UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO

Anuario de Derechos Humanos 2005

Centro de Derechos Humanos

Sobre la Inviolabilidad de las Comunicaciones Electrónicas

Ley N°19.927 que Tipifica los Delitos de Pornografía Infantil

Daniel Álvarez Valenzuela*
Alberto Cerda Silva**

I. Introducción: Reseña de la Ley N°19.927

La intensificación en el uso de nuevas tecnologías, como ya apuntaba Frossini a mediados de la década de los sesenta, ha abierto una serie de interrogantes respecto a cómo el Derecho debe enfrentar las situaciones o conflictos que el desarrollo tecnológico genera, las que el legislador ha procurado resolver –con la dilación propia, cabe señalar– mediante el dictado de nuevos cuerpos legales o la modificación de los ya existentes.

El caso de la pornografía infantil es un buen ejemplo de esta situación: hasta antes de la promulgación de la Ley N°19.927, la persecución de los ilícitos de producción y distribución de material pornográfico infantil resultaba particularmente difícil de realizar, debido a la falta de normas penales específicas que sancionaran este tipo de conductas, sumada a la deficiente determinación de las facultades legales para llevar a cabo las diligencias de investigación, en especial cuando tales conductas se verificaban por medios electrónicos o digitales.

En efecto, con la publicación, el pasado 12 de enero de 2004, de la Ley N°19.927 que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil, se ha pretendido, según consigna el mensaje legislativo: i) sancionar como delito la distribución, difusión, transmisión, importación y exportación de pornografía infantil; ii) aumentar las penas aplicables a quienes participan en estos delitos; y, iii) establecer normas de procedimiento que otorguen facultades especiales a fiscales del Ministerio Público, jueces y agentes policiales para investigar y acreditar estos ilícitos.

II. Retención de Comunicaciones Electrónicas

De las normas sustantivas y procesales introducidas por la ley en examen, sin desmerecer la importancia de sus diversos contenidos, parece oportuno detenerse particularmente en aquellas que se refieren a la intervención y retención de comunicaciones electrónicas, incluidas por el legislador atendiendo al hecho de que la distribución, difusión y/o transmisión de pornografía infantil se realiza preferentemente a través de redes como Internet[1].

* Investigador, Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile.

** Profesor Asistente de Derecho Informático, Facultad de Derecho, Universidad de Chile.

[1] De hecho, la premura de la tramitación legislativa se debió al descubrimiento por parte de las policías de importantes redes de comercialización de pornografía infantil que operaban en Internet desde Chile.

Este comentario, junto con el documento principal a que se refiere, están disponibles en formato digital en www.anuariocdh.uchile.cl

En concreto, el artículo 2° N°2 de la ley otorga las facultades especiales a los tribunales que investigan estos delitos, para interceptar y/o grabar todo tipo de telecomunicaciones. Tratándose de comunicaciones electrónicas, la ley establece dos obligaciones especiales para las personas naturales o jurídicas que hacen las veces de Proveedores de Servicios Internet ("ISP" por sus siglas en inglés) a saber: la creación de un registro de rango de las direcciones IP utilizadas en la prestación de los servicios; y, la mantención de un registro de las conexiones que realicen sus abonados por un período no inferior a 6 meses[2].

En el caso de la primera obligación, se trata de un listado de las direcciones IP utilizadas por el ISP. Por ejemplo, la Universidad de Chile (que para estos efectos cumple las funciones propias de un ISP) utiliza el rango IP que va desde el 146.83.12.0 hasta el 146.83.16.0. De esta manera, conforme a la ley, la Universidad está obligada a mantener un registro con esta información actualizada, el cual debe estar disponible permanentemente para el Ministerio Público o los tribunales.

Por lo que toca al registro de conexiones, éste consiste básicamente en un sistema computacional que deja constancia automática de ciertas operaciones que realiza un usuario en Internet, información que es almacenada en los equipos e instalaciones del ISP; usualmente el registro consigna la dirección IP utilizada por el usuario –la cual es asignada por el ISP–, la hora de conexión y la hora de desconexión de la red. De esta manera, su procesamiento posterior permite localizar o identificar el computador desde el cual se realizó una determinada operación en Internet, funcionando de manera similar al sistema de control de llamadas que las compañías telefónicas utilizan para efectos de facturación.

Hasta aquí no hay nada digno de reproche ni amenaza alguna.

Sin embargo, el registro de conexiones no sólo almacena la información antes mencionada, sino que, además, permite registrar el tráfico realizado por el usuario mientras estuvo conectado a Internet. En otras palabras, hace técnicamente factible establecer no sólo entre qué horas y desde dónde se estuvo conectado, sino que registra los sitios que se visitó, los correos electrónicos leídos, con quienes se chateó, etc., siendo estas prácticas objeto de abundantes críticas en el derecho comparado, por cuanto su concreción implicaría la violación de importantes garantías fundamentales.

Esta situación ha motivado arduos debates en el derecho comparado, los que llaman a la cautela de los legisladores al momento de establecer la obligación legal de registro de conexiones electrónicas. Así, por ejemplo, ha sucedido con ocasión de la discusión que precedió a la adopción del Convenio del Cibercrimen por los Estados miembros del Consejo de Europa y terceros Estados, suscrita en Budapest en noviembre de 2001, que decantó en una definición normativa de "datos de tráfico", esto es, aquéllos necesarios para identificar las comunicaciones electrónicas, a saber la información

[2] La dirección IP es un identificador de recursos en línea, que permite la individualización de los computadores desde donde se accede a la red, mediante un código numérico único estructurado conforme a una norma técnica estándar.

sobre origen, destino, hora, ruta, tamaño y duración de éstas, excluyéndose expresamente cualquier información relativa al contenido de las mismas.

Lamentablemente, nuestro legislador no tuvo igual celo al momento de establecer el alcance de la obligación en comento, por lo cual es posible que su implementación se preste a abusos, con el consiguiente menoscabo a libertades y derechos fundamentales, como veremos más adelante.

III. Inviolabilidad de las Comunicaciones Privadas

El derecho a la inviolabilidad de las comunicaciones privadas puede ser definido como aquella derivación y concreción del derecho a la vida privada, en virtud del cual se prohíbe a los poderes del Estado y a los particulares, la captación, interceptación, grabación y/o reproducción ilegal de una comunicación privada. Es un derecho fundamental, de carácter civil y político, cuyo fundamento último es la dignidad de la persona humana, siendo por ello necesario su reconocimiento normativo y el establecimiento de normas sustantivas de protección que sancionen su vulneración.

El tramado normativo que configura en nuestro ordenamiento el derecho a la inviolabilidad de las comunicaciones privadas, está compuesto tanto por normas de rango constitucional como por disposiciones incluidas en diversos tratados internacionales sobre derechos humanos, suscritos y ratificados por Chile, los que en su conjunto tienen la fuerza normativa de límites a la soberanía del Estado y que conforman, al decir de Humberto Nogueira, un verdadero bloque constitucional de derechos fundamentales.

Así, el artículo 19 N° 5 de la Constitución Política de la República de Chile (en adelante "la Constitución") asegura a todas las personas "la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley". Mientras, lo propio hace el artículo 11 del Pacto de San José de Costa Rica, al disponer que "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". Y, en exactamente iguales términos, se expresa el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

Como podemos observar, el derecho a la inviolabilidad de las comunicaciones privadas reconocido en la Constitución difiere en su formulación respecto de las normas de los acuerdos internacionales citados, toda vez que contiene elementos de neutralidad tecnológica que le permiten ampliar su campo de aplicación, no limitándose al elemento "correspondencia" utilizado por estos últimos, el cual podría ser objeto de interpretaciones inapropiadamente restrictivas.

En efecto, tanto el Pacto de San José de Costa Rica como el Pacto Internacional de Derechos Civiles y Políticos son instrumentos internacionales creados a mediados del siglo XX, momento histórico donde el grueso de las comunicaciones era realizado por medios epistolares y telegráficos, ambos comprendidos dentro del concepto de "correspondencia" utilizado en ellos, el cual -conforme a la definición del Diccionario de la Real Academia de la Lengua Española- se refiere al "conjunto de cartas que se reciben o expiden", entendiendo a su vez por carta al "papel escrito y ordinariamente cerrado, que una persona envía a otra para comunicarse con ella". No obstante, en ambas definiciones el elemento central subyacente es la comunicación, siendo la correspondencia y/o la carta sólo uno de los múltiples medios por el cual dicha comunicación se materializa.

No debemos olvidar que la protección que le brindan los instrumentos internacionales sobre derechos humanos a la correspondencia es una especificidad dentro de la protección otorgada a la vida privada de toda persona, lo cual, conforme a la interpretación extensiva que debe hacerse de los derechos y libertades fundamentales, nos permite sostener que la protección se refiere a la comunicación en sí misma, prescindiendo del medio por el cual se verifique.

Este razonamiento es similar al que llevó a los redactores de la Constitución a configurar la garantía de la manera en que lo hicieron: prescindieron absolutamente del medio o soporte por el cual se realice la comunicación. Su preocupación fue proteger las comunicaciones en sí mismas, su contenido más que su forma, el acto humano de comunicar.

De lo anterior, quedó constancia expresa en las actas de la Comisión de Estudios de la Nueva Constitución; en la ocasión en que fue discutida la norma del numeral 5 del artículo 19 de la Constitución, se expresó que "la redacción del texto tiende a cubrir toda forma de correspondencia, o sea, toda forma de comunicación espiritual y material entre dos individuos proyectado el uno hacia el otro, por cualquier medio que esté dentro de las posibilidades técnicas del país y de la sociedad de que se trata (...) la idea es la comunicación privada: puede ser telefónica, telegráfica, epistolar o por otras formas que todavía no se conocen (...) y, al decir 'privadas' el concepto se circunscribe obviamente a las comunicaciones que no son públicas, porque en las comunicaciones públicas no hay inviolabilidad".

Como vemos, no se trata de que cualquier acto de comunicación sea protegido por el Constituyente; se trata de un tipo de comunicación específica: la comunicación privada. Esta es, según el Diccionario de la Real Academia, aquella "que se ejecuta a vista de pocos, familiar y domésticamente, sin formalidad alguna ni ceremonia alguna. Particular y personal de cada uno". En tanto, particular es entendido como aquello que no es público. En consecuencia, cuando hablamos de comunicación privada, estamos hablando de una comunicación

verbal, escrita o por medio de señas, que tiene un carácter personal, que no es pública, en la que se proyecta la intimidad de una persona hacia un otro (que puede ser una o varias personas), que ha sido escogido de manera singular por el emisor y donde no importa la forma o el medio por el cual se materialice la comunicación.

En conclusión, para que una comunicación sea objeto de protección bajo el bloque constitucional de derechos humanos conformado por la garantía contenida en el numeral 5 del artículo 19 de la Constitución y por las normas pertinentes de los instrumentos internacionales antes mencionados, es necesario que: i) sea una acción comunicativa entre personas, y, ii) sea un acto no público, entre personas determinadas o determinables.

Bajo esta interpretación, las principales comunicaciones entre personas que se realizan por medios electrónicos están ampliamente garantizadas constitucionalmente. Así, el correo electrónico, los sistemas de mensajería instantánea, la telefonía IP, etc., gozan de protección constitucional y penal en tanto su interceptación, registro o grabación ilegítima se encuentran prohibidas y penadas por la ley[3] .

IV. Observaciones a la Ley

Como hemos visto, la garantía constitucional cubre o se extiende a cualquier tipo de comunicación privada, no importando el medio por el cual se realice, por cuanto no protege formas o medios específicos, sino que el objeto protegido es el contenido de la comunicación: el diálogo espiritual y material entre individuos determinados, que interactúan socialmente.

Siendo la interpretación precedente adecuada, cabe examinar si las normas de la Ley en comento constituyen o no una restricción legítima del derecho fundamental.

A diferencia de lo dispuesto en el Convenio del Cibercrimen, los vagos e imprecisos términos de redacción de la disposición en análisis dados por la Ley 19.927, dan pie a que en su aplicación práctica por los prestadores de servicio de Internet, éstos menoscaben o pongan en riesgo la garantía a la inviolabilidad de las comunicaciones privadas, al registrarse más información que la estrictamente necesaria para identificar a un usuario de Internet.

Del mismo modo, una interpretación extensiva de la disposición faculta al Ministerio Público para acceder a cúmulos de información sin precedentes, sin necesidad de disponer de autorización judicial; ello contraría la pretensión de la propia reforma procesal penal, que al instituir los Juzgados de Garantía procura poner freno a los excesos a los que haya lugar con motivo de la investigación criminal. Más aún, un registro de tal naturaleza constituye una verdadera interceptación de comunicaciones electrónicas anticipada, que por aplicación del principio de inocencia y atendida la ilicitud de los

[3] Sólo por mencionar algunas de las normas penales aplicables: el artículo 161 A del Código Penal sanciona al que "por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado", siendo un tipo especial de mera actividad ya que no exige elementos subjetivos como dolo o malicia en el actuar; y, el artículo 36 B de la Ley General de Telecomunicaciones, que tipifica como delito la interferencia, intercepción o interrupción de un servicio de telecomunicaciones de aquellos que regula la Ley, siendo Internet uno de ellos, según definición expresa de la autoridad competente.

medios de prueba obtenidos con infracción de derechos fundamentales, no debía ser legitimada siquiera retrospectivamente.

La decisión legislativa de crear un registro de comunicaciones electrónicas en la forma establecida por la Ley, ha requerido de mayor acuciosidad en la determinación del alcance de las obligaciones que pesan sobre los prestadores de servicio de Internet, más cuando –tal como se sostiene en los Principios rectores para la reglamentación de los ficheros computarizados de datos personales, adoptados por la Asamblea General de Naciones Unidas, en diciembre de 1990– la entidad de los intereses en juego demanda intervención legal, vedando el desarrollo normativo por la vía reglamentaria.

Se trata, por consiguiente, de fijar un adecuado equilibrio entre, por un lado, el legítimo interés público por reprimir conductas delictivas y, por otro lado, el igualmente legítimo resguardo de las libertades y derechos fundamentales. Al efecto, es recomendable exigir del legislativo una mayor precisión en torno a los datos susceptibles de ser almacenados en el cumplimiento de la obligación de registro por los ISPs, circunscribiendo la misma, tal cual hace el Convenio sobre Cibercrimen, tan solo a los datos que permitan determinar el origen y destino de las comunicaciones –esto es, dirección IP, con precisión de día y hora de conexión–; solicitar más información que la apuntada importaría un menoscabo a los derechos fundamentales de quienes somos usuarios de Internet.