Investigación de delitos vinculados a la pornografía infantil. Derecho a la privacidad e Internet

TEDH, *Case of Benedik vs. Slovenia*, 24 de abril de 2018

Por Javier Teodoro Álvarez[1]

1. Introducción

La irrupción de Internet, y su posterior masificación, generó un crecimiento exponencial del tráfico de imágenes y videos de abusos sexuales infantiles sin precedente alguno.

La universalidad del medio y su aptitud para relacionar a millones de personas en todo el mundo, como también, los bajos costos para su producción –en particular con la aparición de las cámaras digitales y los teléfonos móviles inteligentes– y la inmediatez en el acceso son diversas circunstancias que abonan a que se trate de un fenómeno delictivo de alcance global y, especialmente, de difícil persecución.

En ese sentido, uno de los principales obstáculos para investigar los delitos relacionados con la producción y tráfico de este material reposa en las posibilidades que el actual estado de la tecnología permite para garantizar la intimidad de quienes navegan en Internet. El desafío, entonces, se encuentra en delimitar los márgenes de la persecución estatal frente al derecho a la privacidad en la actual era digital.

1 Abogado (UBA). Especialista y Magíster en Derecho Penal (UTDT). Profesor de Derecho Penal y Procesal Penal (UBA, UAI). Profesor de "Delitos Contra la Integridad Sexual" (UBA). Funcionario de la Procuración General de la Nación.

En líneas generales, una investigación estándar vinculada a estos delitos comienza con la identificación de lo que se conoce como valor *hash,* o sea, la clave o combinación alfanumérica que permite identificar un archivo digital con independencia del nombre que cada usuario le asigne.

El rastreo de este dato suele estar en manos de las divisiones policiales específicas encargadas de la ciberdelincuencia en distintos países, las que albergan bases de datos de archivos de pornografía infantil con los valores *hash* de cada uno de ellos. Este código es un dato público, por lo que su rastreo y búsqueda no requiere autorización judicial alguna.

El paso siguiente será la verificación de las descargas del mismo en Internet lo que permitirá conocer las direcciones IP que están compartiendo el archivo, como también la fecha y la hora.

El número de IP –*Internet Protocol*– es un número que identifica, de manera lógica y jerárquica, una conexión de un dispositivo a Internet. Existe una IP fija, asignada para siempre a cada usuario y otra dinámica, que varía en función de cada conexión.

Una vez que se revela la dirección IP, la hora y la fecha de conexión en la cual se intercambió el archivo cuyo valor *hash* refiere a materiales de pornografía infantil, será el momento de establecer la titularidad del servicio de Internet mediante el cual se utilizó esa dirección IP dinámica.

Así, se solicitará mediante oficio a la compañía prestadora del servicio que indique a quién corresponden esas direcciones IP según su número, día y hora de conexión detectada.

El paso siguiente será proceder al allanamiento del domicilio de esa persona con el propósito de incautar los dispositivos electrónicos, como también de resguardar toda evidencia digital para su posterior análisis pericial.

Está claro que el registro domiciliario requiere de una orden judicial que lo autorice con los alcances y exigencias que la propia ley procesal impone. La discusión, sin embargo, radica sobre la dirección IP y la información que esta permite obtener.

Así, el debate central se ubica en definir si las direcciones IP son datos públicos y, por ende, no alcanzados por el derecho a la privacidad o, por el contrario, si se refieren a información que solo puede ser revelada por orden judicial. Las posturas suelen ser encontradas.[2]

A modo de ejemplo, y con el propósito de ilustrar la discusión, es interesante examinar, por un lado, la tesis del Tribunal Supremo de España, que expresó:

> Los rastros que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (*internet protocols*) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa autorización judicial para conseguir lo que es público y el pro-

2 Ver Álvarez, J. T. (2018). *Delitos sexuales. Coerción sexual e internet.* Buenos Aires: Ediciones DyD.

> pio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada –como puntualiza con razón el Ministerio Público– queda registrada siempre y ello lo sabe el usuario.[3]

Por su parte, el Tribunal de Justicia de la Unión Europea, en oportunidad de analizar el alcance del concepto "datos personales" en razón del artículo 2 (a) de la Directiva de Protección de Datos, en una sentencia de 24 de noviembre de 2011 afirmó que las direcciones IP de los usuarios eran datos personales protegidos porque permiten que esos usuarios sean identificados con precisión.[4]

El Tribunal Europeo de Derechos Humanos (en adelante, TEDH) tuvo oportunidad de resolver esta controversia en el caso *Benedik vs. Slovenia* del 24 de abril de 2018. Allí definió el alcance del derecho a la privacidad en relación a la identificación de una persona a través de la dirección IP dinámica por la que se conectaba a Internet para la comisión de delitos vinculados a la pornografía infantil.

2. Antecedentes del caso

2.1. Los hechos

En el año 2006, la policía suiza realizó una serie de monitoreos sobre los usuarios del servidor *Razorback*, red habitualmente utilizada en *software* de intercambio de archivos a través del sistema p2p.

Se trata de un método que permite que diversos usuarios compartan archivos digitales entre sí abreviando los tiempos de descarga de estos, de allí su nombre "*peer to peer*" (p2p), pues al conectarse a la red, la persona puede acceder a todos los archivos que otra tenga en su carpeta y así ir descargando y compartiendo al mismo tiempo el material.

Como resultado de ese ejercicio, las autoridades suizas identificaron que algunos usuarios de la red se intercambiaban fotos y videos con contenido de pornografía infantil. Entre las direcciones IP identificadas, una de ellas pertenecía a Eslovenia, por lo que ese dato fue remitido a la policía de aquel país.

Al recibir esta información, la policía eslovena solicitó a la compañía proveedora del servicio de Internet que revelara la información sobre el usuario a quien se le había asignado esa dirección IP dinámica a la 1.28 pm del día 20 de febrero de 2006.

La policía basó su solicitud en el artículo 149b (3) de la Ley de Procedimiento Penal local, que exigía a los operadores de redes de comunicación electrónica que divulgaran a la autoridad policial información sobre los propietarios o usuarios de ciertos medios de comunicación electrónica cuyos detalles

3 Sentencia del 9 de mayo de 2008. En igual sentido, sentencias del 07/10/10, 17/11/11 y 30/1/14, citadas en Pillado Quintas, V. *Pornografía infantil: regulación de estos delitos en el código penal. Dificultades en su investigación*, Fiscalía Provincial de Girona, p. 42.

4 Scarlet Extended, C-70/10, EU: C: 2011: 771, párr. 51.

no estaban disponibles en el directorio correspondiente. El 10 de agosto de 2006, la empresa reveló el nombre y la dirección del titular del servicio de Internet relacionado con aquella dirección IP.

El 12 de diciembre de 2006, la policía propuso que la Oficina del Fiscal Estatal solicite al juez de instrucción del Tribunal de Distrito de Kranj que emita una orden exigiendo que la empresa proveedora de internet divulgue tanto los datos personales del suscriptor como los datos de tráfico vinculados a la dirección IP en cuestión.

Con esos datos, el 12 de enero de 2007 el juez de instrucción emitió una orden para llevar a cabo un allanamiento en el domicilio, donde se secuestraron cuatro computadoras. Durante el registro domiciliario, también la policía advirtió –sobre la base de conversaciones con la familia– que el sospechoso era el hijo del titular del servicio, de nombre Igor Benedik. En una de las computadoras se encontró material de pornografía infantil y los registros del uso del *software* p2p *e-mule* para el intercambio de archivos.

Benedik fue imputado por el delito de exhibir, fabricar, poseer y distribuir material pornográfico tipificado en el art. 187 (3) del Código Penal de Eslovenia.

Durante el juicio, la defensa solicitó la nulidad de todo lo actuado en base a que la evidencia sobre la identidad del usuario de la dirección IP respectiva se había obtenido ilegalmente. En su opinión, esa información se refería a los datos de tráfico –o sea el contenido de una comunicación– y, por lo tanto, no debería haberse obtenido sin una orden judicial.

El 5 de diciembre de 2008, el Tribunal de Distrito de Kranj declaró a Igor Benedik culpable de la infracción penal por la que había sido acusado. Así, afirmó que el imputado debía haber tenido conocimiento de las 630 fotografías y 199 videos que involucraban a menores de edad en comportamientos sexuales que había descargado a través de las redes p2p y se habían puesto a disposición para compartir con otros usuarios. Benedik fue condenado a una pena de prisión en suspenso de ocho meses con un período de prueba de dos años.

El fallo fue recurrido tanto por la fiscalía como por la defensa. El 22 de noviembre de 2009, el Tribunal de Apelaciones hizo lugar al recurso de la fiscalía y convirtió la sentencia en una pena de prisión efectiva de 6 meses, al tiempo que rechazó los argumentos sobre la ilegalidad de la prueba.

La defensa recurrió la decisión ante la Suprema Corte reiterando el agravio por el cual afirmaba que una dirección IP dinámica no puede compararse con un número de teléfono ingresado en una guía telefónica, ya que esta clase de IP se renueva y se asigna a una computadora cada vez que el usuario ha iniciado sesión.

En consecuencia, la defensa sostenía que dichos datos deben considerarse como datos de tráfico que constituyen circunstancias y hechos relacionados con la comunicación electrónica y que, por ello, están alcanzados por la protección de la privacidad de las comunicaciones. Dicho en otras palabras: la policía suiza no debería haber obtenido la dirección IP dinámica respectiva sin una orden judicial, y la policía eslovena tampoco debería haber obtenido los datos sobre la identidad del suscriptor asociado con la dirección IP sin dicha orden.

El 20 de enero de 2011, la Suprema Corte desestimó la apelación al entender que los sitios web son de acceso general y la policía suiza podía verificar los intercambios en la red p2p simplemente monitoreando a los usuarios que comparten ciertos contenidos, es decir, sin una intervención particular en el tráfico de Internet. En función de ello, dicha comunicación no podría considerarse privada y, por lo tanto, protegida por el artículo 37 de la Constitución de Eslovenia.

Frente a ello, la defensa interpone un recurso ante la Corte Constitucional, pero este Tribunal resuelve desestimarlo el 13 de febrero de 2014 afirmando que no se había violado ningún derecho.

La Corte Constitucional reconoció que el derecho a la privacidad, amparado por la Constitución de Eslovenia, también protegía cualquier información transmitida en una red de comunicaciones electrónicas, entre las que se encontraban las direcciones IP. Sin embargo, concluyó que, en este caso, el imputado no había ocultado de ninguna manera la dirección IP a través de la cual había accedido a Internet, por lo que se había expuesto de manera consciente al público y no podía legítimamente esperar privacidad.

2.2. El reclamo ante el TEDH

Igor Benedik demandó al gobierno de Eslovenia ante el TEDH por la violación a su derecho a la privacidad en base a dos argumentos: por un lado, que la empresa proveedora del servicio de Internet retuvo ilegalmente sus datos personales y, por el otro, que la policía había obtenido diversos datos de su navegación y tráfico en Internet asociados con una dirección IP dinámica y, en consecuencia, también había obtenido su identidad sin orden judicial.

Así, a su entender, se había transgredido el artículo 8 del Convenio Europeo de Derechos Humanos, que ampara el respeto a la vida privada, el domicilio y la correspondencia.

El TEDH resolvió admitir la demanda solo con relación al segundo argumento.

3. La decisión del TEDH

3.1. El voto de la mayoría

El voto mayoritario comenzó sus consideraciones cuestionándose si Benedik, como cualquier otra persona que usa Internet, tenía una expectativa razonable de que su actividad –independientemente del carácter legal o ilegal– permanezca en el anonimato.

En ese sentido, el TEDH recordó que el concepto "vida privada" es un término amplio que no es susceptible de una definición exhaustiva. En esa inteligencia, reconoció que el artículo 8 del CEDH protege tanto el derecho a la identidad y el desarrollo personal como el derecho a establecer y desarrollar relaciones con otros seres humanos y el mundo exterior. En consecuencia, afirmó que existe

una zona de interacción de una persona con otras, incluso en un contexto público, que puede ser alcanzado por el término "vida privada".[5]

En refuerzo de este argumento, con cita al precedente *Delfi As vs. Estonia,*[6] el Tribunal consideró también la importancia de garantizar el anonimato en Internet para evitar represalias o una atención no deseada, con el propósito de promover el libre flujo de ideas e información.

En el caso antes citado, el TEDH había observado una suerte de grados de anonimato que un usuario puede gozar en Internet. En ese sentido, afirmó que se puede ser anónimo para el público en general y ser identificado por un proveedor de servicios a través de una cuenta o datos de contacto que pueden, o bien no estar verificados, o estar sujetos a algún tipo de verificación, como, por ejemplo, cuando se solicita la activación de una cuenta a través de una dirección de correo electrónico o una cuenta de red social para asegurar la autenticación.

De igual forma, un proveedor de servicios también puede permitir un amplio grado de anonimato para sus usuarios, en cuyo caso los usuarios no deben identificarse en absoluto y solo pueden rastrearse, hasta cierto punto, a través de la información retenida por las empresas proveedoras del servicio de Internet.

Para el TEDH, la revelación de dicha información requiere de una orden judicial por parte de las autoridades investigativas, sujeta a condiciones restrictivas.

En el caso concreto de Benedik, el voto mayoritario observó que la información del suscriptor, asociada con las direcciones IP dinámicas específicas asignadas en ciertos momentos no estaba disponible públicamente y, por lo tanto, no podía compararse con la información que se encuentra en la guía telefónica tradicional o, por ejemplo, en la base de datos pública de números de registro de vehículos, tal como argumentó el gobierno de Eslovenia.

En efecto, la mayoría entendió que para identificar a un suscriptor a quien se le asignó una dirección IP dinámica particular en un momento determinado, la empresa proveedora de Internet debe acceder a los datos almacenados relacionados con eventos de telecomunicación particulares. Estos datos, ya por sí solos, revelan consideraciones de la vida privada del usuario.

En ese entendimiento, el TEDH también valoró que, en el caso particular de Benedik, el único propósito de obtener la información del suscriptor era identificar a una persona en particular detrás del contenido recopilado de forma independiente que revelaba los datos que había estado compartiendo. La información sobre dichas actividades se relaciona con el aspecto de la privacidad en el momento en que se vincula o se atribuye a una persona identificada o identificable.

5 TEDH, *Case of Benedik v. Slovenia*, Application no. 62357/14, Judgment, Fourth Section, 24 de abril de 2018, párr. 99.

6 TEDH, *Case of Delfi As vs. Estonia*, Application no. 64569/09, Judgment, Court (Grand Chamber), 16 de junio de 2015, párr. 147.

Por lo tanto, lo que parecería ser información periférica solicitada por la policía –el nombre y la dirección de un suscriptor–, en situaciones como en el caso en análisis, debe tratarse como conectado de manera inexorable con los datos relevantes de información preexistente.

Así, concluye que sostener lo contrario sería negar la protección necesaria a la información que pueda revelar mucho sobre la actividad en línea de un individuo, incluidos los detalles sensibles, como sus intereses, creencias y estilo de vida íntimo.[7]

Finalmente, el voto mayoritario coincide con el Tribunal Constitucional de Eslovenia y acepta que Benedik, cuando intercambiaba archivos con material pornográfico a través de la red *Razorback*, esperaba, desde su perspectiva subjetiva, que esa actividad siga siendo privada y que su identidad no se divulgue.

Sin embargo, a diferencia del Tribunal Constitucional, el TEDH considera que el hecho de que no ocultó su dirección IP dinámica –suponiendo que es posible hacerlo– no puede ser decisivo en la evaluación de si su expectativa de privacidad era razonable desde un punto de vista objetivo.

A este respecto, señala que la pregunta a formularse para la solución del caso no es si Benedik podría haber esperado razonablemente mantener su dirección IP dinámica en privado, sino si podría haber esperado razonablemente la privacidad en relación con su identidad.

En cuanto al marco legal local, el TEDH observó que el artículo 37 de la Constitución de Eslovenia garantiza la privacidad de la correspondencia y de las comunicaciones, y exige que cualquier interferencia con este derecho se base en una orden judicial. En función de ello, la mayoría afirma que, también desde el punto de vista de la legislación vigente, no puede sostenerse que la expectativa de privacidad de Benedik con respecto a su actividad en línea haya sido injustificada o irrazonable.

A mayor abundamiento, es interesante destacar que el voto mayoritario recordó que el Convenio sobre Ciberdelincuencia obliga a los Estados a tomar medidas tales como la recopilación en tiempo real de datos de navegación en Internet para combatir, entre otras cosas, delitos relacionados con la pornografía infantil.

Sin embargo, tales medidas son, de conformidad con el artículo 15 de esa misma Convención, "sujetas a las condiciones y salvaguardas previstas en el derecho interno de [los Estados partes]" y deben "según proceda, teniendo en cuenta la naturaleza del procedimiento o poder en cuestión, entre otras cosas, incluir supervisión judicial u otra supervisión independiente, motivos que justifiquen la aplicación y limitación del alcance y la duración de dicha facultad o procedimiento".

Por todo ello, el TEDH concluye que el interés de Benedik en tener protegida su identidad con respecto a su actividad en línea se encuentra alcanzado por la noción de "vida privada" contenida en el CEDH y, por lo tanto, el artículo 8 fue lesionado por Eslovenia.

7 TEDH, *Case of Benedik vs. Slovenia*, cit., párr. 109.

3.2. El voto de la minoría

El juez Faris Vehabovic emitió el único voto en disidencia por el cual rechazó que se haya lesionado el derecho a la privacidad de las comunicaciones de Benedik.

Sostuvo, por un lado, que la información revelada por la empresa proveedora del servicio de Internet se refería a los datos de suscripción del titular del servicio que no era Benedik sino su padre, quien no formaba parte del reclamo ante el TEDH.

En relación con la expectativa razonable de privacidad, no estaba de acuerdo en que debiera considerarse la perspectiva subjetiva, pues el caso reposaba sobre actividad delictiva.

En su razonamiento, las personas que cometen delitos no desean que sus actividades sean conocidas por otros, por lo que este tipo de expectativa de privacidad no sería razonable cuando se basa en un incentivo ilegal. En otras palabras: una expectativa de ocultar actividad criminal no debe considerarse como razonable.

Pero más allá de eso, valoró que Benedik intercambió archivos que incluían pornografía infantil a través de una cuenta de una red pública que era visible para otros. Por lo tanto, sabía –o debería haber sabido– que sus acciones no eran anónimas, por lo que puede afirmarse que no tenía la intención de ocultar su actividad en el momento de la comisión del delito.

Finalmente, expresó que la injerencia al derecho a la privacidad para la prevención de un delito ha sido considerada como un objetivo legítimo por el TEDH en muchos casos. Así, citó, por ejemplo, el caso *S. and Marper vs. the United Kingdom,*[8] donde el Tribunal afirmó que la retención de huellas dactilares e información de ADN persigue el propósito legítimo de la detección y, por lo tanto, la prevención del delito. Así, mientras que la toma original de esta información persigue el objetivo de vincular a una persona en particular con el delito del que se sospecha, su retención persigue el propósito más amplio de ayudar en la identificación de futuros delincuentes.

Por esas razones, se apartó de la decisión de la mayoría.

4. Consideraciones finales

La investigación de determinados delitos cometidos a través de Internet revela ciertos obstáculos que deben ser examinados con cautela para evitar resultados adversos. El tráfico de pornografía infantil es un ejemplo paradigmático de estas dificultades en la medida que, en la generalidad de los casos, su pesquisa enfrenta el avance de la tecnología con derechos básicos en un terreno aún exploratorio.

Por cierto, el caso "Benedik" representó la primera vez que el TEDH se avocaba al estudio de las direcciones IP en relación con sus alcances y características en mira a la privacidad de las comunicaciones.

8 TEDH, *Case of S. and Marper vs. The United Kingdom*, Application nos. 30562/04 y 30566/04, Judgment, Court (Grand Chamber), 4 de diciembre de 2008.

En ese sentido, el eje central del debate se ubica en la noción del término "expectativa razonable de privacidad", concepto que nació en la jurisprudencia de la Corte Suprema de los Estados Unidos en el caso *Katz vs. USA.*[9]

Allí, se estableció que el test para la determinación de esta expectativa reposaba en dos criterios: por un lado, un juicio subjetivo por el cual una persona debía demostrar la expectativa real de privacidad y, por el otro, una pauta objetiva por la cual se debía afirmar que la sociedad estaba lista para admitir que esa expectativa era razonable.

De este modo, la cuestión a resolver es si existe esa expectativa razonable de privacidad cuando una persona utiliza Internet, más allá de los propósitos que persiga. Este punto me parece importante remarcarlo, pues lo que en "Benedik" se trató de resolver era si el contenido de la navegación y uso de Internet de una persona –que solo pueden revelarse a través de las direcciones IP dinámicas– son datos públicos y, por ende, pasibles de ser examinados sin orden judicial o, por el contrario, si se refiere al contenido de comunicaciones alcanzadas por el derecho a la privacidad –tal como el uso de un teléfono–, por lo que su intercepción solo debe ser habilitada por la autoridad judicial.

En esa inteligencia, entonces, resulta atinado lo resuelto por el voto de la mayoría, ya que no existen dudas de que Internet se ha convertido hoy en día en el medio de comunicación por excelencia y, por lo tanto, es claro que los usuarios confían –más allá de las posibilidades técnicas– en que su uso, con independencia de su fin, se mantendrá en reserva.

Varios ejemplos abonan esta conclusión, pero quizás uno de los más gráficos ha sido demostrado por Schneier, quien en su libro *Data and Goliat*[10] expuso un ejercicio realizado por la Universidad de Stanford, a través del cual se examinó la navegación en Internet de diversas personas. El resultado demostró no solo que se las pudo identificar fácilmente, sino también que esa inspección revelaba información sensible como afectaciones médicas, el uso de estupefacientes o los planes de interrupción de un embarazo.[11]

En pocas palabras, en la medida en que las direcciones IP dinámicas revelan información sobre los datos de navegación de los usuarios y estos, a su vez, deben ser considerados abarcados por el derecho a la privacidad en razón de una legítima expectativa a la intimidad, su utilización como evidencia en una causa judicial solo puede lograrse mediante orden judicial.

9 389 U.S. 347 (1967)

10 Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* Nueva York: W.W. Norton & Company.

11 Ver voto concurrente de los jueces Yudkivska y Bosnjak.