceptación de comunicaciones que solo puede ser dispuesta por orden judicial en el marco de un proceso penal en curso.

3. Derecho comparado en la interceptación de comunicaciones

La interceptación de comunicaciones se realiza mediante una orden judicial que corresponde a la investigación procesal y limita el derecho al secreto de las comunicaciones con el objetivo de reunir las pruebas necesarias para confirmar la vinculación o desvinculación de una persona en un proceso determinado por la comisión de un delito.

Esta medida utilizada por el gobierno, afecta a los derechos fundamentales que amparan las normativas de los distintos países, por ende, se debe buscar el equilibrio entre el derecho a la privacidad con raigambre constitucional y la interceptación permitida en el proceso penal, cuya finalidad es evitar una intromisión ilegal.

En la República Argentina, la medida se realiza mediante el art. 236 del Código Procesal Penal, por su parte en la legislación de Italia, sólo puede ser ordenada por una autoridad judicial en la parte investigativa del Codice di Procedura Penale, arts. 266 al 271, siempre y cuando exista un indicio grave de culpabilidad del investigado.

En España se realiza mediante el art. 579 de la Ley de Enjuiciamiento Criminal, en cuanto a Francia, luego de la modificación del Código Penal francés en 1991, el juez puede ordenar la interceptación mediante la aplicación de los arts. 100 al 100-7 y en su vecino país de Alemania, cuando existen factores de sospecha de que una persona fue el autor, instigador o partícipe de un delito grave, tiene previsto en su Código Procesal Penal la orden de interceptación en los arts. 100a al f y 101.

En todos los casos la medida requiere un auto fundado sin consentimiento de los afectados y puede ser grabada, reproducida y adjuntada a la causa.

Por último, en los Estados Unidos, la interceptación se realiza mediante la Ley Ómnibus de Control del Crimen y Calles Seguras, también con la Ley de Vigilancia de Inteligencia Extranjera (FISA) y con la Ley Patriótica o Patriot Act.

4. E2EE vs. interceptación de comunicaciones y seguridad pública

Para determinar la autoría de hechos delictivos como terrorismo, estafas, trata, narcotráfico, venta ilegal de órganos y armas entre otros, las instituciones encargadas del mantenimiento de la seguridad pública requerían con más frecuencia la interceptación de comunicaciones como medida fundamental para la investigación en el proceso penal.

Ello cobró notoriedad en muchos medios periodísticos, por lo que los usuarios vieron comprometida su privacidad y comenzaron a solicitar comunicaciones más seguras.

Fue entonces cuando los dispositivos electrónicos para comunicaciones comenzaron a fabricarse en base a la criptografía moderna y los desarrolladores de las aplicaciones de mensajería instantánea y redes sociales, elevaron el nivel de seguridad con la robustez de las claves de cifrado para evitar que las comunicaciones sean vulneradas por los gobiernos, sin advertir, que las mismas también serían utilizadas por terroristas fundamentalistas, ciberdelincuentes, narcotraficantes y otros.

Es por ello, que hubo un punto de inflexión entre la privacidad de los usuarios, las empresas de tecnología y las investigaciones policiales solicitadas por la justicia, ya que las comunicaciones encriptadas E2EE llegaron a la sociedad para quedarse.

Las profundas y exhaustivas investigaciones policiales después de los delitos o atentados, determinaban que los terroristas, por ejemplo, reclutaban combatientes extranjeros o lobos solitarios que utilizaban tecnología de encriptación avanzaba a través de sitios de redes sociales de acceso público y otras en la innumerable cantidad de plataformas de mensajería privada que figuran en la web, aunque la participación

tecnológica no se circunscribía a eso solamente, falta otro elemento esencial y eso era “Internet”.

Entonces, existe una dicotomía entre las Agencias de Inteligencia y las Fuerzas de Seguridad junto a la Justicia, porque ellos no están interesados en el ciudadano promedio de un país para escuchar su conversación, sino en aquellos que cometen delitos, utilizando éstos y otros medios.

Todo lo expuesto anteriormente es lo que ha enfrentado en los últimos años a los gobiernos con las empresas desarrolladoras y con los fabricantes de dispositivos móviles para solicitar en las comunicaciones E2EE una “Backdoor” para interceptación de uso exclusivo de las FF.SS. y la justicia, conflicto que actualmente continúa.

5. Vigilancia en redes sociales

La evolución de la tecnología aplicada a las telecomunicaciones, fue sin lugar a dudas una pieza clave en el punto de inflexión más importante de las últimas décadas de la nueva era digital donde se vislumbraba nuevos servicios en la nube.

Como consecuencia de ello, trajo aparejado un aumento de la capacidad de la red para transmitir en tiempo real el desarrollo de las nuevas aplicaciones digitales, es así como las empresas de telecomunicaciones y los fabricantes de equipos trabajaron en la unificación de un entorno de interconexión de productos y servicios estandarizado e interoperable, a los que luego se sumaron los desarrolladores de aplicaciones.

Las nuevas plataformas digitales dependían de la conectividad a la red que era cada vez más rápida y segura, donde poco a poco fue encontrando su lugar el Wi-Fi, teniendo un especial cuidado en la privacidad de la transmisión de los datos de los usuarios, la que a esta altura de los acontecimientos ya se había filtrado transversalmente en la vida de las personas de todos los estratos sociales, incluido a edades tempranas mediante la educación y el esparcimiento.

Esta nueva era digital del conocimiento, se puede medir, supervisar, determinar el comportamiento humano, saber cómo vive parte de una población, la cantidad de personas que hay en un determinado radio con sus mismos gustos, hobbies, profesión, estilo de vida, nivel de gastos e incluso mapear sus relaciones con tan solo presionar una tecla.

La tecnología sigue evolucionando y le está presentando a la sociedad una nueva forma de ver la realidad, de vivir, de pensar y de prepararse para un futuro en donde el debate entre la seguridad y la libertad se instala con más fuerza en la sociedad, pues sigue latente la preocupación por la vulneración de la privacidad de sus comunicaciones por parte de los gobiernos que tienen la mirada puesta en los ciberdelincuentes.

Es por ello que la vigilancia masiva de las comunicaciones en las redes sociales, fue abordada desde muy temprano por los servicios de inteligencia de las potencias mundiales con el lema “En nombre de la seguridad nacional”.

Las legislaciones vigentes de algunos países, van detrás de estos acontecimientos, pero muchas veces también son los mismos gobiernos los que incumplen o violan los derechos y las libertades civiles.

6. Agresiones en redes sociales: Italia

Con el advenimiento de la internet hacia fines de la década del 60 y ya implementándose en forma comercial en la siguiente década, se fue vislumbrando el impacto que ésta en conjunto con las Tecnologías de la Información y la Comunicación, le darían a la sociedad mundial un desarrollo en todas las áreas, transformándose en décadas posteriores en la Era Digital.

El desarrollo de las primeras redes sociales en 2002 fue el otro hito que marcó un nuevo rumbo en las comunicaciones sociales y que sigue creciendo en forma vertiginosa. Para el 2016, Telegram, Twitter, Instagram, We Chat, Facebook Messenger, WhatsApp, Facebook y otras, tuvieron entre 100 millones de usuarios (Telegram) a 1500 millones (Facebook).

Pero sin lugar a dudas la red social elegida por excelencia a nivel mundial fue WhatsApp cuando en 2016 implementó en sus comunicaciones la criptografía Curve25519, AES-256 y HMAC- SHA256 todas ellas con propiedades matemáticas modernas y avanzadas, que hicieron de las comunicaciones de esta red social la más segura de todas pues ahora era una comunicación E2EE de extremo a extremo.

Esto hizo que en ese mismo año la cantidad de usuarios creciera exponencialmente en millones alrededor del mundo, para luego caer en 2021 cuando los nuevos términos y condiciones legales indicarían que ciertos datos de los usuarios quedarían a resguardo de la empresa, sin saber el usuario que destino podían tener sus datos personales por lo que dejaba de ser tan anónima como lo era al principio.

Por este motivo, sus clientes migraron en forma masiva a Telegram que también tenía las comunicaciones encriptadas mediante la criptografía ECDH, AES-256 y RSA-2048, de similares características, pero no E2EE, sino una encriptación parcial, aunque al menos seguía ofreciendo el anonimato en el inicio de la registración.

Estas y otras plataformas de redes sociales, basadas en complejos algoritmos matemáticos, les permitieron a los millones de usuarios publicar cualquier tipo de contenido donde circula casi en forma instantánea por todo el mundo.

Pero, así como en los medios periodísticos hay noticias falsas, en la actualidad, siempre y cuando haya conectividad a internet, los desarrolladores de las plataformas digitales descubrieron que los usuarios tenían una puerta abierta a nuevos medios de comunicación que no les generaba ninguna responsabilidad y que podían expresar lo que quisieran. De hecho, los clientes comenzaron a enfatizar el contenido de sus publicaciones, en los videos, en los comentarios, llegando a generar discursos de odio, difamación, etc., que se hacían virales en las redes generando un debate público.

La manipulación de la información, el desprestigio, la propaganda maliciosa, los contenidos falsos o “Fake News”, los agresivos, etc., en definitiva, era una acción violenta que realiza una o varias personas con la intención de causar un daño a otra donde esto no estaba previsto ni pensado por los desarrolladores, por ende, éstos iniciaron un proceso de moderación post hoc para que el material de odio, violento o falso sea marcado, revisado y finalmente eliminado.

Más allá de lo expuesto, ese daño psicológico a la persona ya se había producido y en estos términos la justicia italiana actuó rápidamente cuando los usuarios

expresaron en sus demandas una reparación por el daño sufrido, entre otras solicitudes.

Es así que un empleado de una empresa realizó la creación de un grupo de WhatsApp para ofender o denigrar al empleador, provocando una disminución de su poder y autoridad. Eso fue causal de despido para el creador del grupo y de sus colegas que fueron despedidos también mediante la misma red social (Tribunal de Milán, Sección Laboral, sentencia del 30/5/17).

También cuando la crítica, expresada en publicaciones en redes sociales, muestra un evidente desprecio hacia la empresa, los administradores, representantes y potenciales socios de la misma, va más allá, cruzando la frontera, hasta el punto de la difamación (sentencia del Juzgado de Busto Arsizio n° 62 del 19/2/18).

Es importante destacar, que cuando una persona ocupa un cargo o posee una responsabilidad mayor que la de un empleado, lo que escriba en una red social también tiene un peso mayor, esto ocurrió con un empleado sindical en donde sus expresiones no son evaluadas como las de un empleado común, sino que el sindicalista tiene un derecho de crítica diferente o superior al de otros empleados (Tribunal de Milán, sentencia n° 3153 del 28/11/17).

Vale recordar, que el delito de “difamación” se ubica en el Código Penal italiano, art. 595 y es uno de los tantos delitos que se producen en las redes sociales. Si bien el art. 21 de la Constitución Italiana garantiza el derecho de la libertad de expresión, es obvio que esto tiene un límite cuando se daña el honor de un tercero.

Específicamente, la difamación en línea, puede tener dos variantes, ya sea por medio de la prensa digital, la prensa escrita, radio y televisión o en los distintos medios posibles por internet, ya que queda representado por el propio art. 595 del Código Penal cuando dice “o por cualquier otro medio de publicidad”, teniendo en cuenta que internet es el otro medio de publicidad por el cual una difamación puede llegar a más personas.

Ello es interesante, porque en esta nueva Era Digital, los distintos tipos de comunicaciones que existen incluido internet, hace que cada vez haya más casos de delitos e incluso transfronterizo, como sucedió en una difamación contra un ciudadano italiano con residencia en Italia utilizando el correo electrónico.