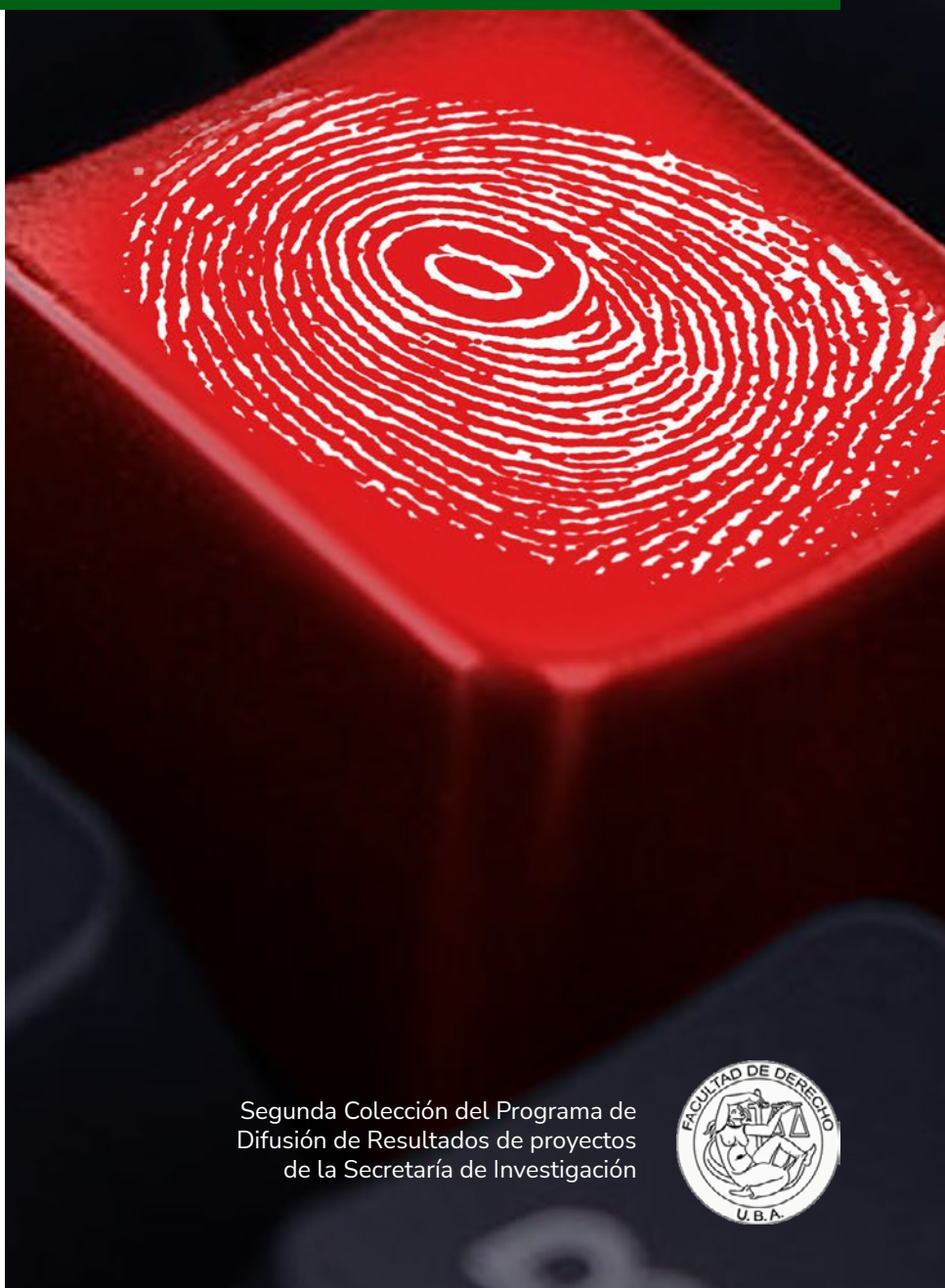
Marcos Salt *(Editor)*

VALORACIÓN JURISPRUDENCIAL DE LA EVIDENCIA DIGITAL



VOL. XI

Segunda Colección del Programa de Difusión de Resultados de proyectos de la Secretaría de Investigación

FACULTAD DE DERECHO U.B.A.

VALORACIÓN JURISPRUDENCIAL DE LA EVIDENCIA DIGITAL

Marcos Salt
(Editor)

Salt, Marcos
Valoración jurisprudencial de la evidencia digital en el proceso penal / Marcos Salt.- 1a ed. - Ciudad Autónoma de Buenos Aires : Universidad de Buenos Aires. Facultad de Derecho de la Universidad de Buenos Aires. Secretaría de Investigación , 2023.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-950-29-1990-4

1. Derecho Penal. 2. Procedimiento Judicial. I. Título.
CDD 345.05

Facultad de Derecho

1° edición: julio de 2022

Av. Figueroa Alcorta 2263, CABA
www.derecho.uba.ar

Coordinación académica: Daniel R. Pastor, Emiliano J. Buis y Luciana B. Scotti
Coordinación administrativa: Carla Pia Victoria Alizai
Edición y Corrección de estilo: Laura Pérgola
Diseño y diagramación de interior y tapa: Eric Geoffroy ericgeof@gmail.com

Imagende tapa: “Huella dactilar”, por pearleye. Imagen licenciada por Istockphoto.

Impreso en la Argentina – Made in Argentina
Hecho el depósito que establece la ley 11.723

Índice

I. Introducción

Mediante la Resolución (CD) N° 1771/19, del 15 de noviembre de 2019, la Facultad de Derecho de la Universidad de Buenos Aires aprobó el proyecto de investigación "Valoración jurisprudencial de la evidencia en el proceso penal".

El objeto de la presente investigación es el de estudiar el modo en que la jurisprudencia nacional y comparada ha considerado la incorporación de evidencia digital en procedimientos penales (elementos de prueba en formato informático, medios de prueba usados para la incorporación al proceso y mecanismos o herramientas de investigación que permiten acceder a los datos o elementos de prueba en entornos digitales).

Entendemos que el tema reviste una importancia superlativa en la actualidad y que requiere un análisis urgente. Esta afirmación se sustenta en el hecho de que, en primer lugar, la tecnología ocupa un lugar central en la vida de las personas y el rol de los dispositivos digitales en la humanidad nunca ha sido tan importante como en la actualidad.[1]

[1] Se calcula que en un minuto de internet 900 000 personas se conectan a Facebook, 3 500 000 realizan una búsqueda en Google, 452 000 postean un tuit y se suben a Instagram 46 200 fotos, según un estudio de la consultora

Toda la información de nuestra interacción con dispositivos digitales queda resguardada en ellos o en servidores, alojados en distintas jurisdicciones.[2] Esta circunstancia resulta de particular interés para cualquier investigación penal. No solamente aquellos delitos que fueron cometidos a través medios digitales requieren de la producción de evidencia digital para su investigación, sino que, hoy en día, es probable que cualquier delito genere evidencia digital que resulta de utilidad para las autoridades encargadas de la persecución penal[3] y para quienes deben ejercer la defensa en procesos penales. Es más, hoy es posible afirmar que la tendencia de reemplazo de la prueba física por prueba digital en todos los procesos penales se ha acelerado de tal forma que es muy posible que, en un futuro cercano, estos medios de prueba tecnológica sean el eje central probatorio en los procesos y la prueba física quede relegada a un segundo plano.[4]

Pensemos por ejemplo en un robo a un local de ropa a la calle. El hecho transcurre en la vía pública, una persona ingresa al local y, bajo amenaza, le exige al encargado del local que le entregue el dinero de la caja registradora y algunos productos de valor que están en exhibición para su venta. Este delito, si bien fue cometido sin la utilización de medios digitales, puede ser correctamente investigado a raíz de la producción de evidencia digital. El impacto de señales de celular de la antena cercana al local robado nos podría brindar información que nos permita identificar al autor o situar al sospechoso en el lugar del hecho, dado que posiblemente haya utilizado un dispositivo celular como la

---

Commulus Media, citado en Golombek "este libro (y esta colección), prólogo en Sosa Escudero, W., *Big Data*, 5ta. ed., Buenos Aires, Siglo XXI Editores, 2019, p. 1 y según Daily Mail, en promedio las personas pasamos más tiempo conectadas a internet (8:41 h) que durmiendo (8:21 h)". Ver: http://www.dailymail.co.uk/health/article-2989952/How-technology-taking-lives-spend-time-phones-laptops-SLEEPING.html

[2] Ver por ejemplo, Price, M., *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, June 29, 2015, p. 1. Disponible en: https://www.brennancenter.org/analysis/rethinking-privacy-fourth-amendment-papers-and-third-party-doctrine

[3] Ortiz Pradillo, J. C., *Problemas procesales de la ciberdelincuencia*, Madrid, Colex, 2013, pp. 158 y ss.

[4] Salt, M, *Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos* informáticos, Buenos Aires, Ad Hoc, 2017, pp. 23 y ss.

mayoría de las personas.[5] Los testigos del hecho pudieron haberlo registrado con sus dispositivos, por lo que acceder a tales videos podría resultar de gran interés. A su vez, cámaras de videovigilancia en la zona, públicas o privadas, podrían haber registrado al autor. A través de redes sociales alguna persona podría haber posteado datos sobre el delito (por ejemplo, para alertar a las autoridades), lo que facilitaría la identificación de testigos. A su vez, los productos del robo podrían ser ofrecidos a través de sitios de internet, respecto de los cuales resultaría de gran interés conocer los datos de conexión de quienes los ofrecieron para determinar su identidad. Los elementos de prueba digital resultan también fundamentales para una adecuada estrategia de la defensa. Supongamos, a modo de ejemplo, que la defensa de la persona imputada pudiera incorporar al proceso elementos de prueba (datos de geolocalización, aplicaciones) que ubicaran el teléfono del imputado lejos de la zona en que ocurrió el hecho o que los datos informáticos de los medios públicos de transporte (tarjeta sube) o registros informáticos del uso de su tarjeta de crédito, ubicaran geográficamente al imputado lejos del lugar a la hora en que sucedió el ilícito. La lista de posibilidades probatorias que brinda la evidencia digital es muy amplia, muchas veces más sencilla de producir y más fehaciente que la que permite la prueba física. Aquí solo enumeramos a modo de ejemplo, algunos elementos de prueba digital que podrán ser útiles para conocer el hecho histórico que es objeto del proceso.

Los problemas que presenta la incorporación de este tipo de evidencia al procedimiento penal argentino son de diversa índole. En primer lugar, cabe destacar que la evidencia digital es sustancialmente diferente a la evidencia física.[6] En este aspecto, expertos del Consejo de Europa han destacado que la evidencia digital es no visible para las personas que no poseen conocimientos y formación técnica especial, es frágil y volátil, puede ser alterada o destruida, incluso mediante el uso habitual de los dispositivos electrónicos y puede "copiarse" ili-

[5] Según el INDEC, 8 de cada 10 personas en el país utilizan teléfonos celulares. Ver: https://www.telam.com.ar/notas/201905/357981-tecnologia-celulares.html

[6] Salt, M., *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ad Hoc, 2017, pp. 23 y ss.

mitadamente.[7] La evidencia digital, por su parte, viaja por el mundo sin pasaporte y sin atender a los límites territoriales de los países. De hecho, puede estar copiada en varios lados a la vez, o en uno solo, o en cuestión de segundos trasladarse desde un continente a otro.[8]

Sin perjuicio de sus características particulares, en la práctica tribunalicia actual, la evidencia digital se incorpora a las investigaciones de la mano del principio de libertad probatoria y sobre la base de aplicación analógica de reglas y garantías que regulan los medios de prueba tradicionales.[9] Esto se debe a que no existe en nuestra norma federal de procedimiento penal una regulación específica que atienda a las particularidades de la evidencia digital. Si bien el artículo 151 del código procesal penal aprobado por la Ley Nro. 27.063 regula en un artículo lo que denomina "incautación de datos", lo que sin dudas constituye un avance en materia regulatoria, lo cierto es que este artículo no prevé un catálogo completo de medios de prueba e investigación pensados para las necesidades que plantea la evidencia digital al proceso penal moderno ni responde a muchas de las particularidades que diferencian a los elementos de prueba en formato digital de los tradicionales elementos de prueba física. A modo de ejemplo: ¿la incautación de datos prevista en el art. 151 es un peritaje?[10], ¿cómo se deben inspeccionar los datos para preservar la intimidad y privacidad de las personas en la mayor medida posible?, ¿qué sucede si los datos se encuentran alojados en servidores ubicados en extraña jurisdicción?, etc.

Dada la falta de regulación específica sobre el tema, cabe también preguntarse por el alcance de la protección constitucional de nuestros datos íntimos y privados que almacenamos en dispositivos digitales. En nuestros teléfonos celulares, por ejemplo, tenemos fotos persona-

---

[7] Data Protection and Cybercrime División del Consejo de Europa, *Guía de Prueba Electrónica. Guía Básica para fuerzas y cuerpos de seguridad, jueces y fiscales*, elaborada en marzo de 2013

[8] Ver, por ejemplo, Daskal, J., The un-territoriality of data, en *Yale Law Journal*, vol. 125, 2015.

[9] Salt, M., *ob. cit.*, pp. 26 y 27.

[10] Ver Daray, R. y otros, *Código Procesal Penal Federal. Análisis doctrinal y jurisprudencial,* 2da. ed., Buenos Aires, Hammurabi, 2021, p. 615, quien sostiene que en la incautación deberá participar un perito a efectos de garantizar la inalterabilidad y fidelidad de la información, asegurando la cadena de custodia.

les, correos electrónicos, registros de comunicaciones, mensajes, datos sobre nuestro geoposicionamiento, etc.[11] Los desafíos que plantea la evidencia digital no solo impactan en la necesidad de elaborar nuevas normas que regulen su incorporación al proceso penal, sino que también implica reinterpretar las garantías constitucionales en pos de mantener el equilibrio entre la protección de la privacidad e intimidad de las personas y el deber del Estado de investigar los delitos.[12]

La irrupción de la pandemia generada por el COVID-19 agravó aún más la situación, en tanto aceleró de manera vertiginosa la digitalización y el proceso de reemplazo de prueba física por digital.

Este trabajo se propone analizar de qué forma los desafíos que plantea la incorporación de prueba digital han sido tratados por la jurisprudencia nacional, ante la falta de normativa específica (los códigos procesales penales no han previsto un catálogo de medios de prueba pensados y elaborados conforme a las características de este nuevo fenómeno).

En esta investigación se abordó el tratamiento de los siguientes temas:

- Autoincriminación y desbloqueo compulsivo de teléfonos celulares
- Registro y secuestro de datos informáticos
- Orden de presentación para obtener datos digitales
- Cadena de custodia
- Hallazgos causales en el marco de registro de sistemas informáticos
- Acceso transfronterizo a datos digitales
- Utilización de OSINT, (Open Source Intelligence) en investigaciones penales
- Agente encubierto digital
- Utilización de *software* a distancia
- Entrega vigilada digital
- Uso de drones
- Acceso a comunicaciones electrónicas desarrolladas a través de plataformas de mensajería instantánea y a correos electrónicos laborales en el marco de políticas de *compliance*

[11] Polansky, J., *Garantías constitucionales del procedimiento penal en el entorno digital*, Buenos Aires, Hammurabi, 2020, pp. 73 y 74.
[12] Ver *Id.*, p. 25.

El proyecto se concentró en abordar el tratamiento de estos temas en la jurisprudencia nacional, provincial (en provincias seleccionadas) y comparada en países con larga trayectoria doctrinaria, normativa y jurisprudencial en lo referido a la incorporación de evidencia digital al procedimiento penal y la emanada de organismos internacionales. Se consideró que el estudio comparado de tales jurisdicciones (Estados Unidos, España, Sistema Interamericano de Derechos Humanos y Unión Europea) nos permitiría ampliar la percepción de todas las aristas de los conflictos que se generan por la incorporación de evidencia digital al procedimiento penal.

Para llevar a cabo tal tarea, se realizaron búsquedas en fuentes abiertas[13], en sitios de búsqueda de jurisprudencia[14], se recurrió al análisis de doctrina nacional e internacional especializada[15] y se cursaron consultas a la Cámara Federal de Casación Penal, Cámara Nacional de Casación Penal, al Supremo Tribunal de Justicia de la Ciudad de Buenos Aires, a la Fiscalía Especializada en Cibercrimen de Córdoba, a la Fiscalía General de Córdoba, Fiscalía General de Mendoza y fiscalía especializada de dicha provincia y a la Fiscalía General Especializada en Delitos Informáticos de España.

En todas las consultas, se les solicitó a las autoridades representantes del Poder Judicial y del Ministerio Público Fiscal la remisión de la jurisprudencia de su jurisdicción sobre los temas detallados precedentemente.

Una vez recopilada toda la jurisprudencia que fuera remitida, los integrantes del equipo de investigación procedieron a la lectura particularizada de cada uno de los fallos a efectos de determinar su pertinencia con la investigación. Esto se debió a que en algunos casos se advirtió que, posiblemente, las oficinas consultadas habían realizado búsquedas en sus bases de datos por medio de ingreso de palabras clave relacionadas con los temas de esta investigación y que habían arrojado como resultados falsos positivos. Es decir, se habían remitido fallos que contenían, por ejemplo, la palabra clave "datos digitales", pero que el caso no correspondía con los temas que aquí se investigan.

[13] Por ejemplo, Google.
[14] Jstor y Westlaw.
[15] Que se detallará en la sección bibliografía.

Una de las hipótesis iniciales de este trabajo fue que, en la práctica cotidiana de nuestros tribunales, se incorpora frecuentemente evidencia digital, mediante alguna de las técnicas o herramientas tecnológicas que son objeto de este estudio, pero que los sujetos procesales (fiscalía, defensa, jueces) no han aun reparado en los problemas procesales y constitucionales que genera la utilización de esas nuevas tecnologías en investigaciones penales y que, en consecuencia, no hay fallos que den tratamiento específico y explícito a estas cuestiones, mucho menos pronunciamientos de tribunales superiores ya que no son objetados o las cuestiones son resueltas en primeras instancia o ni tan siquiera cuestionadas. Es decir, que se trataba de "jurisprudencia oculta" o situaciones resueltas en los hechos sin decisiones judiciales expresas. Por ejemplo, se advirtió que por el uso actual de los *smartphones* es probable que mucha evidencia contenida en teléfonos celulares se encontrara, en verdad, almacenada en "la nube", es decir en un servidor en extraña jurisdicción. A su vez, se tiene conocimiento que algunas fuerzas federales de nuestro país poseen *software* de extracción de datos de dispositivos celulares con capacidad de extraer información almacenada en la nube.[16] En consecuencia, es probable que en algunos casos se haya extraído este tipo de información, sin que las partes hicieran algún planteo sobre los problemas que genera el acceso transfronterizo a la evidencia. Por este motivo, se estimó que no resultaría probable encontrar resoluciones jurisprudenciales en las que se hubiera procedido de esta forma, en tanto la problemática detectada no fue objetada por los sujetos procesales y, en consecuencia, no se generó pronunciamiento judicial. De la misma manera, uso de agentes encubiertos digitales, envío de programas para obtener la dirección IP real de sospechoso que utiliza formas de anonimato en la navegación, etc.

Para poder corroborar esta hipótesis, se celebraron entrevistas con los referentes técnicos Pablo Romanos y Adrián Acosta para conocer si en la práctica se llevaban a cabo medidas que generarían tensión con

[16] Por ejemplo, la Gendarmería Nacional Argentina posee el equipo UFED Cloud que permite extraer información almacenada en la Nube. Ver https://www.cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

nuestro sistema procesal pero que no fueron discutidas explícitamente en la jurisprudencia.

En este documento se detallan todos los fallos encontrados a nivel nacional (incluyendo fueros federales, nacional y de las provincias de Córdoba, Mendoza y de la Ciudad Autónoma de Buenos Aires) que tratan sobre los temas que son objeto de esta investigación. También se detalla la jurisprudencia relevante sobre la temática encontrada en las jurisdicciones de Estados Unidos, España, Sistema Interamericano de Derechos Humanos y Unión Europea.

En todos los casos se procedió a analizar los fallos, resumirlos a efectos de destacar los hechos, el *holding* y referencias relevantes, siempre circunscribiendo el trabajo a los objetos de la investigación. En consecuencia, los fallos que abordaban múltiples cuestiones fueron resumidos de forma tal que, en este documento, únicamente se detallan las cuestiones inherentes a las temáticas de interés.

Cada fallo se encuentra agrupado en el capítulo que le corresponde, según el tema de esta investigación que trata. Previo al inicio de cada capítulo, se detalla una introducción al tema en la que se destacan los problemas procesales y constitucionales que se advierten respecto de su aplicación.

También se incluyen en el documento las transcripciones relevantes de las entrevistas realizadas a efectos de detectar la existencia de lo que hemos denominado "jurisprudencia oculta".

II. Autoincriminación y desbloqueo de teléfonos celulares mediante el ingreso compulsivo de datos biométricos

II. a. Introducción

La utilización de teléfonos celulares se encuentra tan expandida en el país[1], que resulta razonable considerar que en la mayoría de los delitos existe algún dispositivo celular involucrado del cual se podría obtener prueba relevante para corroborar la existencia del hecho ilícito y la responsabilidad de su autor.[2] A modo de ejemplo, los teléfonos celulares almacenan conversaciones o mensajerías de diferente tipo, datos de geoposicionamiento, fotografías, videos, correos electrónicos, agendas, registros de comunicaciones, historiales de búsquedas en la web, claves y contraseñas, en muchos supuestos accesos a redes so-

[1] Según el INDEC 8 de cada 10 personas en el país utiliza teléfonos celulares. Ver TELAM, ocho de cada diez personas tienen acceso a celulares en la Argentina, publicado en TELAM el 8 de mayo de 2019. Disponible en: https://www.telam.com.ar/notas/201905/357981-tecnologia-celulares.html. En EE. UU., el 96 % de las personas posee Smartphones. Ver PEW RESEARCH CENTER, Mobile fact sheets, del 12 de junio de 2019. Disponible en: https://www.pewinternet.org/fact-sheet/mobile/

[2] Por ejemplo, ver Ortiz Pradillo, J.C. *ob. cit.*161.

ciales, etc. Todo este tipo de información se encuentra protegida por el artículo 18 de nuestra Constitución Nacional.[3]

Ahora bien, lo cierto es que, pese a obtener una autorización judicial para secuestrar un dispositivo de telefonía móvil (*smartphone*), en un allanamiento o requisa para luego acceder a la información almacenada en él, resulta probable que las autoridades estatales se vean imposibilitadas de lograr tal acceso (para realizar las tareas necesarias de búsqueda y secuestro de datos), debido a que la mayoría de los equipos de telefonía móvil poseen mecanismos de encriptación que impiden el acceso a la información contenida en ellos a todo aquel que no posea las correspondientes llaves de desbloqueo.[4] Estas llaves pueden consistir en una clave numérica y/o alfabética, en el ingreso de un patrón de desbloqueo, el reconocimiento de las huellas dactilares, características faciales o del iris del usuario del dispositivo.[5] En la presente sección se describirán y detallarán el modo en que la jurisprudencia nacional y extranjera ha resuelto casos en los que la garantía contra la autoincriminación y el derecho de defensa se han tensionado con la necesidad de desbloquear un dispositivo de telefonía digital para acceder a evidencia digital.

---

[3] Carrió, A., *Garantías Constitucionales en el Proceso Penal*, 6ta ed., Buenos Aires, Hammurabi, 2015, pp. 448- 458 y Hairabedián, M., "El acceso a información y datos de teléfonos celulares", en Dupuy (Dir.) *Cibercrimen. Aspectos del derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet*, Buenos Aires, B de F, 2017, pp. 456 y caso CCC 37443/208/CA2, resuelto por la Sala 6 de la Cámara Nacional de Apelaciones en lo Criminal y Correccional el 31 de julio de 2018, por cuanto determinó "(...) Recordemos que el artículo 18 dispone la inviolabilidad del domicilio, la correspondencia epistolar y los papeles privados. No caben dudas a que dentro de esa enunciación quedan comprendidas también las comunicaciones realizadas mediante correos electrónicos, llamados telefónicos o mensajes de texto, entre otros. Sobre ellos prácticamente no hay controversia jurisprudencial ni doctrinaria y los avances tecnológicos día a día establecen nuevas formas de relacionarnos lo cual convierte a tal enumeración en simples ejemplos...".

[4] Kerr, O., Compelled Decryption and the Privilege Against Self-Incrimination, en *Texas Law Review*, Vol. 97, Issue 4, 2019, p. 1.

[5] Ver por ejemplo, Kerr, O., y Schneier, B., Encryption Workarounds, en *Georgetown Law Journal*, Vol. 106, Issue 4, 2018, pp. 994 y ss. y 1003 y ss.

Cabe señalar que en este supuesto también hemos podido detectar que en la práctica existen muchos casos en los que el imputado ha aportado de manera voluntaria las claves o ha aceptado que sus datos biométricos sean utilizados para desbloquear los dispositivos sin que constara en resolución judicial alguna y muchas veces ni siquiera en las actas de secuestro.

II. b. Jurisprudencia argentina

II. b. 1. Fuero federal

Cámar*a Federal de Apelaciones de La Plata, Sala I. Causa FLP n° 14.149/2020 caratulada "Melo Facundo y otros S/ Inf. Art. 210 del Código Penal y Violación a la Ley Nacional de Inteligencia", 20 de octubre de 2020*

El 25 de julio de 2020, el Juzgado Federal N° 2 de Lomas de Zamora dispuso el registro de distintos inmuebles vinculados al imputado Darío Nieto, el secuestro de dispositivos de telefonía celular, entre otras cosas. A su vez autorizó a que las fuerzas de seguridad utilizaran *la mínima fuerza pública necesaria a los efectos de que el investigado sea trasladado al asiento de dicho organismo pericial, y para que los mismos sean desbloqueados a través de la utilización de las huellas dactilares, lectores de retina o identificación de rasgos faciales.*

En efecto, al practicar la medida y al darle a conocer la autorización mencionada para proceder al desbloqueo de los dispositivos celulares, el imputado Nieto, en presencia de su abogado defensor, aportó las correspondientes claves de acceso, manifestando su disconformidad con la orden judicial que autorizaba al desbloqueo compulsivo mediante el ingreso datos biométricos.

La defensa de Nieto solicitó la nulidad de la medida. El juez de primera instancia rechazó el planteo, por lo cual se interpuso un recurso de apelación. La Sala I de la Cámara Federal de La Plata confirmó la decisión del magistrado de primera instancia. Al respecto consideraron: *En relación al planteo vinculado a la presunta coacción ejercida sobre el imputado para lograr el desbloqueo de su teléfono celular, debe señalarse que no se advierte que con ello se haya violentado el derecho constitucional de defensa, ni la prohibición de la autoincriminación, que*

consagra el artículo 18 de la Constitución Nacional. En efecto, para el acceso al aparato no se ha requerido ningún tipo de declaración del interesado, sino tan solo el aporte de la clave para su desbloqueo. Sobre el particular, corresponde mencionar en primer lugar, que la orden judicial expresamente indicaba que en caso de que los aparatos de telefonía celular a secuestrar presentaran un bloqueo dispuesto por el usuario, se autorizaba al personal policial interviniente "a la utilización de la mínima fuerza pública necesaria a los efectos de que el investigado sea trasladado al asiento de dicho organismo pericial, y para que los mismos sean desbloqueados a través de la utilización de las huellas dactilares, lectores de retina o identificación de rasgos faciales". Agregaron que si bien era cierto que existía una orden judicial para lograr el desbloqueo del teléfono, debía forzarse su interpretación para concluir que la negativa a aportarla implicaba la detención de Nieto en tanto la orden era clara al disponer que se autorizaba el traslado del interesado al asiento del cuerpo pericial al solo efecto de proceder a su desbloqueo mediante su huella, lector de retina o reconocimiento facial pero que nada decía sobre llevar a cabo su detención en caso de negativa.

Juzgad*o Federal de Dolores, Causa FMP n° 88/2019 caratulada "Marcelo D'Alessio y otros s/ asociación ilícita y otros", 21 de febrero de 2019*

El juzgado ordenó diversos allanamientos en el marco de una investigación por asociación ilícita, en la que se secuestró, entre otras cosas, algunos dispositivos de telefonía celular.

En este marco, se le solicitó al imputado D'Alessio que aportara la clave de desbloqueo de su equipo. Ante su negativa, se lo obligó a asistir al lugar donde se realizaría el peritaje, para que el imputado compulsivamente ingresare sus datos biométricos, a efectos de desbloquear los dispositivos. En efecto, el juez interviniente entendió que *contamos con que –según se explicó– entre las medidas de accesibilidad al equipo telefónico que era usado por D´Alessio (IPhone 8 Plus y IPhone 10) más allá que no se cuente con sus claves o patrones de ingreso, "existe la posibilidad de ingresar o extraer sus datos si se ingresa con su huella o rostro"... De este modo, estamos en un tramo de la investigación donde contamos con "pocas posibilidades seguras de acceder a esos equipos", la que se podría sortear con el aporte del Sr. D´Alessio de su huella o rostro para desactivar las medidas de seguridad y accesibilidad mencionadas. Así es que parece razonable, necesario, proporcional y pertinente al fin*

investigado, "contar con su presencia en el acto que se desarrollará en la Sección de Pericias Informáticas de la PNA para que aporte" –voluntaria o compulsivamente– "su rostro o huella" (art. 218 CPPN).

Luego, el magistrado indicó que la comparecencia del imputado al acto de pericia se presentaba como el único modo seguro y menos lesivo que otros medios, pues fácilmente se advertía que el aporte de su huella dactilar o la lectura de rostro que la cámara del equipo telefónico podía hacer no producían una invasión corporal que menoscabaran su pudor, como tampoco conculcaban o vulneraban derechos que tiene como imputado.

II. b. 2. Provincia de Buenos Aires

Cámar*a de Apelación y de Garantías en lo Penal del Departamento Judicial Pergamino. Causa N° I. P. P 17673, "N.N. s/ Estupefacientes - Tenencia con fines de comercialización" 6 de noviembre de 2019*

N.N. fue detenido por la policía junto a otra persona, oportunidad en que les pidieron sus DNI y documentación de la moto. Pese a no haber impedimento para circular, los agentes policiales los requisaron, encontrándose estupefacientes a N.N., todo ello a plena luz del día, siendo alrededor de las 15:30 horas. En el acta inicial se volcaron los dichos de los jóvenes, a quienes les pidieron el código de desbloqueo de sus aparatos celulares. Posteriormente, se realizó un peritaje sobre los teléfonos celulares y se extrajo la información allí contenida, sin que fuera necesario el ingreso de los códigos de desbloqueo.

La defensa solicitó la nulidad de la medida, fundándose, entre otras cuestiones, en que los códigos de desbloqueo habían sido obtenidos en violación a la garantía contra la autoincriminación. El magistrado de primera instancia hizo lugar al pedido de nulidad y consideró que los códigos de desbloqueo fueron obtenidos de manera ilegítima. No obstante, consideró que el peritaje resultaba valido ya que existía un *cauce independiente de investigación* y que en el peritaje no se requirieron esos códigos para acceder a los teléfonos. La defensa apeló la medida. La Cámara, en lo que aquí interesa, confirmó lo resuelto por el juez de primera instancia.

II. c. Jurisprudencia internacional

II. c. 1. España

Tribu*nal Supremo, Sala de lo Penal, Procedimiento N° 10545, Auto núm. 3/2020 de 16 enero de 2020*

Eliseo, Evelio y Ezequiel fueron acusados del delito de comercialización de sustancia estupefaciente. La policía, en los primeros momentos de sus detenciones, y sin presencia de sus letrados, les ofreció la posibilidad de efectuar una llamada personal con el único fin de obtener el PIN y el código de desbloqueo de sus teléfonos móviles. Los imputados fueron juzgados y condenados.

Las defensas interpusieron recurso de apelación ante la Sala de lo Civil y Penal del TS de Justicia de Madrid, confirmando parcialmente el anterior pronunciamiento. Contra dicha sentencia se interpuso recurso de casación. Los abogados alegaron, entre otras cosas, que los agentes policiales actuaron de forma incorrecta.

La cuestión que se debió dilucidar fue si esta manera de acceder al código personal de aquellas personas para así obtener información en su contra resultaba violatoria del art. 18 de su Constitución Nacional que consagra el derecho a la protección de datos.

El Tribunal Superior destacó en sus fundamentos jurídicos que la obtención del número PIN y del código de desbloqueo fue lícita, en tanto tales datos fueron facilitados de forma voluntaria, conforme declararon los agentes; tales extremos fueron comunicados a los agentes al preguntarles estos dicha información para que pudieran realizar la llamada personal a que tenían derecho.

El juez indicó que el Tribunal Constitucional y esa misma Sala de casación han venido admitiendo justificadas injerencias en la intimidad personal si son moderadas, van encaminadas a la averiguación de delito y respetan el principio de proporcionalidad. La STS 551/2016, de 22 de junio, señala que el número de PIN es un dato de acceso a la terminal telefónica cuyo conocimiento no requiere autorización judicial, por no tratarse de dato alguno relativo a las comunicaciones. También hizo referencia a STS 302/2019, de 7 de junio, que conforme ha señalado el Tribunal Constitucional en su sentencia 208/2007, de 24 de septiembre, "... la asistencia letrada solo es constitucionalmente

imprescindible en la detención y en la prueba sumarial anticipada (...) en los demás actos procesales y con independencia de que se le haya de proveer de abogado al preso y de que el abogado defensor pueda libremente participar en las diligencias sumariales, con las únicas limitaciones derivadas del secreto de sumario, la intervención del defensor no deviene obligatoria hasta el punto de que hayan de estimarse nulas, por infracción del derecho de defensa, tales diligencias por la sola circunstancia de la inasistencia del abogado defensor" (SSTC 206/1991, de 30 de octubre, FJ 2; 229/1999, de 13 de diciembre, FJ 2; 38/2003, de 27 de febrero, FJ 5).

Expresó que en este caso existían abundantes indicios de la existencia del delito que se estaba investigando, que está castigado en la Ley penal con penas de hasta nueve años y que, por ello, se trató de una infracción muy grave y por tanto cumpliría el principio de proporcionalidad. Y que aquí fueron los titulares de los móviles los que facilitaron el PIN y el código de desbloqueo.

Asimismo, indicó que la autorización judicial del volcado de los móviles intervenidos estaba suficientemente justificada, a la vista de la cantidad de droga incautada y relacionada con los titulares de dichos terminales, que motivó su detención; estando justificada la necesidad de tal diligencia de volcado de los móviles para el esclarecimiento de los hechos y de la identidad de otras personas que pudieran estar involucradas en estos.

Por lo expuesto, la Sala acordó no hacer lugar a la admisión de los recursos de casación formalizados por las partes recurrentes contra la sentencia dictada por la Sala de lo Civil y Penal del Tribunal Superior de Justicia.

II. c. 2. Estados Unidos

Segun*do Circuito Judicial del Estado de Virginia, caso CR-14-1439 Commonwealth of Virginia v. David Charles Baust, 28 de octubre de 2014)*

David Baust fue acusado de estrangular a su acompañante en la habitación de su domicilio. La víctima manifestó que la agresión fue filmada por dispositivos de grabación que estaban conectados al teléfono celular del agresor.

La policía, en el marco de la investigación, ejecutó una orden de allanamiento en el domicilio de Baust y secuestró –entre otros elementos– el dispositivo de telefonía móvil que se había utilizado en el hecho. Al encenderlo, verificó que se encontraba encriptado y que requería, para permitir el acceso a su información, el ingreso de una clave o de la huella dactilar de su usuario.

La acusación solicitó que se ordenara al imputado desbloquear su teléfono. La defensa sostuvo que tal medida resultaría violatoria de la garantía contra la autoincriminación, consagrada en la 5ta. Enmienda a la Constitución de los Estados Unidos.

En efecto, la cuestión que se debió resolver era determinar si obligar a un imputado a colocar su huella dactilar para desbloquear un teléfono celular resultaba violatorio de la garantía contra la autoincriminación.

El magistrado autorizó a la acusación a que obligue al Sr. Baust a colocar su huella en el teléfono para desbloquearlo, pero no autorizó a que se lo obligue a entregar la clave de acceso. Consideró que el desbloqueo compulsivo del teléfono celular mediante el ingreso de su huella dactilar no constituía una violación a la garantía constitucional contra la autoincriminación, toda vez que tal medida carecía de contenido testimonial.

El juez advirtió que obligar al imputado a otorgar su clave o colocar su huella dactilar en su teléfono para desbloquearlo y, en consecuencia, permitirles a las autoridades encargadas de la persecución penal acceder a su contenido constituía una medida compulsiva que podría tener consecuencias incriminantes contra el propio imputado.

Sin perjuicio de eso, el juez destacó que la jurisprudencia de Estados Unidos consideraba que obligar al imputado a realizar ciertas medidas –que eventualmente lo podrían perjudicar– no resultaban en sí mismas violatorias de la garantía contra la autoincriminación. La garantía en cuestión solo protegía la autoincriminación forzada proveniente de actos testimoniales.

Se afirmó que medidas tales como la extracción compulsiva de sangre, la obligación de que el imputado utilizara determinada vestimenta con fines identificatorios, la toma compulsiva de huellas dactilares carecían de contenido testimonial (no implicaban revelación del pensamiento del imputado), por lo que eran admitidas desde una perspectiva constitucional.

Por un lado, el juez entendió que obligar al imputado a ingresar su clave de acceso para desbloquear el teléfono constituía una medida

testimonial, dado que la clave no era conocida *fuera de su mente* y la producción de tal medida demandaría la externalización de su pensamiento en su propio perjuicio. En consecuencia, la producción de tal medida estaba vedada por la garantía contra la autoincriminación.

Por el otro, afirmó que el desbloqueo del dispositivo de telefonía móvil mediante el ingreso compulsivo de la huella dactilar de su dueño era permisible desde la óptica de la 5ta. Enmienda, ya que esta medida no implicaba exteriorización de pensamiento alguno, es decir no resultaba testimonial.

Unite*d States District Court Northern District of California, Caso No. 4-19-7005 3, 10 de enero de 2019*

En el marco de una causa en la que se estaba investigando a dos individuos sospechados de estar involucrados en un caso de "sextorsión", la jueza del Noveno Distrito Norte de California, Kandis Westmore, denegó un pedido de autorización para obligarlos a desbloquear un teléfono mediante huella dactilar o reconocimiento facial.

Según la pesquisa, los imputados habrían usado Facebook Messenger para comunicarse con una víctima a quien habrían amenazado con distribuir un video íntimo si no les pagaba. La Fiscalía solicitó la autorización de una "orden de registro" para incautar distintos elementos relacionados con el delito en un domicilio ubicado en Oakland, California, entre ellos, dispositivos electrónicos.

Si bien la magistrada consideró acreditada la "causa probable" para la orden de registro, denegó el pedido para que se obligue a cualquier persona presente al momento del allanamiento, a presionar un dedo (incluido el pulgar) o utilizar otras funciones biométricas, como "Reconocimiento facial o del iris", con el fin de desbloquear los dispositivos digitales encontrados para permitir una búsqueda de los contenidos según lo autorizado por la orden de registro.

Para rechazar la petición, la jueza entendió que esa manda vulneraba las Enmiendas 4ta. y 5ta. de la Constitución de los Estados Unidos, que es garantizar la garantía contra la autoincriminación. Admitió que la tecnología está superando a la ley y ponderó que el acto de comunicar el código de acceso es un testimonio, ya que la expresión del contenido de la mente de un individuo cae directamente dentro de la protección de la 5ta. Enmienda. Incluso, indicó que, si existe una causa probable para incautar los dispositivos, ello no permitiría que se pueda obligar

a un sospechoso a renunciar a los derechos que de otro modo dispone la Constitución, lo que ocurría en el caso, donde se estaba utilizando la característica biométrica de un sospechoso para desbloquear potencialmente un dispositivo electrónico.

La jueza interviniente entendió que, aun en el proceso de ejecución de una orden de registro válida, la vulneración desproporcionada de cualquier otro derecho fundamental (como la privacidad) intrínsecamente tacha a toda búsqueda e incautación de irrazonables.

La magistrada concluyó entonces en que el desbloqueo de un teléfono mediante el escaneo con el dedo excede con mucho la evidencia física creada cuando un sospechoso se presta a brindar sus huellas digitales para así compararlas con la evidencia física encontrada en la escena del crimen, porque se requieren otras corroboraciones para confirmar una coincidencia positiva. En su lugar, un escaneo confirma la propiedad o el control del dispositivo y la autenticación de sus contenidos no pueden ser refutados razonablemente.

Comprendió que la protección que la 5ta. Enmienda les otorga a las contraseñas numéricas y alfanuméricas debe lógicamente extenderse al método de desbloqueo biométrico, cuyo sentido es idéntico al de las primeras. Es tajante al sostener que la prohibición del testimonio autoincriminatorio no puede limitarse solo a la comunicación verbal o escrita, sino que "los actos que impliquen afirmaciones de hecho" deben considerarse como tales también. Y más aun teniendo en cuenta que, mediante un acto propio como es el sistema de desbloqueo biométrico, se reconoce tanto la posesión, el acceso previo y el control sobre el dispositivo, así como la autenticidad de los documentos digitales almacenados (e incluso desconocidos para la investigación) y que podrían incriminarlo irrefutablemente.

Supre*me Court of Indiana Caso No. 18S-CR-595 Katelin Eunjoo Seo, Appellant (Defendant), 23 de junio de 2020*

Cuando Katelin Seo fue arrestada por la posible comisión de un delito, le fue solicitado su teléfono celular iPhone bajo una orden que les permitía a los policías ingresar en el dispositivo. Al estar bloqueado con una contraseña, se vieron obligados a solicitar la ayuda de la sospechosa, quien se negó.

Esto motivó una segunda orden judicial que dispuso forzar a Katelin a brindar el código de desbloqueo del celular quien nuevamente se rehusó, motivo por el cual se la consideró en desacato a la autoridad.

En la audiencia que siguió, Seo argumentó que obligarla a desbloquear el iPhone violaría su derecho de la 5ta. Enmienda contra la autoincriminación. El tribunal de primera instancia no estuvo de acuerdo y mantuvo a Seo en desacato, concluyendo: "[e] l acto de desbloquear el teléfono no sube al nivel de autoincriminación testimonial". Seo apeló, pero el tribunal de primera instancia confirmó el desacato.

La impugnación de Seo a la orden de desacato del tribunal de primera instancia alega una violación constitucional. La Corte Suprema de Indiana, Estados Unidos, anuló la decisión del Tribunal de Apelaciones y declaró la inconstitucionalidad de la orden de desbloquear un teléfono celular.

Así lo resolvió basándose en la 5ta. Enmienda que protege a cualquier sospechoso de dar a las Fuerzas Policiales datos potencialmente incriminatorios que podrían ser utilizados en su perjuicio, en tanto Seo proporcionaría a las fuerzas de seguridad información que aún no conoce, que luego el Estado podría utilizar en su contra.

En este sentido, explicó la Corte que brindarle a la policía un teléfono inteligente desbloqueado significaría, como mínimo, que 1) el sospechoso conoce la contraseña 2) los archivos del dispositivo existen y 3) el sospechoso posee esos archivos. Y, a menos que el Estado pueda demostrar que ya sabe esta información, los aspectos comunicativos de la producción caen dentro de la Protección de la 5ta. Enmienda. De lo contrario, el acto obligado del sospechoso comunicará al Estado información que no conocía. Lo que no sucedió en el caso. La producción obligada del desbloqueo de un teléfono inteligente es un testimonio y tiene derecho a la protección de la Quinta Enmienda, a menos que el Estado demuestre que se aplica la excepción de conclusión inevitable.

Expresa que incluso si se asume que el Estado ha demostrado que Seo conocía la contraseña a su teléfono inteligente, no ha demostrado que existía algún archivo en particular en el dispositivo o que ella poseía esos archivos. El agente simplemente confirmó que estaría buscando "pruebas incriminatorias" desde el dispositivo. Creía que Seo, para llevar a cabo los presuntos crímenes, estaba utilizando una aplicación o programa de internet para disfrazar su número de teléfono. Sin embargo, el propio testimonio del detective confirmó que no sabía qué aplicaciones o archivos estaba buscando.

III. Registro y secuestro de datos informáticos

III. a. Introducción

El registro y secuestro de datos informáticos es una medida central en la obtención e incorporación de prueba en formato digital a los procesos penales. Con el correr de los años y los desarrollos tecnológicos las personas confiamos el almacenamiento de nuestros datos cada vez más en dispositivos de almacenamiento digital de todo tipo. Los datos personales, bancarios financieros, la documentación societaria, archivos de todo tipo que antes podían encontrase en soportes físicos hoy paulatinamente se reemplazan por dispositivos informáticos. Desde *pendrives*, memorias de almacenamiento SD, discos rígidos y de estado sólido hasta teléfonos celulares. Hoy prácticamente no hay ninguna medida de allanamiento que no incluya medidas vinculadas a la necesidad de registrar y secuestrar elementos informáticos.

En virtud del desarrollo de la tecnología *Internet of Things (IoT)*, una gran variedad de dispositivos, tales como Smart TV, *routers* de acceso a internet, impresoras, cafeteras, etc., almacenan información sobre nosotros.

En este sentido, ante un proceso penal y la necesidad de averiguar la verdad, se hace necesario por parte de los organismos de persecución penal acceder a los datos contenidos en tales dispositivos.

Sin embargo, las legislaciones procesales tanto en el ámbito federal como el de la mayoría de las provincias no prevén una regulación adecuada del registro y secuestro de datos. Salvo algunas normas aisladas en los CPP más modernos, la práctica de nuestros tribunales se basa en la aplicación por analogía y sobre la base del principio de libertad probatoria, que la regularon prevista para el registro y secuestro de cosas físicas en los procesos penales.[1] La diferencia entre las evidencias físicas y digitales es de tal magnitud[2] que requeriría una regulación especial respecto de estas últimas, en atención a su particular naturaleza. Resulta oportuno remarcar la importancia de introducir en los ordenamientos jurídicos legislación específica en el tema, teniendo en cuenta la potencial afectación al derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho al entorno virtual como un derecho omnicomprensivo.[3] Esto porque la información que los usuarios almacenan en los dispositivos informáticos suele estar protegida por normas constitucionales y de los DD. HH. Pensemos en los registros de nuestras conversaciones en aplicaciones de chat en nuestros teléfonos, el historial de nuestras consultas en motores web de búsqueda, como Google, nuestros correos electrónicos, fotos, videos, etc.

En esta sección se detallará el modo en que la jurisprudencia nacional y extranjera ha abordado la obtención y el acceso a datos digitales contenidos en dispositivos de almacenamiento mediante el registro y secuestro de datos. Especial importancia adquiere la distinción entre los requisitos y características de ejecución del secuestro de un dispositivo que contiene datos informáticos (por ejemplo, un teléfono

---

[1] Salt, Marcos, *Nuevos desafíos de la evidencia digital*, 2017, 26; Informe Explicativo del Convenio para la Ciberdelincuencia de Budapest, STE núm. 185, elaborado por el Consejo de Europa. Considerando 184. Accesible en https://rm.coe.int/16802fa403.

[2] Salt, Marcos, *Nuevos desafíos de la evidencia digital*, 2017, 32; Barroso Toledo, Reina, *Revista Faro*, número 13, 2011.

[3] En España puede analizarse la distinción entre estos tres derechos en la Circular 5/2019 de la Fiscalía General del Estado, páginas 3 a 7. Circular de la Fiscalía General del Estado accesible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_5-2019.pdf?idFile=2a2c765e3a04-4656-87c0-8b56ef73d0b6

celular o una computadora) en el marco de un allanamiento o requisa personal y autorización para acceder a su contenido.

III. b. Jurisprudencia argentina

III. b. 1. Fuero federal

Cámar*a Federal de Casación Penal, Sala IV Causa No 17200/2013 "Bejarano, Alexis Ezequiel", 4 de diciembre de 2015*

Alexis Bejarano fue condenado por la comisión de un homicidio calificado con alevosía a la pena de prisión perpetua. Para ello, el tribunal valoró, entre otras cosas, una serie de impresiones obtenidas de la red social Facebook. La defensa de Bejarano interpuso un recurso de casación contra la sentencia. Por esa vía se impugnó que no había mediado orden judicial para extraer de la cuenta de Facebook la información que utilizó el tribunal para fundar su determinación. El recurrente sostuvo que "al ser equiparado el correo electrónico y las redes sociales a la correspondencia epistolar, tal información para que tenga valor probatorio debe ser obtenida por medio de la orden judicial correspondiente, de conformidad con lo establecido en el art. 234 del CPPN". Afirmó que tanto el Ministerio Público Fiscal, como los funcionarios policiales y los jueces del tribunal oral habían incurrido en el tipo penal del art. 153 del C.P. al convalidar y denegar el pedido de nulidad de la obtención sin orden judicial de las impresiones de la red social Facebook.

La Cámara Federal de Casación Penal rechazó el recurso y confirmó la condena. "La red social 'Facebook' es un sitio web que se encuentra disponible para cualquier usuario de la red y se utiliza para que sus usuarios puedan intercambiar comunicación fluida y compartir contenido de forma sencilla a través de internet.

A partir de sus características públicas la página de Facebook propiedad del imputado no goza de la protección de la privacidad como la clásica vía postal. Ello así, desde que, si bien para su funcionamiento y utilización se requiere indispensablemente de un prestador del servicio, el nombre de usuario y clave de acceso destinados a impedir que terceros extraños se entrometan en los datos y contenidos que se emiten y reciben, lo cierto es que el perfil de BEJARANO en la red social

en cuestión era público y casi toda la información que compartía podía ser vista por cualquier persona que accediera a través de internet a la página.

En este sentido, la página de Facebook no puede ser considerada la 'correspondencia epistolar' que protege la Constitución Nacional, razón por la cual el modo en que fue obtenida e incluso su incorporación como prueba al juicio, mal puede violar la garantía contenida en el art. 18 de la CN.

A partir de lo expuesto, la Cámara Federal de Casación Penal entendió que el procedimiento por el cual se obtuvo e incorporó como prueba la página de Facebook mediante la cual se pudo corroborar que el sujeto apodado 'Chucky' se correspondía con el nombre y fotografía que figuraban en ese perfil de la red social fue realizado conforme a las disposiciones legales vigentes sin afectar la garantía que prohíbe intromisiones arbitrarias en la intimidad y privacidad del imputado y por ello propongo rechazar el presente agravio" (voto del juez Hornos, al que adhirieron los jueces Borinsky y Gemignani).

III. b. 2. Fuero nacional

Cámara *Nacional de Apelaciones en lo Criminal y Correccional - Sala 1, Causa CCC 53154/2019, "Soto, Gastón Ernesto y otros s/incidente de nulidad", 31 de octubre de 2019*

La defensa solicitó la nulidad del registro del teléfono celular secuestrado (que Soto habría olvidado en la casa de Roberto Carlos Garzón y Pablo Esteban Goldbaum), así como de los registros de comunicaciones almacenadas en dicho aparato, y de todo lo actuado en consecuencia, basándose en que no se emitió una orden judicial mediante auto fundado, no se notificó a la defensa de ello y no se preservó adecuadamente la evidencia.

El Tribunal, luego de interpretar el criterio restrictivo en materia de nulidades (artículos 2 y 166 del CPPN) dijo que *el estudio del teléfono no se materializó hasta después de que la fiscalía aclarara el alcance de su orden primigenia y el juzgado, en la voz de su secretario, indicara que* "dada la urgencia del caso en virtud de que el teléfono celular podría arrojar información sobre los autores del hecho, se autoriza por medio de consulta telefónica a que se perite el teléfono secuestrado a

los efectos de recabar la información útil para establecer la identidad del o los autores del hecho. Todo ello acorde a lo normado por el Art. 236 CPPN".

Efectivamente, ambas comunicaciones se realizaron el 8 de julio de 2019 antes de las 14.11 hs. y, conforme se observa de la planilla de custodia, el celular fue entregado por el inspector Claudio G. Cabezas al oficial primero José M. Pons ese día a las 18.15 hs., tras lo cual este hizo lo mismo con el oficial Juan Manuel González a las 16.36 hs. del 10 de julio de 2019 en un sobre cerrado y firmado. A mayor abundamiento, el licenciado Santiago Pociello Argerich, auxiliar "c" de la División Análisis de Inteligencia Informática de la Policía de la Ciudad, dejó constancia de que procedió a la apertura del aparato el 12 de julio de este año en presencia de dos testigos, de acuerdo con lo solicitado por oficio judicial de fecha 11 del mismo mes.

La mera falta de asentamiento de la anuencia del juez no permite sostener válidamente que ello no fuera así. Asimismo, la omisión de notificar a la defensa responde a que no se había individualizado a ninguna de las personas que habrían cometido el hecho denunciado. Además, explica el Tribunal que *el teléfono fue envuelto en papel de aluminio para resguardar la información– se efectuó en presencia de dos testigos y la planilla de cadena de custodia no refleja movimientos que avalen la postura de la parte, máxime cuando los damnificados habían reconocido al hombre que aparece en la foto de fondo de pantalla del dispositivo antes de este procedimiento.*

El Tribunal concluyó diciendo que *lo actuado se ajustó a las previsiones del artículo 233 del código adjetivo, dado que la operación tuvo por fin obtener una copia espejo de la totalidad del contenido de la cosa. Por lo tanto, corresponde rechazar los agravios por aplicación del principio "pas de nullité sans grief" (no hay nulidad sin perjuicio).*

Por ello, el Tribunal resolvió confirmar el auto apelado que rechazaba la nulidad.

Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala 1, Causa N° CCC 47967/2019, "Sandoval, Natalia Patricia s/incidente de nulidad", 12 de noviembre de 2020

Los imputados solicitaron la nulidad del secuestro del teléfono celular por haber sido dispuesto sin orden fundada y, a su vez, que en el momento del procedimiento policial no existían indicios suficientes

para afirmar la intervención de la nombrada en los hechos denunciados. Por otro, indicó que la creación de una copia de seguridad con los datos contenidos en dicho dispositivo era una medida desproporcionada que inevitablemente genera tensión entre el derecho a la intimidad y el interés del Estado en la averiguación de la verdad.

El Tribunal concluyó que las decisiones en crisis deben ser confirmadas. Esto porque *el secuestro del aparato en posesión de la encausada fue ordenado telefónicamente por el juzgado instructor luego de que el oficial Pablo Gabriel Zalazar (quien describió con claridad las circunstancias que motivaron su intervención) promoviera la consulta correspondiente, de modo que la diligencia contó con el debido control judicial y se ajustó a los términos del artículo 231 del CPPN. La norma de cita no establece ni orden escrita, ni fundada, ni un standard probatorio determinado, como parecería cuestionar la defensa en su planteo, la que tampoco informa de qué precepto del ordenamiento positivo derivarían estas supuestas exigencias.*

Respecto a la oposición a la extracción de datos a partir de la copia de seguridad autorizada por el juzgado tampoco ha de prosperar. El Tribunal dice que, *en concreto, resulta aplicable lo dispuesto por el artículo 233 del código de forma, que prevé la facultad del juez de "ordenar la obtención de copias o reproducciones de las cosas secuestradas cuando estas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la instrucción". En atención a ello, no parece desproporcionado proceder de esa manera en pos de cumplir con la finalidad de la instrucción (artículo 193 del CPPN).*

Por ello, el Tribunal resolvió confirmar el auto apelado que rechazaba la nulidad.

Cámara *Nacional de Apelaciones en lo Criminal y Correccional - Sala 4 –, Causa N° CCC 81978/2018, "Morales, Sergio Daniel y otros s/incidente de nulidad", 20 de septiembre de 2019*

Los imputados solicitaron la nulidad del acceso a la información existente en los teléfonos incautados porque esta medida no fue notificada a la defensa. El Tribunal calificó la apertura de los teléfonos celulares como la obtención de una copia de la información que obraba en los aparatos, es decir, la guarda en un soporte informático de los datos que estaban almacenados en el dispositivo mencionado. En este contexto,

la defensa alegó una manipulación del teléfono sin intervención de la defensa, lo que, a su criterio, implicaría la nulidad de esa actuación.

El Tribunal dijo que *el agravio no puede prosperar por cuanto la operación realizada por la Dirección de Inteligencia Informática de la Policía de la Ciudad no constituye un peritaje, sino que corresponde equipararla al resguardo de elementos preservados en un dispositivo que había sido ya legalmente incautado en el legajo. Una vez reservado el elemento físico (el teléfono celular), la diligencia encargada para proceder a la copia de los datos acumulados en su interior no constituye una pericia en tanto operación que valore o dictamine en función de una especialidad científica o técnica (artículo 253, a contrario sensu, del CPPN), y por lo tanto la omisión puesta de resalto por los recurrentes (*falta de notificación a la defensa*) no acarrea su invalidez, ya que resulta aplicable el artículo 233 del digesto ritual, que no contiene el requisito en cuestión, y que regula la facultad del juez de obtener copias o reproducciones de las cosas secuestradas.*

En el caso, parece factible recurrir al artículo 144 de la Ley 27.063 como pauta interpretativa, que regula el registro de un sistema informático o de un medio de almacenamiento de datos informáticos o electrónicos con el objeto de secuestrar los componentes del sistema, obtener una copia o preservar datos o elementos de interés para la investigación. Dicha diligencia no constituye un peritaje (regulado en el artículo 161 y sstes. del Código Procesal Penal Federal) ni exige notificación previa a la defensa.

A la luz de ello, el contenido de los elementos que obran en el legajo debe ser interpretado como datos informáticos de índole documental, que la jueza de grado ordenó que sean incorporados a la causa.

Los apelantes también pusieron en duda la cadena de custodia de los teléfonos que, a su criterio, no habría garantizado suficientemente la inmutabilidad de su contenido al momento de su manipulación. El Tribunal sobre este punto dijo que *solo procede su declaración cuando, por la violación de las formalidades, resulta un perjuicio real, actual y concreto para la parte que las invoca, mas no en los casos en que estas se plantean en el único interés de la ley o para satisfacer formalidades desprovistas de aquel efecto perjudicial (en ese sentido, CSJN, B. 66 XXXIV, "Bianchi, Guillermo Oscar s/ defraudación", del 27/6/02 y A. 63 XXXIV, "Acosta, Leonardo y otros s/ robo calificado en grado de tentativa", del 4/5/00). El personal policial consignó haber colocado los dispositivos en "modo avión" a fin de no recibir ni emitir datos, conectándolos seguida-*

mente a un ordenador de la dependencia y logrando la duplicación de su contenido mediante el software *"UFED 4PC", comúnmente utilizado para la extracción forense de información existente en equipos de telefonía móvil y afines, de lo que no puede deducirse ninguna irregularidad en la manipulación de los aparatos secuestrados.* Por ello, el Tribunal resolvió confirmar el auto apelado que rechazaba la nulidad.

Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VI,". Causa No 39.427. "R., R. y otros". Causa No 39.427, 14 de junio de 2010

Una empresa dedicada a brindar servicios de consultoría informática y licenciar *software* para la optimización de procesos contrató, en relación de dependencia y como gerentes de consultoría, a dos personas. Precisó que sus empleados al ingresar firman un convenio de confidencialidad tendiente a preservar la información que allí se maneja. La empresa, al realizar una copia de seguridad de sus computadoras, advirtió que ambos tenían documentos que describían acciones y tácticas para captar sus proyectos y presentarlos como propios a través de otra compañía. La política de la empresa, en estos casos, consistía en guardar también otra copia con ese material en su servidor.

La empresa tomó conocimiento que estas dos personas, los imputados, tenían previsto transferir a ciertos empleados a otra empresa. El empleador las denunció por los delitos de concurrencia desleal, estafa, defraudación por administración fraudulenta y violación de secretos y aportó, como prueba, los archivos en cuestión. El juzgado de instrucción anuló el acto por el que se incorporó la prueba. El empleador –constituido en querellante– interpuso recurso de apelación.

La Sala VI de la Cámara de Apelaciones, por unanimidad, rechazó el recurso y confirmó la nulidad resuelta en primera instancia. En efecto, indicó las empresas les asignan a los empleados distintas "herramientas laborales" dentro de las que se encuentran computadoras personales, portátiles y cuentas de correo electrónico, entre otras y que junto a ellas se les proporciona una clave o *password* que les garantiza confidencialidad en sus comunicaciones y archivos personales, lo cual ya sugiere su carácter privado.

Por tal motivo, el ingreso a su contenido y su eventual utilización como prueba puede conculcar elementales garantías individuales, fundamentalmente de raigambre constitucional, que ya se han extendido a estos nuevos soportes aportados por la tecnología moderna.

Sostuvo que las Cortes de los países europeos y sudamericanos en su jurisprudencia y doctrina, casi unánimemente avalan la postura, sobre la base de que el e-mail además de su traducción (correo) es la comunicación escrita en computadora, enviada o recibida vía internet y que documentos privados son los que están en el archivo de una computadora con una clave personal.

De ello se desprende que la orden judicial fundada sería indispensable para la intromisión en ese marco de intimidad.

Asimismo, destacaron como característica del correo electrónico la opinión vertida por el Dr. Donna en la causa n° 20.009 del registro de la Sala I, al concluir *que dentro de los derechos de una persona, ya sea como derivación del de la propiedad o como un derecho autónomo a la intimidad, existe un derecho a que se respeten por parte del Estado aquellos ámbitos privados donde sus titulares han exhibido un interés en que así se mantengan...esa expectativa de respeto a los ámbitos privados, se vería claramente reflejada en que el correo electrónico posee características de protección de privacidad más acentuadas que la tradicional vía postal –que por otra parte, sí posee garantía de protección expresa en el art. 18 de la C.N.–, ya que para su funcionamiento se requiere un prestador de servicio, el nombre de usuario y un código o contraseña de acceso, que impide el acceso de terceros a él* (autos 'Yelma, Martín y otros', resuelta el 22/4/2003).

A su vez, se hizo referencia a que, *en función de las previsiones constitucionales mencionadas, es el empleador quien tiene prohibido, en principio, leer e-mails enviados o recibidos por sus empleados. El contenido de tal prohibición no es otro que la violación del derecho de privacidad del trabajador, facultad que no comporta un elemento configurativo del débito contractual y que, por ello, hace a la indiscutible e impenetrable dignidad y autodeterminación que como sujeto titulariza...* (CCC, Sala IV, causa no 25.065, 'Redruello', resuelta el 15/11/04)" (voto de los jueces Lucini y Filozof).

El Tribunal destacó que la empresa, con conocimiento de comentarios sociales sobre el comportamiento desleal, no haya aprovechado la oportunidad del *back up* para obtener datos que den certeza a esas sospechas.

Finalmente, determinó que no hay duda de que la computadora y el correo electrónico asignados son instrumentos de trabajo en nuestros días, pero ello de modo alguno permite a una empresa avanzar sobre sus contenidos avasallando derechos de primera jerarquía.

Cámara Nacional de Apelaciones en lo Criminal y Correccional, sala VI
Causa N.º 37443, sala VI, 31 de julio de 2018

En junio de 2018, la policía detuvo a dos personas por haber presuntamente robado un teléfono celular de una persona mientras se encontraba en la parada de un colectivo. En el procedimiento, uno de los agentes inspeccionó el dispositivo sustraído para desbloquearlo, retirar el chip y colocarlo en el suyo para llamar al primo de la víctima y, de este modo, confirmar que el dispositivo era robado.

La defensa de uno de los detenidos planteó la nulidad del registro realizado por la policía pues no existió urgencia ni peligro alguno de perder información necesaria para ubicar al damnificado, por lo que la inspección del aparato habría sido ilegal. El juzgado de primera instancia rechazó la nulidad.

En la apelación, la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional declaró la nulidad del registro del celular y de todo lo actuado en consecuencia. Asimismo, sobreseyó al joven y dispuso su libertad. Consideró: *El personal policial se excedió en los límites que la ley fija a sus facultades de intervención ya que no se vislumbra una situación de urgencia o gravedad que lo legitimara a actuar de tal forma (...) Actualmente la prueba física y la digital comparten los mismos fundamentos del modelo de la criminalística en lo que refiere a minimizar la contaminación en el lugar del hecho. Utilizar los principios y estándares establecidos es el objetivo primario para la admisibilidad de la evidencia [...]. Es decir que la actuación policial estaría vedada no solo por su deber de resguardo de la intimidad, sino también por la idoneidad requerida para operar un instrumento electrónico pasible de ser objeto de prueba. Por otro lado se ve afectado el derecho de defensa del imputado pues la parte no tuvo oportunidad de controlar la prueba que en este caso derivó en la forma en la que se habría dado con el damnificado que se realizó sin la presencia de testigos, medida que así resultó irreproducible (...)* [*E*]*s un principio garantizador tan básico que, si no se lo cumple, las restantes garantías dejan de desarrollar su función específica y es el derecho intangible que tiene todo ciudadano a responder a los cargos que se le realicen en el curso de un proceso penal y actúa en forma conjunta con las demás garantías y las torna operativas. De ahí la importancia de su resguardo* (...) *[El] artículo 18 [de la Constitución Nacional] dispone la inviolabilidad del domicilio, la correspondencia epistolar y los papeles privados. No*

*caben dudas a que dentro de esa enunciación quedan comprendidas también las comunicaciones realizadas mediante correos electrónicos, llamados telefónicos o mensajes de texto, entre otros. Sobre ello prácticamente no hay controversia jurisprudencial ni doctrinaria y los avances tecnológicos día a día establecen nuevas formas de relacionarnos lo cual convierte a tal enumeración en simples ejemplos (...) La protección tiene por finalidad garantizar el respeto a la vida privada de la persona, aún en sus ámbitos más íntimos, por lo que resulta difícil excluir a los registros audiovisuales que un individuo conserva en su computadora personal, sea en una memoria de almacenamiento (*pendrive*) o, como en este supuesto, en un teléfono móvil con información extraída de un chip que no es más que el eventual listado de llamadas que con él se realizaron. El avance de la tecnología y el desarrollo de los medios de comunicación obligan, necesariamente, a extender el resguardo a todos aquellos objetos que se encuentran "dentro de la esfera de custodia de cada individuo" y que contengan datos de su vida privada, u otras cuestiones personales que desea preservar [...], debiéndose destacar que, si bien estaba en duda la titularidad del bien, lo expuesto debe ser ampliamente interpretado, abarcando aquí el secuestrado en poder del imputado (...) No hay dudas que de actuar correctamente y conforme las disposiciones del Fiscal –que vela por la legalidad del proceso– y de la autoridad judicial, se habría llegado de todos modos a la identificación de la víctima. Bastaba con un simple peritaje. Pero ello no puede utilizarse para justificar el accionar del policía pues estaríamos haciendo de la excepción la regla y permitiendo la extralimitación de los funcionarios en casos tan simples como el que nos ocupa. En definitiva, [...] debemos seguir un criterio restrictivo en la aplicación de la excepción, no aplicable en este supuesto, para que no se convierta la doctrina del descubrimiento inevitable en un vehículo que derogue el derecho de todos los ciudadanos a estar libres de las intromisiones ilegales del Estado.*

III. c. Jurisprudencia internacional

III. c. 1. Corte Interamericana de Derechos Humanos

Corte *Interamericana de Derechos Humanos, Escher y otros v. Brasil CIDH, 06 de julio de 2019*

Los hechos del presente caso se producen en un contexto de conflicto social relacionado con la reforma agraria en varios Estados de Brasil, entre ellos Paraná. Arlei José Escher, Dalton Luciano de Vargas, Delfino José Becker, Pedro Alves Cabral y Celso Aghinoni eran miembros de dos organizaciones sociales, ADECON y COANA. La primera tenía como objetivo el desarrollo comunitario y la integración de sus asociados a través de actividades culturales, deportivas y económicas, mientras que la segunda buscaba integrar a los agricultores en la promoción de las actividades económicas comunes y en la venta de los productos. Las dos organizaciones mantenían alguna relación de hecho con el MST, con el cual compartían el objetivo común de promover la reforma agraria.

Entre abril y junio de 1999 miembros de la policía presentaron a una autoridad judicial una solicitud de interceptación y monitoreo de una línea telefónica, instalada en la sede de COANA, en tanto presumían que en dicho lugar se estarían realizando prácticas delictivas. La solicitud fue otorgada de manera expedita y sin fundamentación. La solicitud mencionaba supuestos indicios de desviaciones por parte de la directiva de COANA de recursos financieros concedidos a través del Programa Nacional de Agricultura Familiar (PRONAF) y del Programa de Crédito Especial para la Reforma Agraria (PROCERA), a los trabajadores del Asentamiento Pontal do Tigre en el municipio de Querencia do Norte. Asimismo, se refería al asesinato de Eduardo Aghinoni, *cuya autoría [...] est[aba] siendo investigada y [se sospechaba que] entre los motivos de tal crimen [estaba el] desvío de los recursos, ya especificados*

Los peticionarios interpusieron una serie de recursos judiciales a nivel nacional para que destruyesen las cintas grabadas. Sin embargo, las solicitudes fueron rechazadas por las autoridades judiciales de Brasil. El 7 de junio de 1999 por la noche, extractos de los diálogos grabados fueron reproducidos en el Jornal Nacional, uno de los noticieros televisivos de alcance nacional de mayor audiencia en el país.

El 8 de junio de 1999 por la tarde, el ex secretario de seguridad realizó una conferencia de prensa con periodistas de diversos medios, en la cual comentó la actuación de la policía en las operaciones de desalojo de los campamentos del MST; brindó explicaciones respecto de las interceptaciones telefónicas, y expuso su opinión sobre las conversaciones divulgadas, y las providencias que la Secretaría de Seguridad adoptaría al respecto. En esa conferencia de prensa se reprodujo el audio de algunas de las conversaciones interceptadas, y por medio de la asesoría de prensa de la Secretaría de Seguridad se entregó a los periodistas presentes un material con extractos transcritos de los diálogos interceptados de los miembros de COANA y ADECON.

Las personas involucradas solicitaron que se destruyesen las grabaciones. Además, la fiscalía sostuvo, entre otras cuestiones, que la policía militar no tenía legitimidad para solicitar la intervención telefónica y que el pedido había sido elaborado de modo aislado, sin que existiera una investigación en curso. En consecuencia, requirió que se declarara la nulidad de las intercepciones y la inutilidad de las grabaciones. El juzgado rechazó el planteo por considerar que no se encontraba probada la ilegalidad de las interceptaciones; sin embargo, ordenó la incineración de las grabaciones.

La Corte Interamericana de Derechos Humanos consideró que Brasil era responsable por la violación de los artículos 11 (derecho a la vida privada y derecho a la honra y a la reputación) y 16 (derecho a la libre asociación) de la Convención Americana de Derechos Humanos.

En efecto, sostuvo: *(...) El artículo 11 de la Convención prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, enunciando diversos ámbitos de esta, como la vida privada de sus familias, sus domicilios o sus correspondencias. En ese sentido, la Corte ha sostenido que "el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública". Aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación incluida dentro del ámbito de protección de la vida privada. El artículo 11 protege las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla. De ese modo, [...] se aplica a las conversaciones telefónicas independientemente de su contenido e incluso,*

puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación. (...) La fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. Este progreso, en especial cuando se trata de interceptaciones y grabaciones telefónicas, no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o a los particulares. De allí que el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada (...) *Como las conversaciones telefónicas de las presuntas víctimas eran de carácter privado y dichas personas no autorizaron que fueran conocidas por terceros, su interceptación por parte de agentes del Estado constituyó una injerencia en su vida privada. Para que resulte conforme a la Convención Americana una injerencia debe cumplir con los siguientes requisitos: a) estar prevista en ley; b) perseguir un fin legítimo, y c) ser idónea, necesaria y proporcional. En consecuencia, la falta de alguno de dichos requisitos implica que la injerencia es contraria a la Convención.*

A su vez, determinó: *La divulgación de conversaciones telefónicas que se encontraban bajo secreto de justicia por agentes del Estado implicó una injerencia en la vida privada, la honra y la reputación de las víctima (...) La Corte considera que guardar secreto de las conversaciones telefónicas interceptadas durante una investigación penal es un deber estatal: a) necesario para proteger la vida privada de las personas sujetas a una medida de tal naturaleza; b) pertinente para los efectos de la propia investigación, y c) fundamental para la adecuada administración de justicia. En el presente caso, se trataba de información que debía permanecer solo en conocimiento de un reducido número de funcionarios policiales y judiciales y el Estado falló en su obligación*

de mantenerla con el resguardo debido (...) Las decisiones que adopten los órganos internos que puedan afectar derechos humanos deben estar debidamente motivadas y fundamentadas, pues de lo contrario serían decisiones arbitrarias. Las decisiones deben exponer, a través de una argumentación racional, los motivos en los cuales se fundan, teniendo en cuenta los alegatos y el acervo probatorio aportado a los autos. El deber de motivar no exige una respuesta detallada a todo argumento señalado en las peticiones, sino puede variar según la naturaleza de la decisión. Corresponde analizar en cada caso si dicha garantía ha sido satisfecha. En los procedimientos cuya naturaleza jurídica exija que la decisión sea emitida sin audiencia de la otra parte, la motivación y fundamentación deben demostrar que han sido ponderados todos los requisitos legales y demás elementos que justifican la concesión o la negativa de la medida. De ese modo, el libre convencimiento del juez debe ser ejercido respetándose las garantías adecuadas y efectivas contra posibles ilegalidades y arbitrariedades en el procedimiento en cuestión.[4]

III. c. 2. Estados Unidos

Corte *Suprema de Justicia de Estados Unidos, Riley v. California, 573 U.S. 373, 25 de junio de 2014*

David León Riley pertenecía a una pandilla criminal del Parque Lincoln de la ciudad de San Diego, California en EE. UU. El 2 de agosto de 2009, él y otros miembros de su banda efectuaron disparos a una banda rival cuando estos pasaron en su automóvil por el lugar donde Riley y sus compañeros se encontraban. Luego, los que efectuaron los disparos se subieron al automóvil propiedad de Riley y escaparon del lugar. El 22 de agosto de 2009 la policía detuvo a Riley mientras manejaba un automóvil diferente por estar conduciendo con un registro de conducir vencido.

Dado que el registro de conducir estaba suspendido la policía estaba obligada a secuestrar el vehículo. Antes de secuestrar un vehículo la

[4] Ministerio Público de la Defensa, Secretaría General de Capacitación y Jurisprudencia. https://jurisprudencia.mpd.gov.ar/

policía está obligada a realizar un registro e inventario para verificar que el vehículo tiene todos sus componentes al momento del secuestro a los efectos de resguardarse de un posible reclamo civil futuro y para descubrir artículos de contrabando ocultos.

Durante el registro la policía encontró dos armas de fuego y detuvo en consecuencia a Riley por posesión de dichas armas. Riley tenía su teléfono celular en su bolsillo al momento de su detención, por lo que un detective de la Unidad de Pandillas analizó videos y fotografías de Riley realizando gestos y signos de pandilla como otros indicios de pertenencia a pandillas que estaban alojados en el dispositivo para determinar si Riley pertenecía o era miembro de alguna pandilla. Riley fue luego vinculado al hecho del 2 de agosto a partir de peritajes balísticos y en consecuencia también se le imputó además el haber disparado a un vehículo ocupado, tentativa de homicidio y lesiones graves con arma de fuego semiautomática.

Antes del juicio oral, Riley solicitó que se declare la nulidad de la evidencia relacionada con su pertenencia a una pandilla criminal obtenida a través de su teléfono celular. Su solicitud fue denegada. Durante el juicio, un experto en pandillas declaró que Riley era miembro de la pandilla de Lincoln Park, los rivales que tenían esa pandilla y las razones por las cuales los disparos efectuados habrían estado relacionados con la actividad de las pandillas. El jurado condenó a Riley por los tres hechos. La Cámara de Apelaciones del Estado de California confirmó la condena.

El caso llegó a la Corte Suprema de Justicia en la que se planteó si la evidencia obtenida del registro del teléfono celular de Riley admitida en el juicio en su contra violó su inmunidad contra registros irrazonables establecido en la Cuarta Enmienda de la Constitución.

El máximo tribunal de aquel país revocó la sentencia. La opinión unánime fue escrita por el presidente de la Corte, el juez John Roberts. Se sostuvo que la excepción para registros sin orden judicial luego de una detención existe con el único propósito de preservar la integridad física del oficial de policía y para preservar la evidencia. Ninguna de esas cuestiones se encuentra en juego en el registro de datos digitales. Se determinó que los datos digitales no pueden ser utilizados como armas en contra de los oficiales involucrados en la detención y la posibilidad de preservar la evidencia contenida en un dispositivo digital mientras se obtiene la orden judicial se materializa con la desconexión

del aparato y su inserción en una "bolsa de Faraday" (dispositivo de almacenamiento que no permite el paso de ondas electromagnéticas).

En particular, se dijo: *Los teléfonos celulares difieren tanto en un sentido cuantitativo como en un sentido cualitativo de otros objetos que podrían mantenerse en una persona del arrestado. El término "teléfono celular" es en sí mismo una taquigrafía engañosa; muchos de estos dispositivos son, de hecho, minicomputadoras que también tienen la capacidad de ser utilizadas como un teléfono [...]. Una de las características distintivas más notables de los teléfonos celulares modernos es su inmensa capacidad de almacenamiento. Antes de su uso, la investigación sobre una persona se encontraba limitada por las circunstancias físicas y tendía a significar solo una estrecha intrusión en la privacidad... Sin embargo, la posible intrusión en la privacidad no se halla limitada físicamente de la misma manera cuando se trata de celulares [...]. La capacidad de almacenamiento de los teléfonos celulares tiene varias consecuencias interrelacionadas para la privacidad. En primer lugar, en un solo lugar se recolecta una gran variedad de información –una dirección, una nota, una receta, un extracto bancario, un video– que revela mucho más en combinación que cualquier grabación. En segundo lugar, la capacidad de un teléfono celular permite incluso que la información pueda transmitir mucho más que antes. La suma de la vida privada de un individuo puede ser reconstruida a través de mil fotografías etiquetada son fechas, lugares y descripciones; lo mismo no puede ser realizado a través de una fotografía o dos de sus seres queridos metidos en una billetera. En tercer lugar, los datos de un teléfono pueden remontarse al momento de su compra o incluso antes [...]. Finalmente, hay un elemento de omnipresencia que caracteriza a los teléfonos celulares, pero no a los registros físicos. Antes de la era digital las personas normalmente no llevaban un caché de información personal sensible con ellos. Ahora la excepción es la persona que no lleva un celular [...]. [N]o es exagerado sostener que [...] más del 90% de los adultos estadounidenses que poseen un teléfono celular mantienen [...] un registro digital de casi todos los aspectos de sus vidas, desde lo mundano a lo íntimo [...]. Permitir a la policía escrutar dichos registros de forma rutinaria es muy diferente a permitir, ocasionalmente y en un caso concreto, el registro de uno o dos elementos personales. Aunque los datos almacenados en un teléfono celular se distinguen de los registros físicos solo por cantidad, los tipos de datos también son cualitativamente diferentes. El historial de búsqueda y navegación en internet,*

por ejemplo, se puede encontrar en un teléfono. Esto podría revelar los intereses o preocupaciones privadas de una persona [...]. Los datos en un teléfono celular también pueden revelar dónde ha estado localizada la persona, y puede reconstruir los movimientos específicos de alguien minuto a minuto, no solo alrededor de la ciudad sino también dentro de un edificio particular... Nuestra consideración, por supuesto, no es que la información en un teléfono celular sea inmune a su inspección; es, en cambio, que se requiera una orden de registro antes de tal registro, incluso cuando sea incautado en la detención. Nuestros casos han reconocido históricamente que el requisito de la orden es "una parte importante de nuestra maquinaria de gobierno", no simplemente "un inconveniente para de alguna manera ser 'sopesada' contra las afirmaciones de eficiencia policial" (...) Los teléfonos celulares modernos no son solo otro medio tecnológico. Con todo lo que contienen y pueden revelar, contienen para muchos estadounidenses "la privacidad de la vida" [...]. El hecho de que la tecnología ahora permita que un individuo lleve tal información en su mano no hace que la información sea menos digna de la protección por la que lucharon los constituyentes. Nuestra respuesta a la cuestión sobre qué debe hacer la policía antes de registrar un teléfono incautado es también simple: obtener una orden judicial.

Distri*ct Court, Massachusetts, U. S., Alasaad v. McAleenan - Summary Judgment Order, 12 de Nov. 2019*

Un grupo de 10 ciudadanos norteamericanos demandó al gobierno norteamericano (Dept. Homeland Security, ICE, CBP) por considerar que los registros y, en algunos casos, confiscaciones de sus teléfonos celulares y dispositivos electrónicos en las fronteras (pasos fronterizos y aeropuertos) violaron sus derechos constitucionales. Específicamente alegaron que se violaba la 4ta. enmienda (protección contra registros y allanamientos ilegales) y la 1ra. enmienda (protección a la libre expresión). Solicitaron la desactivación de las políticas ilegales implementadas por las agencias federales demandadas, así como también la eliminación de todos los datos y registros obtenidos de sus dispositivos electrónicos. Respecto de la violación a la 4ta. enmienda, alegaron que los registros de los dispositivos se realizaron sin orden judicial.

Los demandados contestaron que existe una excepción al requerimiento de orden judicial para registrar personas o sus bienes cuando se trata de lugares fronterizos (incluidos aeropuertos) y que tal excepción

se funda en el derecho de ejercer autoridad soberana, sujeto a limitaciones, para controlar a quienes ingresan al país. Si bien la excepción no habilita un registro sin límite alguno, sí implica una expectativa reducida de privacidad para todas aquellas personas que ingresen al territorio. Esa excepción fue reconocida en la jurisprudencia.

La Corte Suprema de EE. UU. tiene establecido que los registros rutinarios pueden realizarse sin orden judicial y sin que exista sospecha o indicio alguno, causa probable. Por el contrario, sostiene que aquellos controles no rutinarios requieren un estándar más estricto de causa probable.

Los demandados alegaron que tienen la tarea de monitorear el ingreso de millones de personas que viajan por día a Estados Unidos y que, gracias a la práctica de registrar dispositivos electrónicos en la frontera, se desarticularon amenazas a la seguridad nacional y de terrorismo como así también se información relativa a hechos de contrabando y otras actividades ilegales. No obstante, los demandados no demostraron la naturaleza o la frecuencia de dichos resultados o si estos no podrían haber sido obtenidos aplicando estándares de sospecha más elevados.

El tribunal determinó que los registros de dispositivos electrónicos en la frontera no entran en la categoría de "registros rutinarios" dada la escala y cantidad de información personal que contienen, la sensibilidad por naturaleza de dicha información y su extrema portabilidad que determina que es poco probable e irreal suponer que un viajero dejará dichos dispositivos en su casa antes de viajar.

El tribunal estableció también que si bien no es necesaria una orden judicial para registrar dispositivos electrónicos en la frontera, las agencias gubernamentales sí deben tener una "sospecha razonable" para hacerlo. Este grado de sospecha debe estar fundamentado en hechos específicos y articulables.

III. c. 3. España

Tribu*nal Supremo, Sala de lo Penal, Sentencia núm. 332/2019, 27 de junio de 2019*

Un hombre fue condenado por los delitos de agresión sexual, producción de pornografía infantil, posesión de pornografía infantil y descubrimiento y revelación de secretos. En el transcurso de la investigación

preparatoria se allanó su domicilio y se secuestraron distintos elementos informáticos: varias computadoras, memorias USB, discos duros, discos en formato CD y DVD, tarjetas de memoria, entre otros. Al ingresar a los elementos secuestrados se encontraron imágenes, videos y chats que demostraban la materialidad de los hechos investigados y denunciados.

En su recurso de apelación ante el Tribunal Supremo, el imputado impugnó la condena alegando que se accedió de forma irregular a unas computadoras y material informático, sin autorización y sin la existencia de una resolución judicial motivada que habilitaba a los agentes para ello. Destacó que no existió su consentimiento para que se recolectaran los efectos informáticos existentes en el interior del inmueble, pues solo había consentido para que su domicilio fuera revisado. Por otra parte, indicó que su computadora se encontraba protegido por una contraseña y que esta fue violada sin su consentimiento.

El Tribunal, en su resolución, indicó que el consentimiento había sido expreso y con asistencia letrada, tanto para el ingreso al domicilio como para también al secuestro, registro y análisis de los elementos informáticos.

Recordando una sentencia anterior, el Tribunal afirmó: *la necesidad de esta autorización judicial (subsidiaria del consentimiento: si el afectado accede de forma libre, no hay cuestión) obedece a la consideración de estos instrumentos como esferas de almacenamiento de una serie compleja y densa de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones tuteladas por el art 18.3 CE; contactos, fotografías, archivos personales, tuteladas por el art 18 10 CE ; datos personales y de geolocalización, que pueden cobijarse en el derecho a la protección de datos, art 18 40 CE).*

La sala citó también su jurisprudencia anterior en tanto *que En STC. 142/2012 de 2.7, se precisa que debe delimitarse es si el acceso a los datos del ordenador es un acto con solo incidencia en el derecho a la intimidad (art. 18.1 CE) o alcanza también al derecho al secreto de las comunicaciones (art. 18.3 CE), lo que, en última instancia, tiene relevancia por el diferente régimen constitucional de protección de ambos derechos. A esos efectos, cabe recordar que este Tribunal ha señalado que si bien, de conformidad con el art. 18.3 CE, la intervención de las comunicaciones requiere siempre resolución judicial, no existe en el art. 18.1 CE esa misma garantía de previa resolución judicial respecto del derecho a la intimidad personal, de modo que excepcionalmente*

se ha admitido la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, STC 281/2006, de 9 de octubre, FJ 9).

El Tribunal desestimó en su totalidad todos los agravios del recurrente y confirmó la condena impuesta.

III. c. 4. Tribunal Europeo de Derechos Humanos

Tribu*nal Europeo de Derechos Humanos, Caso 459/2018, SABER c. NORUEGA, 459/2018, 17 de diciembre 2020*

El demandante Mohammed Imran Saber, ciudadano noruego, alegó vicios en las actuaciones relativas al registro y la incautación de datos de su teléfono inteligente, en el que había correspondencia entre él y sus abogados. Al respecto, se había hecho una copia en espejo (o copia *bit a bit*) del teléfono, ya que la policía necesitaba registrarlo. Cuando se llevaron el teléfono, el demandante declaró que contenía correspondencia con dos abogados que lo defendían en otro caso penal, en el que era sospechoso, y con otros abogados más. Por ende, había parte del contenido de la copia *bit a bit* que estaría exenta de incautación en virtud de los artículos 204 y 119 del Código de Procedimiento Penal de Noruega.

El Tribunal Superior tomó como punto de partida el primer apartado del artículo 204 del Código de Procedimiento Penal, según el cual los documentos sobre cuyo contenido un testigo tendría derecho a negarse a declarar estaban exentos de incautación. Según el artículo 119, un tribunal no está autorizado a tomar declaración a los abogados sobre asuntos que les hayan sido comunicados en su calidad de tales. Según el Alto Tribunal, era la autoridad fiscal la que tenía la competencia principal para tomar decisiones sobre la incautación, así como la responsabilidad principal de garantizar que las incautaciones no se decidieran con respecto a los datos que estaban exentos de incautación. Al llevar a cabo dicho examen, la autoridad fiscal tendría que filtrar cualquier dato que pudiera estar exento de incautación. Estos datos deberían devolverse al solicitante o eliminarse sin necesidad de una nueva inspección. Tras la decisión, la copia en espejo fue remitida a

la policía para su registro. Este registro fue entonces realizado por la propia policía, sin ningún control por parte del tribunal regional en esta fase.

El demandante se quejó de que permitir a la policía llevar a cabo un examen introductorio de su teléfono inteligente con el fin de filtrar los datos que podrían estar exentos de incautación, supuso una violación del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales que dice que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

El TEDH comenzó diciendo que es indiscutible entre las partes que el registro del teléfono inteligente del demandante y/o la copia en espejo de este, supuso una injerencia en su derecho al respeto de su correspondencia en virtud del primer párrafo del artículo 8 del Convenio, y considera que esto no puede ser cuestionado. El Tribunal determinó que se debía analizar si en el acceso a la correspondencia entre el demandante y sus abogados que podía obtenerse a través de la copia *bit a bit* de su teléfono, la ley en cuestión tenía suficiente calidad y ofrecía suficientes garantías para asegurar que la confidencialidad no se viera comprometida durante el procedimiento de registro e incautación. En el contexto de los registros y las incautaciones, el derecho interno debe proporcionar cierta protección al individuo contra la injerencia arbitraria en los derechos del artículo 8. Así, la legislación nacional debe ser lo suficientemente clara en sus términos para dar a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades públicas están facultadas para recurrir a tales medidas.

El TEDH enfatizó la importancia de la confidencialidad de la relación cliente-abogado y la necesidad de su protección. El Tribunal de Justicia observó que el Código de Procedimiento Penal no incluía ninguna disposición expresa destinada originalmente a prescribir el procedimiento para estas situaciones. Luego indicó que los procedimientos relativos al filtrado en casos como el presente carecían desde el principio de un fundamento claro en la Ley de Enjuiciamiento Criminal. En segundo lugar, la forma concreta del procedimiento difícilmente podía ser previsible para el demandante, a pesar de que se le permitió oponerse. En tercer lugar, el Tribunal Supremo noruego no había dado ninguna instrucción sobre la forma en que la policía debía llevar a cabo la tarea de filtrar la información, aparte de indicar que las palabras de búsqueda debían decidirse en consulta con el abogado. La copia de la imagen en

espejo fue efectivamente devuelta sin más a la policía para su examen, sin que existiera ningún esquema procesal práctico para ello. Por ende, el TEDH verificó la falta de regulación adecuada. Esta falta de previsibilidad en el presente caso, debida a la falta de claridad del marco jurídico y a la ausencia de garantías procesales, deriva en que haya habido una violación al art. 8 de la Convención.

IV. Orden de presentación para obtener datos digitales

IV. a. Introducción

Se advierte una creciente necesidad, en el marco de investigaciones que implican en algún modo la recolección de prueba digital, de contar con datos informáticos que muchas veces se encuentran en poder de terceros ajenos a la investigación. En este sentido, se ha indicado que la evolución de la tecnología ha modificado a la sociedad y, en la actualidad, prácticamente todos los sectores han racionalizado sus procedimientos y actividades mediante la utilización de la tecnología de la información.

El derecho penal es considerado como un derecho de *ultima ratio* y la actividad de investigación llevada a cabo en los procesos puede afectar derechos de los involucrados, por ejemplo, el registro y secuestro de objetos o datos afecta al derecho de la privacidad y al de propiedad. Por lo que resulta una "buena práctica" aplicar medidas que afecten en menor intensidad a esos derechos y es aquí donde la medida de orden de presentación juega rol importante en el escalonamiento de la coerción en materia de obtención de prueba en formato digital. Este medio de prueba se define como la facultad de las autoridades competentes de ordenar a una persona que se encuentre en su territorio que comunique determinados datos informáticos o datos relativos a los abonados que obren en su poder o estén bajo su control, almacena-

dos en un sistema informático o en un dispositivo de almacenamiento de datos (Art. 18 del Convenio para la Ciberdelincuencia de Budapest). En el marco de la actividad probatoria relacionada a la recolección de prueba digital adquiere una nueva centralidad, ya que existen numerosos organismos públicos o privados que poseen en su poder datos o información útil para la investigación a los que se les puede ordenar que entreguen los datos sin la necesidad de emitir una orden de allanamiento. Esta medida se encuentra regulada en el Código Procesal Penal de la Nación, en el art. 232 de la siguiente manera *en lugar de disponer el secuestro, el juez podrá ordenar, cuando fuere oportuno, la presentación de los sujetos o documentos a que se refiere el artículo anterior; pero esta orden no podrá dirigirse a las personas que puedan o deban abstenerse de declarar como testigos por razón de parentesco, secreto profesional o de Estado.* Asimismo, la mayoría de los códigos procesales provinciales prevén esta medida; a modo de ejemplo el Procesal de Córdoba en su artículo 211 y el de Mendoza en su artículo 224. Sin perjuicio de que estas normas de los CPP habilitan la posibilidad de ordenar la presentación de documentos y ello puede ser extendido a los elementos de prueba en formato de datos informáticos entendidos como documentos, los CPP no han regulado las órdenes de presentación de datos informáticos de manera expresa ni han abordado algunas de las problemáticas que la especificidad de los datos informáticos presentan como puede ser el hecho de que estén físicamente alojados en servidores en extraña jurisdicción.

IV. b. Jurisprudencia argentina

IV. b. 1. Fuero Federal

Corte *Suprema de Justicia de la Nación, "Halabi, Ernesto c/ PEN ley 25.873 y decreto 1563/04 s/ amparo", 24 de febrero de 2009*

Ernesto Halabi promovió acción de amparo reclamando que se declare la inconstitucionalidad de la Ley 25.873 y de su decreto reglamentario 1563/04, en virtud de considerar que sus disposiciones vulneraban las garantías establecidas en los artículos 18 y 19 de la Constitución Nacional, en cuanto autorizaban la intervención de las comunicacio-

nes telefónicas y por internet, así como retención de datos de tráfico y de abonado por diez años, sin que una ley determine en qué casos y con qué justificativos, violando entonces el derecho a la privacidad, en su condición de consumidor, y el derecho a la confidencialidad, en su condición de abogado.

La Corte entendió que la Ley cuestionada resultaba inconstitucional porque las previsiones de la ley exhiben vaguedad en sus previsiones de las que no resulta claro en qué medida pueden las prestatarias captar el contenido de las comunicaciones sin la debida autorización judicial, y, tal como está redactada la norma, existe el riesgo de que los datos sean utilizados para fines distintos que aquellos en ella previstos. El Tribunal agregó que las comunicaciones a las que se refiere la Ley 25.873, y todo lo que los individuos transmiten por las vías pertinentes, integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los artículos 18 y 19 de la Constitución Nacional. El derecho a la intimidad y la garantía consecuente contra su lesión actúa contra toda injerencia o intromisión arbitraria o abusiva en la vida privada de los afectados.

Los Jueces manifestaron que para restringir válidamente la inviolabilidad de la correspondencia, supuesto que cabe extender al presente, se requiere: a) que haya sido dictada una ley que determine los casos y los justificativos en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia; b) que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión; c) que la aludida restricción resulte un medio compatible con el fin legítimo propuesto y d) que dicho medio no sea más extenso que lo indispensable para el aludido logro. A su vez, fines y medios deberán sopesarse con arreglo a la interferencia que pudiesen producir en otros intereses concurrentes.

Cámar*a Federal de Córdoba - SALA A- Causa N° FCB 88747/2018/1/CA1, Incidente de nulidad en causa "Iturria, Matias Emanuel por alteración dolosa", 28 de diciembre de 2020*

En virtud de una denuncia formulada por Andrea Herrera, el Ministerio Público Fiscal solicitó a la AFIP informes, sin autorización judicial, respecto de las direcciones IP desde las cuales se había realizado modificaciones en los registros que el organismo tenía de la denunciante

Dicho informe fue contestado por la AFIP con los números de fecha y hora de las transacciones e IP de proveniencia. En consecuencia, la Fiscalía ordenó la consulta a empresas prestatarias de servicios de internet, requiriendo datos relativos a las cuentas de usuarios, de los que surge la titularidad de Matías Iturria.

La Defensora Pública Oficial en representación de Iturria solicitó la declaración de nulidad de la medida requerida por el Ministerio Público Fiscal sin autorización judicial. La defensa basó su petición en que la información obtenida sin autorización judicial consistía en datos personales de los titulares de IP amparados por el derecho a la intimidad conforme el art. 18 de la Constitución Nacional. Sostiene que las direcciones de IP (Internet Protocolo) son datos de carácter personal protegidos por la Ley 25.326 y por este motivo la solicitud de informe debe equipararse a una "interceptación telefónica" y debió requerirse orden judicial.

La Fiscal se opuso a la nulidad diciendo que los datos no están alcanzados por el secreto fiscal. Además, señaló que la IP constituye simplemente la identificación de la interfaz en red que permite sindicar cuál es el proveedor del servicio de internet, lo que no permite conocer las actividades llevadas a cabo por el usuario, de modo que no es posible sostener que se encuentra vulnerada la intimidad del usuario, máxime cuando el tipo de información cuestionada ya era conocido por la Fiscalía con anterioridad a que el usuario accediera a los IP consultados. El Juez de Instrucción rechazó la nulidad planteada, haciendo suyo los fundamentos expuestos por el Fiscal. Explicó que la solicitud de identificación de un usuario (los informes de titularidad de una dirección IP), efectuada por la Fiscalía Federal a las empresas prestatarias del servicio de internet, de manera alguna, se puede equiparar con una interceptación telefónica.

Desde esta perspectiva, consideró que la medida solicitada por el Ministerio Público Fiscal, que se encontraba a cargo de la dirección de la investigación conforme el art. 196 del CPPN, al solicitar información relativa a la IP, se encontraba amparada dentro de sus facultades propias conferidas por el art. 212 y 213 del CPPN, no siendo necesario que requiera autorización al Juez.

La Cámara entendió correcta la argumentación del Juez de primera instancia que dijo que la medida adoptada se encuentra autorizada por la normativa adjetiva y que los informes sobre la titularidad del Protocolo de Internet (IP) no resultan equiparables a las intervenciones

telefónicas. Además, forma parte de las facultades del Fiscal conforme al art. 212 CPPN.

La Cámara consideró que la dirección IP constituye la identificación de la interfaz en red que permite sindicar cual es el proveedor del servicio de internet, pero no implica el acceso a datos personales, ni se trata de conocer las comunicaciones o cuenta de mail de su titular ni las páginas visitadas, por lo no se encuentra vulnerada la intimidad del usuario al no estar equiparada dicha medida a la interceptación telefónica. Por consiguiente, la invocación de la Ley de Protección de Datos Personales no resulta atinente para la discusión del presente caso, toda vez que no se encuentra afectado en el presente caso el secreto de las comunicaciones.

Finalmente, los Jueces agregaron que es necesario precisar que los datos que se han obtenido son solamente nominativos, siendo estos posibles de recolectar sin invadir la esfera de intimidad de sus titulares. Por estos motivos, la diligencia probatoria propuesta no requiere autorización judicial, en cuanto el pedido de informes a la empresa prestataria de internet sobre la titularidad de las IP de donde provenían las operaciones y facturación detectada no vulnera la privacidad del titular, ya que se trata de datos de identificación externos que no permiten conocer el contenido de la información del usuario de internet, donde se encuentran las facultades con que cuenta el Fiscal de conformidad al art. 212 del CPPN.

IV. b. 2. Fuero de la Ciudad Autónoma de Buenos Aires

Cámar*a de Apelaciones en lo Penal, Contravencional y de Faltas, "Vignale, Zulma y Tolaba, Patricio David s/art. 128 CP – Apelación, 53262-04-00/11", 31 de agosto de 2016*

En esta causa seguida por facilitación y distribución de material de abuso sexual infantil a través de redes P2P, fue condenado Patricio Tolaba a la pena de dos años de prisión en suspenso. La Defensa apeló planteando, entre otras cosas, la nulidad de la orden fiscal impartida a la policía federal por el titular de la acción y de todo lo obrado en consecuencia. Al respecto señaló que dicha orden dirigida a la Policía Federal Argentina (PFA) así como la incorporación del oficio librado por la empresa Telecentro S.A. (respecto de la titularidad de la IP) que

respondió a dicho requerimiento resulta nulo, como así lo obrado en consecuencia pues dicha prueba constituyó la base para la posterior orden de allanamiento y de la que derivó el secuestro del material informático utilizado como prueba. Ello en razón de que, al requerir dicho informe no hubo una intervención, o control judicial alguno, por lo que dicha medida de prueba resultó lesiva de los ámbitos de privacidad e intimidad que solo un juez puede realizar de conformidad con lo dispuesto en el arto 13.8 Constitución de la CABA (CCABA). Refiere el Defensor que cuando se pide información sobre una comunicación específica que esa o esas personas habrían realizado, solo puede ser con orden judicial.

El Tribunal señaló que la declaración de invalidez posee carácter excepcional, y que para decidir la cuestión se debían considerar los principios de conservación y trascendencia de los actos procesales. En consecuencia, la nulidad solo resultaría procedente de advertirse algún vicio sustancial o la afectación de garantías constitucionales, debiendo demostrar quien la alega el perjuicio concreto e irreparable que le ocasiona el acto a su entender viciado, y que no puede subsanarse sino con el acogimiento de la sanción.

El Tribunal dilucidó si la orden del titular de la acción penal al personal de la Policía Federal que motivó la solicitud de titularidad y el domicilio de las direcciones de IP, días y horarios consignados en los oficios mediante el cual se determinó que le correspondía a Vignale Zulma, y dio origen a las restantes medidas adoptadas en la presente, resulta equiparable a información personal almacenada en los términos del arto 13.8 CCABA, –tal como alega el defensor– o solamente configuran datos relativos a la titularidad de la IP asignada por la empresa Telecentro a una determinada persona, y entre las facultades establecidas en el art 93 del Código Procesal Penal de CABA para el Ministerio Público Fiscal.

El Tribunal determinó que no se advirtió que la información en cuestión configurara información personal de Vignale o acerca de lo comunicado o transmitido mediante la conexión, sino que el pedido de informe únicamente requirió a quién estaba atribuida una IP determinada que se conectó en una fecha y hora específica, por lo que no se advirtió que el requerimiento de la información en cuestión vulnerara el derecho a la intimidad constitucionalmente consagrado y que por ello sea exigible una orden judicial previa, tal como plantea la Defensa.

Sobre la base del fallo Halabi, el Tribunal diferenció tres tipos de pedidos de información: sobre titularidad de un abonado telefónico, sobre registros de comunicaciones de un abonado (listado de llamadas entrantes y salientes) y, por último, las intervenciones sobre el contenido de las comunicaciones; y concluyó, que tal como ocurriría en el caso la mera solicitud de la titularidad, en el caso de una conexión a internet, en modo alguno afecta el ámbito de privacidad de las personas constitucionalmente garantizado, puesto que tal información solo se limita a dar a conocer la pertenencia de una determinada línea telefónica, sin inmiscuirse en las comunicaciones que su titular o usuario pudiere haber efectuado. De esta forma, por informe de titularidad de un abonado telefónico se debe entender tanto la solicitud de informe acerca de quién es el titular de un determinado número, como la de establecer si una persona determinada es titular de un abonado, ya sea fijo o celular.

Finalmente, destacó que no era posible considerar que la sola solicitud de información acerca de la titularidad de una determinada conexión de IP, aunque sea necesario explicitar fecha y hora de esta, sin orden judicial previa resulte contraria al ordenamiento constitucional, pues únicamente tuvo como objeto conocer a quien pertenecía y *no el contenido* o los datos de dicha conexión. En consecuencia, rechazó el planteo de nulidad.

Juzgado *Penal, Contravencional y de Faltas n° 10 de la Ciudad de Buenos Aires, en fecha 14 de septiembre de 2018*[1]

La resolución versa sobre pedido de informes efectuado por la Fiscalía interviniente en un caso de distribución de Pornografía Infantil, con el objeto de obtener de Microsoft la información de registración y conexión de una cuenta de correo electrónico, para que, una vez recibida la respuesta, se oficie a las empresas proveedores de acceso a internet que correspondan para que brinden los datos de las asignaciones de las direcciones IP que de ella resulten. Finalmente, el Fiscal requirió al tribunal el libramiento de oficio a la firma Facebook Inc. para que informe los siguientes datos respecto del usuario: a. del Registro de

[1] Esta causa está anonimizada. No se pudieron encontrar datos de las partes.

Información Transaccional; b. Registro de direcciones IP utilizadas para el acceso, con indicación de las fechas y horas pertinentes; c. Información Registrada del usuario en cuestión; d. Abonado telefónico registrado por el usuario.

En el mismo acto, dispuso el libramiento de oficio a la empresa de telefonía móvil a fin de que informe la titularidad, domicilio de facturación y listado de celdas de conexión habilitadas, con su correspondiente ubicación geográfica, durante el mes de octubre de 2017 (sin orden judicial).

El Juez entiende que parte de la información que se requiere a las firmas Facebook y Microsoft se encuentra amparada por la garantía de la privacidad, y como tal el acceso a esta por parte de los investigadores sin orden judicial podría redundar en una afectación a esta (art. 17 PDCyP, art. 11.2 CADH, art. 12 DUDH, arts. 18 y 19 CN y art. 12 inc. 3º y 13.8 CCABA) debiéndose interpretar de manera dinámica el derecho a la intimidad. Dice la Resolución que corresponde hablar de "intimidad informativa" y "autodeterminación informativa", como el derecho de cada individuo de definir cómo, quién y bajo cuáles circunstancias y condiciones se puede acceder a su información personal.

El Juez dice que no se trata únicamente en este caso de datos filiatorios o del domicilio de los usuarios, sino que, además, se pretende acceder a una serie de datos de tráfico que permitirían conocer la intimidad de los registros de transacción de una cuenta, los cuales permitirán a su vez determinar a través de las direcciones IP el/los lugares/es desde los que se realizó cada acceso o *logueo* del usuario. Este es el motivo por el cual considera que se está frente a una medida que no puede ser dispuesta unilateralmente por el Ministerio Público Fiscal, sin intervención del juez.

En este punto cita el precedente Benedik c. Slovenia del TEDH, en el que se había requerido a una empresa proveedora del servicio de internet los datos del usuario al que se le había asignado una determinada IP sin orden judicial. Tal sentencia explicó que la información del imputado asociado con la IP dinámica, no era información que estuviera accesible y, por lo tanto, no podía ser comparada a la información encontrada tradicionalmente en un directorio público. Para poder identificar a una persona a través de una IP dinámica, la empresa prestadora del servicio debía acceder a la información almacenada concerniente a eventos de telecomunicaciones particulares, por lo que el uso de esa

información, por sí sola, podía dar lugar a consideraciones sobre la vida privada.

El Juez entiende que el libramiento de los oficios es una medida necesaria e indispensable para permitir el avance de la investigación, ya que en el caso no se cuenta con la dirección de IP que se corresponde específicamente con los incidentes reportados, y la medida guarda correspondencia estricta con los sucesos descritos y existe un grado de sospecha que permite sostener razonablemente tanto la existencia de un delito como la posible participación en carácter de autor. Por ende, autoriza el libramiento de los oficios.

El Juez luego se expide respecto al oficio cuyo libramiento dispuso el señor Fiscal sin orden judicial a la empresa de telefonía celular a fin de que aporte el informe de titularidad, domicilio de facturación y listado de celdas de conexión habilitadas con su correspondiente ubicación geográfica.

Entiende que los fiscales se encuentran legitimados en virtud de lo dispuesto por el art. 93, primera parte, CPPCABA, para requerir autónomamente informes referidos a los datos básicos de los usuarios investigados (datos del titular de la cuenta, como ser, nombre, país, dirección, teléfonos, y demás información registrada; dirección de correo electrónico asociada; número de teléfono celular asociado; número de tarjeta de crédito asociada; dirección IP desde la que se creó la cuenta), pero que el tratamiento que merece la solicitud del listado de celdas de conexión de un teléfono móvil con su correspondiente ubicación geográfica, es diferente. Esto por tratarse de una medida que se encuentra ubicada en otra categoría de mayor sensibilidad, desde la perspectiva de la privacidad. Los usuarios de los teléfonos celulares mantienen una razonable expectativa de privacidad respecto del registro de los sucesivos y constantes movimientos que van quedando capturados por las celdas de geolocalización de las antenas de las empresas prestatarias del servicio, y, por lo tanto, para que puedan ser reveladas en el marco de una investigación penal, se requiere la orden de un juez.

El análisis de las celdas de localización permite determinar, sobre la base de la información con que cuentan las operadoras, la ubicación de todas las terminales móviles que se activaron dentro de una "celda" (rango de cobertura geográfica de una antena) en un momento determinado. Si bien la medida dispuesta por el titular de la acción apunta a conocer los datos acontecidos en el pasado, lo cierto es que la tecnología actual permite un grado de especificidad tal que incluso resultaría

posible requerir datos referidos a tiempo real, que obran en las bases almacenadas de la empresa prestataria del servicio. Por ende, la intervención jurisdiccional constituye una garantía necesaria en virtud del innegable impacto que esta clase de medidas generan desde la perspectiva de la intimidad.

Por último, el Juez cita el caso, "Carpenter v. United States" fallado por la Corte Suprema de Estados Unidos, en el que se estableció por mayoría que, para obtener las celdas de localización de un teléfono celular en una investigación criminal, se *requiere una orden judicial de registro, que se adecue al estándar probatorio de la "expectativa razonable de privacidad", y se requiere el mismo estándar de convicción que para la emisión de una orden de intervención telefónica o un allanamiento. Sostuvo así que no alcanzaba con los "motivos suficientes" dijo que se requería una orden judicial de registro fundada en "causa probable"*.

La medida requerida puede *proceder únicamente por orden judicial*, luego de someterla a un escrutinio estricto, siempre que haya causa probable de la comisión de un delito y de la posible participación en el hecho de determinada persona, y en la medida que la prueba resulte necesaria y proporcional en atención a la gravedad del delito investigado. Por ende, se declaró la nulidad del oficio.

IV. c. Jurisprudencia internacional

IV. c. 1. España

Tribu*nal Supremo, Sala de lo Penal, Recurso de Casación Resolución 723/2018. 23 de enero de 2019*

En la sentencia fueron condenados los acusados por los delitos de robo con violencia e intimidación con uso de armas, tentativa de homicidio, lesiones, hurto de uso de vehículos, tenencia ilícita de armas. Contra dicha sentencia interpusieron recursos de Casación. Entre los motivos que aquí importan se encuentra el de supuesta infracción del artículo 24.1, 25 y 18.3 Constitución Española, del principio de legalidad y del secreto de las comunicaciones por inaplicación de las sentencias del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014 y de 21 de diciembre de 2016.

Las defensas cuestionaron la obtención de los datos conservados de repetidores telefónicos (registros de llamadas de voz, SMS entrantes, salientes y aquellas otras comunicaciones que se hubieran efectuado a través de los repetidores), y en su consecuencia solicitaron su nulidad dado que el TJUE, en sentencia de 8 de abril de 2014, declaró inválida y nula la Directiva sobre retención de datos telefónicos y de comunicaciones electrónicas de 2006, con efectos retroactivos. Añadieron que para que sea válida la utilización de los datos recogidos en la Ley de Retención de España 25/2007, a la luz de las exigencias del TJUE, la resolución judicial que acuerde dicha medida debe adoptar la forma de auto y tener la suficiente motivación respecto a su justificación. Consideró el recurrente que los oficios y resoluciones dictados fueron meros formularios que incumplieron la doctrina anterior.

El Tribunal citó en este punto Doctrina Casacional diciendo que el TJUE al declarar la inconstitucionalidad de la Directiva referida dijo que la Carta de Derechos Fundamentales se oponía a una normativa nacional que estableciera, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica y se opone a una normativa nacional que regule el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión.

Agregó, el Tribunal que la Ley española (tanto la 25/2007 como el art. 588 bis a.5 de la Ley de Enjuiciamiento Criminal - LECrim) exigía autorización de una autoridad independiente de la administrativa (judicial), y para la investigación y enjuiciamiento de delitos graves, de forma que en cada caso será el Juez de Instrucción correspondiente el que decida la cesión de los datos de tráfico, lo que implica que la decisión debe ser ajustada al principio de proporcionalidad establecido expresamente en la ley procesal (artículo 588 bis a).5 LECrim), lo que en principio no parece incompatible con la exigencia de una normativa nacional que no admita la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y

usuarios registrados en relación con todos los medios de comunicación electrónica, que fue lo que el TJUE declaró inconstitucional.

La Sentencia concluyó diciendo que en este caso hubo autorización judicial motivada, existió un hecho grave *(robo con intimidación y uso de armas, más dos homicidios intentados y lesiones, a consecuencia de la utilización de estas por los atracadores)* , dado que el vehículo utilizado fue quemado dificultando en grado sumo la obtención de datos identificativos a partir de este, siendo imposible obtener informaciones relevantes para la investigación por otros medios menos gravosas para la intimidad de los implicados, por lo que el juicio de proporcionalidad que justificó la autorización estuvo sustentado.

Por ende, el motivo fue desestimado.

IV. c. 2. Estados Unidos

Caso: *Carpenter v. United States – Corte Suprema de Justicia, 22 de junio de 2018*

En 2011, la policía de Detroit obtuvo registros del proveedor de servicios celulares de Timothy Carpenter que mostraban la información de geolocalización (GPS) de su teléfono celular (12,898 puntos de ubicación individualizando los movimientos de Carpenter durante 127 días, un promedio de 101 puntos de datos por día.). A partir de esos registros, se pudo rastrear el paradero de Carpenter durante unos cuatro meses, detectando que estaba cerca de cuatro de los lugares donde ocurrieron una serie de robos, al momento de los hechos.

Basado en parte en la información obtenida de esos registros, Carpenter fue condenado por seis robos diferentes. Carpenter apeló a la Corte de Apelaciones del Sexto Circuito, en la que argumentó que el gobierno violó sus derechos bajo la Cuarta Enmienda al obtener y examinar esos registros. El tribunal falló a favor del gobierno, concluyendo que Carpenter no tenía expectativas razonables de privacidad en los registros de ubicación de teléfonos celulares. Carpenter pidió a la Corte Suprema que escuchara el caso y accedió a hacerlo.

La Corte Suprema sostuvo que la adquisición por parte del gobierno de los registros de ubicación de teléfonos celulares de Carpenter constituía una búsqueda (*search*) y que el gobierno debería haber obtenido

primero una orden judicial (*warrant*), respaldada por una causa probable antes de adquirir esos registros.

Para así resolver, la Corte dijo que los teléfonos celulares realizan su amplia y creciente variedad de funciones al conectarse continuamente a un conjunto de antenas de radio llamadas "torre de celulares" (*cell-sites*). Cada vez que un teléfono se conecta a un sitio celular, genera una marca de tiempo y registro conocido como "información de ubicación de torre del celular" (*cell-site location information* CSLI). Los proveedores de servicios inalámbricos recopilan y almacenan esta información para sus propios fines comerciales. A veces, estos datos son generados por acciones intencionales de un usuario: al realizar una llamada telefónica, enviar un mensaje de texto o encender el teléfono, el usuario hace que el teléfono se comunique con la torre celular más cercana. CSLI también se puede generar automáticamente: cuando un teléfono recibe un mensaje de texto o cuando el teléfono envía una actualización periódica a la red, por ejemplo. Cuanto mayor sea la concentración de torres de telefonía móvil, más precisos serán los datos de ubicación. Esto significa que es más fácil precisar la ubicación precisa de un individuo en un área urbana que en una rural.

Después de que el FBI identificó los números de teléfono celular de varios sospechosos de robo, los fiscales recibieron órdenes judiciales para obtener los registros de los teléfonos móviles de los sospechosos en virtud de la Ley de comunicaciones almacenadas (*Stored Communications Act),* estándar de sospecha considerablemente más bajo que la causa probable requerida para una orden judicial típica.

La Corte dijo que la Cuarta Enmienda protege no solo la propiedad, sino también la expectativa de privacidad (citando Katz contra Estados Unidos). Así, cuando un individuo busca preservar algo como privado, y su expectativa de privacidad es una que la sociedad está dispuesta a reconocer como razonable, la intrusión oficial en esa esfera generalmente califica como una búsqueda (*search*) y requiere una orden judicial respaldada por una causa probable.

La Corte dijo que los registros históricos de la torre de celulares presentan preocupaciones de privacidad aún mayores que el seguimiento GPS: los datos con sello de tiempo de CSLI brindan una ventana íntima a la vida de una persona, revelando no solo sus movimientos particulares, sino a través de ellos sus asociaciones familiares, políticas, profesionales, religiosas y sexuales. Se trata de una crónica detallada de la presencia física de una persona recopilada todos los días, en cada

momento, durante varios años. Un teléfono celular registra un registro del sitio a fuerza de su funcionamiento, sin ningún acto afirmativo por parte del usuario. Finalmente, sostuvo que se requiere una orden judicial para los datos CSLI.

V. Cadena de custodia

V. a. Introducción

La cadena de custodia es un conjunto de medidas que se llevan a cabo en un proceso penal a los fines de preservar la identidad e integridad de la prueba obtenida desde el momento de su recolección y adquisición, hasta la incorporación formal al proceso, y posterior dictado de la sentencia. Se aplica independientemente del tipo de prueba de la que se trate. Es la forma objetiva de demostrar que la actividad de los equipos auxiliares de justicia tales como la policía judicial, los peritos, o el propio personal de fiscalías y juzgados, mantuvieron la integridad del material u objeto secuestrado y de esta manera no alteraron, indebidamente, la prueba.

En materia de prueba digital este instituto posee una relevancia adicional, dado que esta puede ser fácilmente alterada, destruida y/o modificada. Incluso estas alteraciones pueden ser difíciles de detectar y trazar. La cadena de custodia bien documentada, de acuerdo con estándares rigurosos, trae seguridad jurídica para todas las partes en un proceso penal, ya que demuestra que la prueba no fue alterada y que por ende se puede recurrir a ella sin dudas acerca de su integridad. El Código Procesal Penal Federal de Argentina, aprobado mediante ley 27063, establece en el art. 90 inc. e) que las fuerzas de seguridad

deberán custodiar los elementos secuestrados, dejando debida constancia de las medidas adoptadas con el objeto de preservar la cadena de custodia. Mientras que el art. 150 del citado cuerpo normativo establece una disposición concreta sobre cadena de custodia. La norma prevé que, con el fin de asegurar los elementos de prueba, se establecerá una cadena de custodia que resguardará su identidad, estado y conservación. Se identificará a todas las personas que hayan tomado contacto con esos elementos, siendo responsables los funcionarios públicos y particulares intervinientes. Respecto al Convenio para la Ciberdelincuencia de Budapest, surge del Informe Explicativo que las medidas procesales sobre prueba digital reguladas en el Convenio tienen como fin salvaguardar los datos, es decir, preservar la integridad de los datos o mantener la cadena de custodia de estos, lo que significa que los datos copiados o extraídos serán conservados en el Estado en que fueron encontrados en el momento de la confiscación y permanecerán inalterados mientras duren los procedimientos penales (considerando 197).

V. b. Jurisprudencia argentina

V. b. 1. Fuero federal

Cámar*a Nacional de Apelaciones en lo Criminal y Correccional Federal de la Capital Federal - Causa n° 46.744, "Fiscal s/ apela declaración de nulidad de informe pericial – Ricardo Jaime", 24 de mayo de 2012*

El Fiscal presentó recurso de apelación ante una declaración de nulidad de un peritaje practicado por la División Apoyo Tecnológico de la Policía Federal Argentina sobre las computadoras secuestradas en los domicilios de los imputados, y la nulidad de todo acto que hubiere tenido lugar en la causa como consecuencia de dicho peritaje.

Las defensas denunciaron que, inmediatamente después del secuestro de computadoras efectuado en los domicilios, se ordenó a la División Apoyo Tecnológico de la Policía Federal hacer un peritaje para conocer el contenido de sus discos rígidos, cuya realización no fue notificada a la Defensa –en violación a lo dispuesto por los arts. 200, 201 y 258 del CPPN– con el argumento de que se trataba de una operación

extremadamente sencilla y reproducible en el futuro. Luego se ordenó practicar otra con intervención de técnicos de la UBA. Este segundo peritaje sí fue notificado a las defensas, pero su resultado (el hallazgo de documentos electrónicos que el Fiscal pretende utilizar como prueba de cargo) se encuentra precedido de la advertencia de los peritos de la UBA de que el material que recibieron no había sido debidamente resguardado, habiéndose violado la cadena de su custodia.

Las defensas, por ende, solicitaron que se anulen ambos peritajes: el primero por la omisión de practicar la notificación que manda la ley procesal y la consecuente violación del derecho constitucional de controlar la producción de prueba, y el segundo por la sospechosa contaminación de la evidencia puesta de resalto por los profesionales de la UBA luego de una primera revisión en la que la defensa fue excluida. Luego se ordenó un tercer peritaje.

Respecto del primer peritaje, la Cámara sintetizó que no se evidenció la urgencia que excepcionaría la notificación a las defensas ni tampoco que fuera extremadamente sencilla para suplir la notificación, si se tienen en cuenta las innumerables prevenciones señaladas por los técnicos de la Universidad de Buenos Aires, así como la complejidad propia de las operaciones tendientes a la preservación de la evidencia, al uso de bloqueadores de escritura, a la búsqueda y recuperación de archivos informáticos, a su copiado, al uso de programas de recuperación de archivos eliminados o de observación de archivos ocultos.

En lo que respecta al segundo peritaje, realizado por la Universidad de Buenos Aires y donde se hallaron los correos electrónicos y elementos aquí cuestionados, comprobaron la imposibilidad de aseverar que las computadoras secuestradas contuvieran –sin alteraciones, supresiones o adiciones– los mismos archivos que tenían registrados al momento de su secuestro y, por tanto, tornó ilusoria la exacta reproducción de un estudio sobre ellas.

La tercera pericia advirtió *el hallazgo de numerosos archivos creados con anterioridad al secuestro de las computadoras que aparecen modificados en el tiempo en que estas estuvieron a disposición de la División Policial, o bien que fueron directamente creados en ese espacio de tiempo* (punto F del informe pericial del Lic. PICCIRILLI - Universidad Tecnológica Nacional).

Los técnicos solicitaron al Juzgado la información correspondiente que avale el mantenimiento de la cadena de custodia del material secuestrado, pero el Juzgado no proveyó la correspondiente documenta-

ción. En este sentido la sentencia destacó el informe pericial en el que define a la cadena de custodia como *la fuerza o cualidad probatoria de la evidencia. Debe probarse (si fuese requerido por el juez o fiscal) que la evidencia presentada es realmente la misma evidencia recogida en la escena del crimen, o recuperada a través de algún testigo, entregada por la víctima, o por otros sujetos o adquirida originalmente de alguna otra forma.*

Para cumplir con este requisito debemos mantener un registro minucioso de la posesión y de la cadena de custodia de la evidencia. Este puede asegurarse mediante un sistema de recibos y registro minucioso. La cadena de custodia también implica que se mantendrá la evidencia en un lugar seguro, protegida de los elementos, que no se permitirá el acceso a la evidencia a personas que no están autorizadas.

La sentencia mencionó que e*s una buena práctica de la profesión forense informática "mantener y verificar la cadena de custodia" para asegurar que todos los registros electrónicos originales no han sido alterados. En tal sentido y en virtud del estado del material a periciar que nos fuera entregado, no puede asegurarse que se haya mantenido la cadena de custodia.*

Por eso la Cámara entendió que las diligencias practicadas con posterioridad conducen a excluir la prueba cuestionada *por no haberse preservado adecuadamente la evidencia, como manda la ley.*

La Cámara estableció que, de este peritaje puede advertirse la existencia de archivos creados o modificados en aquel lapso que se refieren, en concreto, a algunas de las operaciones presuntamente delictivas. Así, *y más allá de cuál pudo haber sido la entidad o la extensión de la operatoria que los afectó, lo cierto es que este solo aspecto (su modificación en un tiempo en el cual debieron permanecer imperturbables) impide a la magistratura acordarles algún valor probatorio.*

La Cámara explicó que, de la pericia de la UTN (Piccirilli y Presman), puede concluirse que *emplearon sistemas bloqueadores de escritura de hardware (...) para evitar que al acceder a los discos rígidos se inserte información contaminando la evidencia,* y que *los peritos policiales no utilizaron ningún sistema de ese tipo.*

Por ende, la Cámara concluyó que la cadena de custodia fue violada y que *las prácticas llevadas adelante por la Policía Federal Argentina sobre el material secuestrado contaminaron la evidencia, convirtiendo lo que el juez instructor había considerado una "operación pericial extremadamente simple" y "repetible" en una medida irreproducible.*

El Tribunal confirmó la resolución que anuló los peritajes producidos por la Policía Federal y por la UBA, debiendo proseguirse sin esos elementos con la investigación del delito de enriquecimiento ilícito denunciado.

Cámar*a Federal de Apelaciones de Mar del Plata, FMP 19671/2016/6 "Incidente de Nulidad", FMP 19671/2016/6, 2 de octubre 2018*

El imputado presentó un recurso de apelación contra una resolución del Juez de grado que no hizo lugar a un planteo de nulidad deducido anteriormente. Los letrados solicitaron se revoque el pronunciamiento del *a quo* y se declare la nulidad de lo actuado por violar los derechos de igualdad, propiedad e inviolabilidad de domicilio, intimidad, secreto profesional, defensa en juicio y debido proceso, entre otros.

Los apelantes fundaron su postura en que se les negó el ingreso al allanamiento al estudio jurídico de su defendido, y que se han excedido en el secuestro de documentación, archivos digitales y computadoras del estudio jurídico.

Respecto a la falta de notificación del allanamiento dispuesto, la Cámara sostuvo que este planteo ya ha sido tratado por la Alzada donde fue rechazada la nulidad por lo que no corresponde volver a tratar la cuestión. Acerca de la presencia de los abogados defensores en el allanamiento, la Cámara argumentó que las normas procesales no exigen su asistencia en los registros domiciliarios (arts. 224, 225 y cc. del CPPN) y si bien el art. 200 del CPPN los autoriza a presenciarlos, su falta de intervención no implica *per se* la nulidad del procedimiento. En el caso, no se observa que se haya vulnerado el derecho de defensa en juicio y, además, los recurrentes no acreditaron cuál fue el perjuicio sufrido al no habérsele permitido el ingreso al lugar del allanamiento por parte de la fuerza actuante.

Respecto al exceso ilegal en el material secuestrado la Cámara explicó que el juez de grado, en la resolución puesta en crisis, dio acabada respuesta a tal planteo puesto que explicó basándose en las constancias de la causa que las órdenes fueron claras y precisas. Las órdenes decían que el registro debía limitarse "...estrictamente a aquellos documentos y efectos que guarden relación con los hechos objeto de la causa, ello por tratarse el lugar a allanar de un estudio jurídico, cuyos integrantes se encuentran amparados por el secreto profesional...".

Además, sostuvo que se debía "identificar todo dispositivo electrónico que permita el tratamiento o almacenamiento de información en cualquier tipo *(...) y, a través del personal informático especializado, realizar una copia o* backup *de aquella información estrictamente vinculada con el objeto de la investigación, debiéndose adoptar un protocolo de evidencia informática que garantice la cadena de custodia...*".

La Cámara explicó que el Juez allí también especificó cuál era el objeto procesal y cuáles eran los hechos que, de momento, conformaban la investigación enumerando las personas involucradas en ellos. Por otra parte, se hizo saber a la fuerza que "se debían arbitrar las medidas que resulten pertinentes a fin de garantizar el debido resguardo de la cadena de custodia de los mentados efectos, circunscribiendo el oportuno análisis del contenido de las respectivas computadoras a los datos y documentos que posean vinculación con el objeto de la presente pesquisa".

Explicó el Tribunal que de las actas del procedimiento surgía que, en diferentes momentos, el personal encargado de su ejecución se comunicó telefónicamente con el Juzgado, recibiendo las instrucciones correspondientes, observándose una constante protección no solo a los derechos de defensa sino del secreto profesional y los recurrentes no han alegado algún perjuicio concreto ni precisado cuáles de los elementos secuestrados no se corresponden con el objeto del proceso. Por ende, se confirmó la resolución del Juez de grado apelada, que rechaza la nulidad.

V. b. 2. Fuero nacional

Cámar*a de Apelaciones en lo Penal, Penal Juvenil, Contravencional y de Faltas, Sala III, "Incidente de apelación en autos NN, NN sobre 131 contactar menor de edad por intermedio de tecnologías para cometer delitos de integridad sexual", causa 41459/2019, 5 de octubre de 2021.*

El Tribunal intervino en virtud del recurso de apelación presentado por la defensa del imputado C.B. contra la resolución que no hizo lugar a la nulidad planteada respecto de la cadena de custodia de la evidencia aportada por la fiscalía, es decir, capturas de pantalla efectuadas sobre el teléfono celular de la denunciante.

La defensa había argumentado en primera instancia que se había visto alterado el valor de hash aplicado sobre la misma.

El voto mayoritario expresó que no se vio afectada la cadena de custodia. Señalaron que no es lo mismo *no contar con un código de identificación que, por error, el código original hubiera sido modificado por personal idóneo del Ministerio Público Fiscal.* En este punto señalaron que se habían percatado del error que cometieron y lo solucionaron *asignando el hash pertinente, y dejando constancia de ello en el mismo informe.*

Dijeron además que *no se había tratado de un error de cálculo en el código "hash", sino que, por el contrario, en el acta de resguardo correspondiente al caso se había dejado consignado el número de hash del modelo de acta que se había utilizado, y no se había modificado por el generado luego de realizar la descarga y el almacenamiento de las capturas de pantalla brindadas por la denunciante.*

Señalaron que no se violó la cadena de custodia. Para ello la definieron como *el conjunto de procedimientos de seguridad destinados a garantizar que los elementos de prueba materiales que se incorporan y exhiben en el juicio oral guarden identidad física con el material que ha sido hallado, recolectado e incautado en el lugar donde se afirma que ocurrió el delito o hecho de relevancia penal, y que se encuentra en idénticas condiciones fenomenológicas a las que allí tenían, o sea: que no hayan sido alterados, contaminados, destruidos, dañados o sustituidos".*

A su vez, la cadena de custodia de la evidencia digital se inicia al momento de incorporación del elemento de prueba y debe registrar la información que permita comprender acabadamente cuál es el efecto, cuál es la evidencia, de qué forma fue re- colectada y preservada.

Asimismo, la certificación hash utilizada en el caso constituye uno de los modos más utilizados en la actualidad para dotar a la evidencia digital de credibilidad y verificabilidad, en la medida en que aquella tiene la función de corroborar la identidad del archivo y asegurar que la información no fue alterada por personas no autorizadas u otros medios desconocidos.

Concluyen que no ha habido una modificación en el código hash, *sino que, antes bien, se ha producido un error material en el acta en la que se plasmó la actividad llevada a cabo por el Centro de Investigaciones Judiciales.* Confirman la sentencia apelada y se rechaza la nulidad solicitada.

El voto minoritario estableció que sí hubo violación a la cadena de custodia. En primer lugar reseña que el código hash es "*la huella digital de la información electrónica que permite comprobar que no se alteró la prueba original y que (...) esa evidencia contenida en el dispositivo*

secuestrado es la misma que se encontraba almacenada en el momento del secuestro y que es exactamente la misma que se extrajo y que, luego, se examinará. Estos códigos difícilmente puedan ser alterados o modificados. (...) Si pasado un tiempo de realizada la misma alguien plantea que fue alterada, bastará calcular el hash para ver si es el contenido es el mismo del originalmente obtenido (en este caso, se demuestra que la copia no fue manipulada). Se exige el cálculo del hash sobre cualquier copia forense para asegurar que ella no se vea alterada con posterioridad de su realización, circunstancia fundamental para garantizar la cadena de custodia de una prueba.

Teniendo en cuenta estas apreciaciones concluye en minoría que la cadena de custodia fue alterada y determina su nulidad. Esto porque *el código hash que debería identificarla fue modificado en el transcurso del proceso, circunstancia que no permite garantizar su autenticidad. En efecto, no puede perderse de vista que para que la extracción de la prueba sea un acto procesal válido, debe registrarse el primer hash obtenido. La documentación del primer hash es un acto de gran trascendencia a los efectos de la identificación de la prueba, porque, si bien es cierto que la extracción de la prueba se puede repetir indefinidamente mediante la utilización de las herramientas forenses que impidan que se modifique la prueba, no menos cierto es que si las partes no fueron notificadas de la realización de ese acto nunca podrán controlar que el primer acceso al dispositivo secuestrado se efectuó siguiendo las buenas prácticas sobre extracción de la evidencia digital, no podrán corroborar que el hash obtenido corresponde al valor que tenía la prueba en el momento del secuestro, así como tampoco podrán verificar que la prueba no fue contaminada y (...) no tendrían forma de corroborar que el primer hash corresponde a una extracción no viciada. Solo podrían confirmar que el hash de una nueva y posterior extracción coincide con el primer hash, pero eso no asegura que ese primer hash sea el valor que arrojó la primera extracción.*

Agrega que *el error involuntario presuntamente cometido por el personal del MPF no puede ser subsanado por el reemplazo del hash, ya que ello no permite asegurar que la prueba oportunamente colectada no hubiese sido adulterada con posterioridad.*

V. b.3. Ciudad Autónoma de Buenos Aires

Tribunal Superior de Justicia de la CABA, "Ministerio Público (Defensoría General de la CABA) s/ queja por recurso de inconstitucionalidad denegado en: 'NN s/ inf. art. 181 CP'", causa 13816/2016, 6 de septiembre de 2017.

El Tribunal Superior de Justicia de la CABA intervino en esta sentencia a raíz de que el Defensor General Adjunto en lo Penal, Contravencional y de Faltas presentó queja contra el auto denegatorio del recurso de inconstitucionalidad contra la Resolución de la Sala III que revocó la nulidad dispuesta por la jueza de primera instancia de las pericias informáticas efectuadas en el marco de la investigación por presunta usurpación en 2014 del predio Papa Francisco, en Villa Lugano.

La Cámara había considerado que los efectos secuestrados en los allanamientos (nueve CPUs, diez teléfonos celulares y cuatro netbooks) eran identificables mediante una simple observación al estar preservados en bolsas transparentes con el precinto y numeración original, razón por la cual no advertía la irregularidad denunciada por la defensa y admitida por la jueza de primera instancia.

El Tribunal, al analizar su admisibilidad entiende que debe dar concluido el trámite de queja respecto de uno de los imputados y rechazarlo respecto del otro. No obstante uno de sus votos (jueza Ana María Conde) expresa que *una detenida lectura de las actuaciones me permite concluir que la defensa, a través de sus cuestionamientos, no procura demostrar con seriedad que los efectos inicialmente incautados por la Policía Metropolitana en el marco de los allanamientos prima facie válidos, (es decir, efectos respecto de los cuales sólo se extrajeron "copias forenses" por un analista del Cuerpo de Investigaciones Judiciales de la Ciudad), hubieran sido extraviados, alterados, indebidamente manipulados o defectuosamente resguardados al punto de que en la actualidad no pudiesen ser identificados, reexaminados o cuya trazabilidad no pudiera ser determinada con facilidad a partir del momento mismo en el cual se realizaron aquellos allanamientos; (...). Por el contrario, los cuestionamientos de la defensa tan sólo se limitarían a poner de manifiesto una mera discrepancia con lo resuelto por el tribunal a quo hasta el momento, sin explicar la sinrazón de las conclusiones en las que su pronunciamiento se apoya y sin siquiera rebatir aquello que la Cámara*

fundadamente señaló en cuanto a la inexistencia de un menoscabo relevante al derecho de defensa en juicio de los imputados.

Luego, el voto de la jueza Inés Weinberg agregó que los jueces de la Sala III, por mayoría, argumentaron que *los efectos secuestrados habían sido recibidos por el CIJ y preservados en bolsas transparentes cerradas para que su contenido resultara observable, a las que se les colocó un precinto de color verde, para asegurar su inviolabilidad y que luego de realizarse las operaciones pertinentes se había colocado, además, un precinto blanco de manera tal que los efectos fuesen plenamente identificables mediante una simple observación visual; no existían elementos de convicción que permitieran suponer que, desde el día de su incautación hasta el de su análisis –o a la actualidad– los elementos secuestrados no hayan sido los mismos; la nulidad decretada en base a las deficiencias en los recibos de tales efectos carecía de un fundamento válido, siendo más bien –como señalara el fiscal– producto de una confusión entre la cadena de custodia y su registro; y que las operaciones realizadas –simple obtención de copias forenses– no implicaban actos "definitivos e irreproducibles".*

Los jueces manifestaron que la defensa señaló diferencias en una nota de remisión del director del CIJ al representante fiscal. No obstante concluyen que, *sin perjuicio de los errores materiales en que se haya podido incurrir al confeccionar la nota de remisión, no existen elementos de convicción que permitan descartar que, desde el día de su incautación, hasta el día de su análisis –o la actualidad–, los elementos que se hayan a disposición de los interesados hayan sido siempre los mismos. Siendo los bienes trazables, la nulidad decretada en base a la deficiencia en los recibos de tales efectos no encuentra un fundamento válido, siendo más bien (...) producto de una confusión entre la cadena de custodia y su registro. Lo más relevante aún, es que las defensas no han identificado el perjuicio concreto que los errores sobre los que fundaron su pedido de nulidad generaron a los intereses de sus asistidos (...) máxime cuando su contenido no resulta alterable sin que queden huellas rastreables en él y no se ha planteado y menos aún acreditado, que éste hubiese sido modificado o alterado.*

Entonces, no basta la mera alegación de rotura de la cadena de custodia dado que esta misma tiene la fuerza suficiente como para demostrar que las acciones realizadas sobre la evidencia han sido justas.

Juzgado de primera instancia en lo Penal, Contravencional y de Faltas, número 6, "Ricardo Russo sobre art. 128 1er párrafo"-, causa 33010/2018, 6 de noviembre de 2019.

En la sentencia de Ricardo Russo, condenado a diez años de prisión e inhabilitación especial perpetua para ejercer la medicina por diversos delitos relativos al material de abuso sexual infantil, en lo pertinente a cadena de custodia puso en duda el procedimiento realizado sobre las computadoras y dispositivos secuestrados. El juez de primera instancia en su sentencia escrita y leída en lenguaje claro consideró que "*de las actas no ha habido ningún tipo de discusión o duda y todo esto fue avalado por el testimonio de Cardozo Torres. Los testigos nos hablaron del protocolo de actuación, que se respetó, que tenía que ver con tapar los puertos, tenía que ver con poner una faja de secuestro en los materiales y una bolsa plástica. En este caso intervino personal de Gendarmería. Y de hecho, cuando los elementos fueron peritados, vimos aquí mismo en la sala de audiencias que seguían manteniendo la cadena de custodia y se abrían aquí mismo todos los archivos, lo cual da cuenta de que ese procedimiento, frente a cada pericia, fue respetado".*

Además Russo discutió el procedimiento de secuestro de la computadora del Hospital Garraham dado que se realizó mientras él se encontraba detenido. El juez explicó en este sentido que, quienes participaron del procedimiento, declararon que *no han observado ningún tipo de anomalía y los testigos han dicho que, desde ese momento hasta el allanamiento en que se secuestra el CPU mencionado que transcurren sólo 72 horas, la oficina del imputado quedó clausurada.* Agrega además que esos dichos *se ven verificados con el procedimiento de allanamiento, que cuando ingresan han exhibido las fotos de que estaba la puerta fajada, estaba clausurada, y se les ha acercado a los preventores desde la seguridad del nosocomio las llaves para poder ingresar.*

Respecto del secuestro de la computadora declararon dos testigos que *hablaron del protocolo, del grado del cuidado.* El juez reseñó luego de analizar todas las circunstancias que *los testigos fueron bastante cuidadosos en cada detalle que vieron y hasta que no comprobaron y se abrió la cadena de custodia con la bolsa y observaron la computadora, no afirmaron que se trataba de la misma. Recién cuando vieron qué computadora era y manifestaron cómo era la base de esa computadora, la pudieron identificar. Dice que no encuentra ningún punto en el que hayan faltado la verdad ni mucho menos.*

De esta manera concluye que el procedimiento fue legítimo, la cadena de custodia se ha respetado tanto sobre las fuentes de evidencia como en las pericias realizadas.

V. c. Jurisprudencia internacional

V. c. 1. España

Tribu*nal Supremo, Sala de lo Penal, caso 767/2019. 12 de septiembre de 2019*

Por la Sección segunda de la Audiencia Provincial de Toledo se dictó sentencia, con fecha 6 de noviembre de 2018, en la que se condenó al Sr. Hilario, entre otras cosas, como autor responsable de un delito de distribución de material de abuso sexual infantil del art. 189.1.b y 2.b del Código Penal español. Contra dicha sentencia Hilario interpuso recurso de apelación.

El recurrente entendió que se habían vulnerado sus derechos constitucionales por supuestas irregularidades realizadas con posterioridad al dictado del auto que dispuso la entrada y registro de su domicilio, al no ajustarse a lo acordado en él y porque no se garantizó la correcta cadena de custodia de los efectos secuestrados (en particular, un dispositivo de almacenamiento digital), lo que determinaría la nulidad de la prueba pericial obtenida, insistiendo en la ausencia de copia de seguridad de este, lo que le habría impedido efectuar prueba alguna contradictoria.

Los Jueces del Tribunal Supremo consideraron que *el dispositivo quedó suficientemente identificado y resultaba absolutamente razonable que no pudiera hacerse constar el número de serie del disco duro interno al no haberse extraído el mismo en ese momento. En definitiva, porque lo que constaría acreditado sin duda es que el día en que se llevó a cabo dicho registro, una vez notificado el auto, se procedió al mismo en la habitación del investigado, a su presencia y de los agentes de la Policía Nacional, accediendo aquel voluntariamente a enseñar el ordenador y facilitando la clave de acceso a este.* Así como que, *ante la evidente imposibilidad material de hacer una copia completa de todos los archivos contenidos en el disco duro, se procedió al precinto del aparato en la forma autorizada tanto por el auto judicial como por el art. 588.*

sexies. a y c LECrim para la realización de un análisis más exhaustivo, incorporando a un sobre cerrado las claves de acceso correspondientes, quedando bajo custodia del Letrado de la Administración de Justicia hasta su remisión al Juzgado.

El Tribunal señaló que, a propósito de las exigencias legales del clonado o volcado de datos, *tiene establecido que no es precisa la presencia del Letrado de la Administración de Justicia ni de las partes, quedando garantizada la contradicción a través de la posibilidad de que el acusado designe su propio perito para llevar a cabo otro reconocimiento pericial distinto, ante la imposibilidad o dificultad material de presenciar el proceso de análisis de esta clase de dispositivos, en atención a la larga duración del mismo. Lo decisivo, se dice, es que queden descartadas las dudas sobre la integridad de los datos y la correlación entre la información aprehendida en el acto de registro e intervención de los ordenadores y la que se obtiene mediante el volcado, lo que así se estimó garantizado en el caso.* En consecuencia, el Tribunal rechazó el recurso.

Tribu*nal Supremo, Sala de lo Penal, Resolución 429/2019. 27 de septiembre de 2019*

Ante la Audiencia Provincial de Las Palmas de Gran Canaria, el 5 de diciembre de 2017, se dictó sentencia condenatoria a Donato como responsable de un delito continuado de abusos sexuales, de un delito continuado de exhibición material pornográfico y de un delito de corrupción de menores. El día 12 de enero de 2016, con auto judicial de la misma fecha, funcionarios del Cuerpo Nacional de Policía (CNP) practicaron entrada y registro en el domicilio del acusado, e intervinieron varios aparatos electrónicos, propiedad de aquel, conteniendo abundante material de abuso sexual infantil. Dicho material había sido obtenido mediante programas P2P.

Notificada esta resolución, la defensa instó un recurso de casación ante el Tribunal Supremo. Entre los motivos que aquí interesan se encuentra el de la vulneración del derecho a la tutela judicial efectiva y a un proceso con todas las garantías (art. 24.1 y 2 CE). Aduce el recurrente que el acta de apertura de los sistemas informáticos intervenidos al acusado era nula, *por la inexistencia de un acta de precinto previa, así como por la ausencia del Letrado de la Administración de Justicia (LADJ) durante el volcado de los elementos informáticos, que provocan*

la ruptura de la cadena de custodia, convirtiendo en prueba ilícita el informe pericial derivado de tal fuente de prueba.

El Tribunal sostuvo que *la sentencia recurrida explica de forma clara y concreta la forma en la que se llevó a cabo la incautación de los objetos del acusado, todo ello con los números y descripciones detalladas de cada uno de los aparatos secuestrado. La diligencia se practicó a presencia del propio acusado y de su letrada. En la propia declaración llevada a cabo ante el Juzgado de Instrucción, el acusado autorizó expresamente a que la Policía examine con detalle sus ordenadores y* tablets. *También consta el escrito en el cual se solicita autorización al Juzgado para el volcado y estudio del material informático y telefónico. En dicho escrito se señala sobre qué material se va a realizar el estudio, concretándose de forma específica los aparatos concretos, con su número de identificación. Consta en las actuaciones el acta de desprecinto de los efectos intervenidos, citándose que se realiza a presencia del acusado, su letrado y los agentes del CNP.*

El Tribunal concluyó *que no se desprende de las actuaciones citadas motivo alguno en base al cual se pueda desprender una actuación ilegal o interesada por parte de las Fuerzas y Cuerpos de Seguridad del Estado, que el contenido de los aparatos incautados son los que fueron objeto de informe pericial, y la reseña de todos sus datos en cada una de las actuaciones policiales y judiciales así lo confirman. Así como, con cita de Jurisprudencia, se afirma que la presencia del LADJ ni la del letrado es necesaria en tales actuaciones.*

Finalmente, el órgano judicial agregó que *no se encuentra previsto ni en la ley procesal anterior al año 2015 ni tampoco la nueva normativa de la Ley de Enjuiciamiento Criminal (Ley 13/2015, de 5 de octubre) la necesidad de que estén presentes el letrado del imputado ni un perito nombrado por la parte en el momento de volcar el contenido del ordenador. Es más, el nuevo artículo 588 sexies c) ni siquiera requiere la presencia del LADJ en el momento de abrir el ordenador y obtener el disco duro.*

En virtud de todo lo argumentado, el Tribunal Supremo desestima el recurso de casación interpuesto.

VI. Hallazgos casuales en el marco de registros de sistemas informáticos

VI. a. Introducción

Uno de los desafíos que presenta la prueba digital en el proceso penal son los hallazgos casuales en el marco de registros y secuestro de datos en dispositivos de almacenamiento informático. Si bien en lo que hace a prueba física su aplicación y análisis no ofrece mayores complicaciones de acuerdo con la evolución de su tratamiento por la doctrina y jurisprudencia, el desarrollo de las nuevas tecnologías ha abierto ciertos interrogantes en lo que al registro y secuestro de datos informáticos se refiere. El Código Procesal de la Nación prevé en su art. 224, que, si en el estricto cumplimiento de una orden de allanamiento, se encontraren objetos que evidencien la comisión de un delito distinto al que motivó la orden, deberá procederse a su secuestro, comunicando esta situación al Juez o Fiscal interviniente, de conformidad a la *plain view doctrine*, aceptada por nuestra jurisprudencia.[1] La prueba digital es sus-

[1] Polansky, J., *Garantías constitucionales del procedimiento penal en el entorno digital*, Buenos Aires, Hammurabi, 2020, p. 162 y Carrió, A., *Garantías constitucionales del proceso penal*, 6ta. ed., Buenos Aires, Hammurabi, 2015, pp. 402 y ss.

tancialmente diferente a la prueba física.[2] Asimismo, las formas de almacenamiento son disímiles por lo que muchas veces se hace necesario proceder a un análisis de la totalidad del contenido de un dispositivo de almacenamiento electrónico, para verificar la existencia de elementos que guarden relación con el objeto de investigación en el marco de un caso criminal. En muchos casos es necesario secuestrar varios dispositivos encontrados en el lugar que es objeto de un allanamiento para posteriormente analizarlos. Ya sea a través de un peritaje con participación de la defensa o de la realización de una imagen forense o copia bit a bit para su posterior análisis técnico, a fin de preservar adecuadamente la información primigenia contenida en los dispositivos.

Ahora, dadas las características de los entornos digitales que hacen necesaria una búsqueda más amplia para verificar los puntos de análisis. ¿Qué sucede cuando los peritos descubren prueba de un delito diferente al que motivara la orden de registro y secuestro? ¿Puede incautarse esa evidencia en el marco de una investigación y utilizarse para dar comienzo a otra? ¿Es esa prueba admisible? ¿Se puede extrapolar sin inconvenientes la doctrina de los hallazgos casuales –ampliamente receptada y con gran desarrollo jurisprudencial en los Estados Unidos bajo la denominación *plain view*– a registros en entornos digitales? ¿Cómo sostenemos que ese hallazgo fue casual, si se ha registrado la totalidad de un dispositivo informático?

VI. b Jurisprudencia de Argentina

VI. b. 1. Ciudad Autónoma de Buenos Aires

Cámar*a de Apelaciones en lo Penal, Contravencional y de Faltas Caso N.º INC 2134/2018-1, 26 de septiembre de 2018*
En el marco de una investigación por amenazas contra la diputada de la Nación Elisa Carrió y el Jefe de Gobierno de la Ciudad de Buenos Aires Horacio Rodríguez Larreta, se ordenó el allanamiento del domicilio del

[2] Salt, M., *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ad-Hoc, 2017, pp. 23 y ss.

imputado, toda vez que desde su cuenta de Facebook se habrían publicado mensajes amenazantes. En la medida, se dispuso el secuestro de todos los dispositivos electrónicos con acceso a internet desde los cuales se pudiera haber realizado la publicación en Facebook que dio origen a la investigación.

En efecto, se secuestraron dos teléfonos celulares y una computadora. El juez interviniente, a solicitud del representante del Ministerio Público Fiscal, autorizó realizar un peritaje sobre los dispositivos con el objeto de encontrar evidencia del delito de amenazas investigado.

Durante el peritaje, se advirtió la existencia de presuntas imágenes con contenido de pornografía infantil. A tal efecto, la división de la Policía de la Ciudad que llevó a cabo la medida utilizó *software* específico para detectar imágenes y videos de pornografía infantil. A su vez, en uno de los dispositivos también se encontró una carpeta llamada "S. C. piernas infantiles escolares", entre otras.

La Fiscalía, en virtud de los hallazgos y dado que en ese momento la tenencia de imágenes de pornografía infantil no constituía un delito, solicitó ampliar la investigación a fin de determinar si el imputado incurrió en alguna conducta que excediera la mera tenencia de ese tipo de material.

La defensa solicitó la nulidad del peritaje en lo que refiere a los hallazgos de pornografía infantil. Fundó su postura en que, por un lado, los agentes estatales utilizaron *software* para buscar archivos audiovisuales y que, particularmente, se había utilizado una herramienta específica para encontrar imágenes y videos de pornografía infantil sin orden judicial, dado que la búsqueda de ese material no había sido autorizada en el orden que habilitó la medida. Por el otro, indicó que la apertura de la carpeta "S. C. piernas infantiles escolares", entre otras, también constituía un exceso por parte de los agentes estatales, ya que no estaban autorizado a compulsar material no relacionado con las amenazas.

Por su parte, el representante del Ministerio Público Fiscal argumentó que la defensa fue debidamente notificada del peritaje y que podría haber designado un perito para controlar su desarrollo. Además, manifestó que las imágenes de pornografía infantil aparecieron ante los agentes estatales que desarrollaron la medida de forma espontánea, en el marco de la búsqueda de evidencia de las amenazas.

La mayoría de los integrantes del Tribunal hicieron lugar al pedido de la defensa y resolvieron declarar la nulidad del peritaje en lo referido a la pornografía infantil. Entendieron que la utilización de programas para realizar el análisis del contenido digital de los dispositivos secues-

trados, por cuanto permitían filtrar y organizar archivos audiovisuales implicó una violación de la privacidad del imputado, sin respaldo alguno en la orden judicial dictada en el marco de una investigación por amenazas. Más aún, afirmaron que el uso de una herramienta específica para detectar imágenes y videos de pornografía infantil constituyó una *excursión de pesca* (*sic*).

El voto minoritario consideró que no se debía hacer lugar a la nulidad solicitada por la defensa, dado que los archivos de pornografía infantil fueron encontrados de manera espontánea por los agentes que llevaron a cabo la medida. Entendió que los agentes estatales utilizaron herramientas que tienen por función organizar y filtrar archivos de forma indiscriminada, lo que permite mejorar el modo de analizar el contenido digital de los dispositivos secuestrados para encontrar material relevante para la investigación. Advirtió que no se utilizaron herramientas específicas para encontrar imágenes y videos de pornografía infantil. También destacó que el imputado fue informado debidamente del peritaje y tuvo la oportunidad de presentar un perito de parte para controlar su desarrollo.

VI. c. Jurisprudencia internacional

VI. c. 1. Estados Unidos

Décimo *Circuito Judicial de Estados Unidos, caso Nro. 98-3077 United States vs. Carey, 14 de abril de 1999*

El Sr. Carey estaba siendo investigado por tenencia y distribución de cocaína. Una serie de ventas controladas tuvieron lugar en su domicilio, lo que motivaron a las autoridades estatales a solicitar una orden de arresto. Al proceder a cumplirla, los agentes observaron a simple vista que el Sr. Carey tenía un aparato para fumar marihuana y que, dentro de su departamento, había plantas de cannabis. Eso llevó a que la policía le consulte al imputado sí prestaba consentimiento para dejarlos ingresar a su departamento, a lo que respondió afirmativamente. Al ingresar, la policía secuestró dos computadoras, bajo la sospecha que allí podría haber evidencia respecto de la distribución de estupefacientes. Luego, los agentes estatales solicitaron una orden para analizar el contenido

de las computadoras secuestradas a fin de encontrar información relevante sobre el comercio de estupefacientes. La orden fue concedida. Al analizar la información, los agentes observaron la existencia de aproximadamente 240 archivos .jpg con títulos relacionados a cuestiones sexuales. Los guardaron en 19 soportes ópticos. Únicamente pudieron visualizar algunas porciones de esos archivos de imagen y advirtieron que contenían pornografía infantil.

La defensa de Carey solicitó excluir esas imágenes, dado que el agente las observó sin orden judicial y la investigación sobre tenencia de pornografía infantil estaba fuera del alcance de la orden judicial que les permitió acceder al contenido digital de las computadoras. El agente que llevó a cabo la investigación sostuvo que la primera imagen que observó fue por casualidad, mientras que buscaba evidencia del delito relacionado a los estupefacientes, y que luego abrió el resto de las imágenes porque consideraba que debía revisar todo el material informático.

El Tribunal consideró que se debía excluir la evidencia respecto del delito relacionado con la tenencia de imágenes de pornografía infantil. En primer lugar, índico que las imágenes observadas no se encontraban a simple vista de las autoridades estatales, dado que su carácter ilícito (la imagen pornográfica) se hallaba en el contenido de los archivos y no en su etiqueta (el nombre de los archivos), por lo que, quienes revisaron la información digital, solo habrían podido observar a simple vista los archivos con determinados nombres. También sostuvo que, luego de abrir la primera imagen (que, razonablemente, podría haber sorprendido al agente que buscaba evidencia del delito relacionado al tráfico de estupefacientes), el agente comenzó a buscar archivos de pornografía infantil, lo que excedía el alcance la medida original.

Séptim*o Circuito Judicial de Estados Unidos, caso N.º 08-3041, United States v. Mann, 20 de enero de 2010*

En mayo de 2007, mientras trabajaba como instructor de guardavidas para la Cruz Roja en el Estado de Indiana, el Sr. Mann instaló una cámara de videograbación en el vestuario de mujeres. Una mujer que se estaba cambiando observó la cámara. Al hacer la denuncia y observar el video que se había registrado, pudo identificar al Sr. Mann, a quien la cámara había registrado mientras la instalaba.

La Fiscalía del Estado de Indiana solicitó una orden de allanamiento del domicilio de Mann con autorización para secuestrar dispositivos

electrónicos a fin de determinar si contenían imágenes relacionadas con el delito investigado. La orden fue concedida, se ejecutó y se obtuvieron algunas computadoras y discos rígidos, entre otros.

En la etapa de análisis, los investigadores utilizaron el programa FTK para compulsar la información almacenada en los equipos. Este programa, identificó algunos archivos con unas "alertas rojas". La herramienta, en general, atribuye estas alertas a archivos que posee en su base de datos, identificados como ilícitos, la mayoría de las veces por contener pornografía infantil.

A pesar de las alertas rojas, el agente que realizó el análisis continuó abriendo los archivos contenidos en los equipos secuestrados, sin solicitar una nueva orden para investigar la tenencia de pornografía infantil. El agente encontró evidencia de este delito (tanto en los archivos que habían sido señalados por las alertas, como en otros) y la defensa de Mann solicitó excluirla, dado que se la obtuvo sin orden judicial.

El Séptimo Circuito resolvió la cuestión planteada. Entendió que, respecto de los archivos identificados con una alerta roja, el agente del Estado, tras visualizar la alerta, debió haber solicitado una nueva orden judicial. Respecto del resto de los archivos (sobre los que no se había generado ninguna alerta) de pornografía infantil, el Tribunal consideró que no debían ser excluidos, toda vez que la evidencia del delito de tenencia de pornografía infantil fue advertida a simple vista, mientras se buscaban archivos que pudieran servir para la investigación por el delito de investigado en una primera instancia.

Cuarto *Circuito Judicial de Estados Unidos caso N.º 08-5000, United States v. Williams, 21 de enero de 2010*

En septiembre de 2007 un templo bautista del Estado de Virginia comenzó a recibir correos electrónicos del usuario "Franklin Pugh" con contenido amenazante. En uno de los correos "Pugh", se describió como un pedófilo e indicó que no podría concurrir al templo sin abusar sexualmente de alguno de los chicos que lo frecuentaban. En algunos de los correos se mencionaban los nombres de niños que concurrían a la escuela del templo y en algunas ocasiones *emails* con el mismo contenido eran enviados desde otras cuentas.

Las autoridades policiales observaron que una de las cuentas desde las que se había enviado correos amenazantes había sido accedida por

el usuario llamado Karol Williams, la esposa del imputado, con quien concurría frecuentemente a la iglesia amenazada.

La policía solicitó una orden de allanamiento para el domicilio del imputado, con autorización para secuestrar dispositivos electrónicos relacionados que pudieran estar relacionados a las amenazas. Efectivamente, se secuestraron varias computadoras, CD y DVD, entre otros elementos.

Al analizar los dispositivos, la policía encontró numerosas imágenes de pornografía infantil que habían sido eliminadas. También se encontró instalado el programa TOR, el cual se utiliza para disfrazar la IP desde donde las personas se conectan a internet, de modo tal de dificultar la identificación. El agente que desarrolló la medida le envió un correo al Fiscal interviniente destacando lo que habían encontrado y diciendo que *espero encontrar la colección en la computadora personal de Williams*, en referencia a imágenes con pornografía infantil.

La defensa de William solicitó la exclusión de las imágenes de pornografía infantil, ya que, argumentó, no se encontraban alcanzadas por la orden emitida.

El Tribunal sostuvo que el gobierno estaba autorizado a secuestrar todo el material y que, alternativamente si no lo estaba, los elementos secuestrados debían ser admitidos bajo la *plain view doctrine*. Sostuvo que esta excepción se aplica cuando los elementos se encuentran a simple vista de los agentes del Estado, ya que su dueño no puede tener expectativa de privacidad sobre algo que se encuentra completamente accesible a la observación. En este caso puntual, argumentó que la orden dictada autorizaba a las autoridades estatales a analizar uno y cada uno de los archivos contenidos en los dispositivos electrónicos secuestrados y que se autorizaba su apertura. De otra forma, resultaría muy fácil evadir a la justicia dado que no se podría esperar que quienes cometan un delito etiqueten sus archivos con los nombres de ese delito (por ejemplo, una carpeta en el escritorio de una computadora que se llame "pornografía infantil").

Juzgado de Distrito de Maine, United States vs. Brunette, 76 F. Supp 2d. 30, 08 de noviembre de 1999

En 1999 se habían posteado en una página de internet 79 fotografías que contenían imágenes de pornografía infantil. Un grupo dedicado a detectar la presencia de este tipo de imágenes en la web las descubrió

y alertó al proveedor de servicios de internet sobre su existencia. Un investigador privado de este servicio pudo copiar (para asegurar) 33 de estas fotografías y las entregó a autoridades de Estados Unidos, quienes solicitaron una orden de allanamiento para el domicilio de la persona que había realizado el posteo. El juez concedió la orden y habilitó el secuestro de dispositivos electrónicos. Otorgó un plazo de 30 días para realizar el análisis del contenido digital.

Los investigadores del Estado secuestraron dos computadoras. Antes del vencimiento de los 30 días para su análisis forense, solicitaron una prórroga de 30 días, la cual le fue concedida. Dentro del plazo analizaron el contenido de una de las computadoras. Vencido el plazo, analizaron el contenido de la otra. En ambas encontraron pornografía infantil.

La defensa solicitó la exclusión de la evidencia incriminante encontrada en la computadora analizada fuera del plazo dispuesto en la orden judicial.

En efecto, la cuestión planteada era si resultaba la evidencia encontrada en una computadora debidamente secuestrada que fue analizada fuera del plazo dado para realizar el análisis en la orden judicial que habilitó la medida.

El juez interviniente falló a favor de la defensa. Indicó que la evidencia encontrada en la computadora analizada dentro del plazo dispuesto (60 días desde el secuestro, considerando la prorroga otorgada) resultaba válida; pero que la evidencia encontrada en la computadora que fue analizada fuera del plazo de los 60 días debió ser excluida ya que los investigadores no ofrecieron ninguna razón legitima para justificar la demora.

Noveno Circuito judicial de Estados Unidos, Caso N.º 05-50219, United States vs. Hilll, 11 de agosto de 2006

Justin Hill había enviado su computadora a reparar y la persona que realizó el servicio técnico advirtió que el equipo contenía imágenes de pornografía infantil. En consecuencia, avisó a la policía. Los agentes policiales consiguieron una orden para secuestrar el equipo y concurrieron al lugar de reparación de computadoras, pero para ese momento, el Sr. Hill ya había retirado su equipo. Por tal motivo, los investigadores solicitaron y obtuvieron una orden de allanamiento para el domicilio del Sr. Hill. Al llegar al lugar no encontraron la computadora en cuestión, pero sí una serie de equipos digitales que secuestraron. Al analizarlos, advirtieron que contenían pornografía infantil.

El Sr. Hill solicitó la exclusión de la evidencia encontrada en esos dispositivos ya que, argumentó, los agentes habían analizado el contenido de los dispositivos fuera del domicilio donde se encontraban. Según su postura, los agentes solo deberían haber analizado los equipos en su domicilio y secuestrado, únicamente, los elementos incriminantes encontrados en ellos.

La cuestión que debió resolver el Noveno Circuito, en efecto, fue la validez del secuestro de *hardware* para el posterior análisis en un laboratorio (lo que implicaba una habilitación a que, además del material incriminante que se pudiera encontrar, los agentes estatales secuestraren otra información no relevante para la investigación).

El Noveno Circuito consideró que los agentes actuaron correctamente al analizar los dispositivos digitales en su laboratorio. Entendió que hacerlo en el lugar resultaba poco práctico, requería un gran volumen de equipamiento técnico y podía extender el desarrollo de la medida por mucho tiempo.

No obstante, indicó que *(...) los agentes del gobierno deben demostrar al juez las razones fácticas en virtud de las cuales requieren el secuestro de determinados equipamientos digitales (...)*[3] Los jueces entendieron que, en este caso, no se había autorizado debidamente a analizar los dispositivos secuestrados, pero que, sin embargo, no se debía excluir la evidencia porque si bien no se requirieron las órdenes de análisis necesarias al juez, los agentes policiales actuaron *motivados por cuestiones de practicidad, antes que por el deseo de ir a la pesca.*

Noveno *Circuito Judicial de Estados Unidos, casos Nros. 05-10067, 05-15006, 05-55354 United States vs. Comprehensive Drug Testing, 26 de agosto de 2009*

En 2002, el gobierno federal de Estados Unidos había comenzado a investigar al Laboratorio Bay Lab Cooperative (Balco), respecto del cual se sospechaba que proveía de esteroides a jugadores profesionales de béisbol. Ese mismo año, la Asociación de Jugadores Profesionales de

[3] Traducción del autor del original *(...) the government must still demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand (...).*

Béisbol había acordado con la Asociación *Major Leage Baseball* (MLB) proveer test anónimos y confidenciales a todos los jugadores profesionales de ese deporte para determinar la utilización de sustancias prohibidas. A los jugadores se les había informado que los resultados de esas pruebas serían confidenciales al solo efecto de determinar el porcentaje de jugadores que utilizaban sustancias prohibidas.

MLB contrató a Comprehensive Drug Testing Inc. (CDT) para supervisar las pruebas, las cuales eran desarrolladas por Quest Diagnosis Inc. CDT que llevaba el control de los jugadores que practicaron los *test* y sus resultados. Durante la investigación a Balco, el gobierno de EE. UU. obtuvo información de que las pruebas practicadas bajo supervisión de CDT de 10 jugadores habían dado resultados positivos, es decir, indicaban la utilización de productos prohibidos. Por consiguiente, solicitó órdenes de allanamientos para las sedes de CDT y de Quest Diagnosis Inc., a fin de secuestrar, únicamente, la información relativa a los resultados de las pruebas de esos diez jugadores.

Se autorizó el allanamiento y secuestro de información relativa a los diez jugadores con resultados positivos. El juez que dispuso la medida indicó que un técnico en informática, y no un investigador del caso, debería ingresar al sistema informático de CDT, compulsar la información allí contenida y resguardar, únicamente, la relacionada a los 10 jugadores con resultados positivos.

Al ejecutar la medida, el especialista en informática ingresó al sistema y copió una carpeta que contenía el registro de las pruebas de cientos de jugadores de béisbol y de personas no relacionadas al deporte, es decir, no copió la información relacionada, únicamente a los 10 jugadores. La información se compulsó en una etapa ulterior, en la cual los investigadores buscaron los nombres de los diez jugadores involucrados y donde advirtieron la presencia de otros jugadores cuyos resultados también habían arrojado resultados positivos, por lo que ampliaron la investigación.

La CDT y la Asociación de Jugadores Profesionales de Béisbol solicitaron que el gobierno devolviera toda la información secuestrada, menos la correspondiente a los diez jugadores, cuyos registros se había autorizado a secuestrar en un primer lugar. Esta solicitud fue aceptada por la justicia y el gobierno apeló. El caso fue resuelto por el Noveno Circuito de los Estados Unidos, que dijo que el gobierno no podía utilizar la evidencia adicional (es decir, por fuera de los diez jugadores) descubierta, dado que la compulsa fue desarrollada en incumplimiento de

los protocolos de búsqueda que se habían dado (entiendo que se refiere a la orden de que un especialista en informática y no un investigador del caso copiare solo la información relacionada a los diez jugadores).

A su vez, este Tribunal dispuso las siguientes condiciones para el análisis digital de información almacenada: 1) los jueces deben insistir que, para otorgar una orden de allanamiento, el gobierno debe renunciar a utilizar información adicional encontrada bajo la *plain view doctrine*; 2) la segregación de la información digitalmente almacenada debe ser realizada por personal especializado o una tercera parte independiente. Si la realiza un técnico del gobierno, este debe acordar no otorgarle a los investigadores estatales ninguna información que no sea la estrictamente autorizada a obtener mediante la orden judicial; 3) las órdenes judiciales deben establecer los riesgos reales que conlleva destruir la información y las medidas que se tomaron para secuestrar esa información en otras jurisdicciones; 4) el gobierno debe elaborar un protocolo de análisis para, únicamente, acceder a la información respecto de la cual fue autorizado a obtener mediante la orden judicial y 5) el gobierno deberá destruir o (si corresponde) devolver toda la información secuestrada que no resultare relevante, informándole al magistrado interviniente cuándo la ha devuelto y qué ha conservado.

Octavo Circuito Judicial de Estados Unidos, caso Nro. 09-1106, United States vs. Mutschelknaus, 04 de enero de 2010

En el marco de una investigación por distribución de fotografía de pornografía infantil, agentes estatales identificaron a un usuario situado en Alaska denominado "Aronechee", desde el cual se distribuían imágenes ilícitas. Este usuario les entregó a los agentes estatales permiso para utilizar su identidad *online* y, de esta forma, los agentes del Estado le enviaron un mensaje a Mutschelknaus solicitándole que le vuelva a enviar una colección de fotografías, argumentando que (haciéndose pasar por Aronechee) las había perdido. Mutschelknaus le envió 236 fotografías, la mayoría de ellas con imágenes de pornografía infantil. Los agentes estatales ubicaron la dirección desde donde Mutschelknaus había enviado los archivos y solicitó una orden de allanamiento para inspeccionar el lugar. El juez interviniente aprobó la orden y otorgó un plazo de 10 días para practicar el allanamiento y 60 días adicionales para analizar el material electrónico que, eventualmente, se secuestrase.

Los agentes estatales cumplieron con el plazo interpuesto y encontraron archivos de imágenes de pornografía infantil. La defensa de Mutchelknaus solicitó la exclusión de la prueba, argumentando que el plazo de 60 días era muy extenso.

El Octavo Circuito de los Estados Unidos decidió que el plazo establecido por el juez era correcto y que, dado que la medida se había practicado dentro de ese plazo, la evidencia no debía ser excluida.

VII. Acceso transfronterizo a datos digitales

VII. a. Introducción

Una de las cuestiones de mayor controversia, tanto en el ámbito del Derecho Procesal Penal como del Derecho Internacional, es la posibilidad de que las autoridades encargadas de la persecución penal puedan acceder a prueba digital que se encuentre alojada en servidores o dispositivos informáticos situados en extrañas jurisdicciones. Muchos de los supuestos en que un Estado accede a evidencia alojada en extraña jurisdicción pueden ser considerados por los otros Estados u organismos internacionales como violaciones al principio de territorialidad afectando la soberanía de los Estados. Esta controversia se profundiza aún más en el uso de sistemas informáticos complejos con capacidad de almacenar datos informáticos, como el *cloud computing* también conocida como la nube–, que pueden contener grandes cantidades de datos en servidores que están ubicados a lo largo y ancho del mundo y cuya jurisdicción puede variar según se transporten de un servidor a otro.

En lo que respecta a la legislación actual, el Convenio para la Ciberdelincuencia de Budapest establece que los Estados parte cooperaran entre sí en mayor medida posible en la aplicación de instrumentos internacionales sobre cooperación internacional en materia penal

y de los acuerdos basados en legislación uniforme o recíproca (arts. 23 y 25). La normativa insta a las partes a prestar toda la ayuda mutua posible en el marco de las investigaciones. No obstante, contempla que esta asistencia mutua debe estar sujeta a las condiciones que establezca el derecho interno (salvo excepciones), lo que podría llevar a la parte requerida a rechazar la cooperación. Esto se debe a que, en el núcleo de la cuestión, los acuerdos de cooperación internacional se encuentran atravesados por la mencionada soberanía de los Estados, y esta podría verse vulnerada si se permite a un Estado extranjero recabar evidencia en extraña jurisdicción. Por otro lado, desde mediados de 2019, la Unión Europea aprobó negociar un acuerdo con los Estados Unidos que facilite el acceso transfronterizo en la búsqueda de prueba digital penal. El objetivo prioritario es la confección de un tratado multilateral que reunirá a Estados con ordenamientos jurídicos muy distintos de los propios de los países miembros de la UE, a fin de diseñar mecanismos de asistencia mutua más efectivos, en particular, mediante la cooperación directa con los ISP (Proveedor de Servicios de Internet, o Internet Service Providers por sus siglas en inglés) radicados en otras jurisdicciones.[1]

Esto podría ser un punto de partida para una legislación internacional en materia procesal que cambie el paradigma jurisdiccional, y que logre alcanzar nuestra legislación nacional, en la que carecemos de procedimientos aptos para dichas investigaciones; máxime, cuando hablamos de un mundo digital que no reconoce fronteras y donde la interpretación tradicional del principio de territorialidad pierde esencia frente la persecución de los delitos. El proyecto más ambicioso sobre esta temática es la redacción del segundo Protocolo Adicional de la Convención de Budapest, dedicado específicamente a esta cuestión nucleando a los 65 estados miembros, entre los que participa activamente la Argentina.

Este Segundo Protocolo adicional al Convenio de Budapest está en su última etapa de elaboración. Recientemente se abrió un nuevo

[1] La UE aprueba negociar un acuerdo con EE. UU. para facilitar el acceso transfronterizo a pruebas electrónicas. (2019). Lefebvre. Disponible en: https://elderecho.com/la-ue-aprueba-negociar-acuerdo-eeuu-facilitar-acceso-transfronterizo-pruebas-electronicas

proceso de consultas y opiniones de la sociedad civil. El borrador de Protocolo que fue compartido por las autoridades del Consejo de Europa permitió ver el avance en protección de datos personales y garantías para individuos en los que se está trabajando actualmente. Su objetivo es el de agilizar las investigaciones criminales en entornos digitales. Así, el Protocolo prevé modernas técnicas de cooperación internacional para la obtención de evidencia digital y que al mismo tiempo brinden amplia protección a los datos personales de quienes resultan objeto de dichas investigaciones.

Entre las medidas que incorpora el Segundo Protocolo, se encuentra la posibilidad de dictar órdenes transfronterizas para la obtención de datos directamente a proveedores de servicios de internet, la posibilidad de conformar Equipos Conjuntos de Investigación entre diversos estados miembros para la investigación de ciber-delitos e incluye también medidas de cooperación internacional más ágiles en casos de emergencia.

Los redactores del protocolo, en conjunto con representantes de autoridades europeas de protección de datos personales, elaboraron un texto que brinda un adecuado balance entre la necesidad de posibilitar investigaciones criminales eficientes y efectivas y el debido respeto a los derechos humanos.

El Consejo de Europa estima finalizar el trabajo de redacción del protocolo durante 2021.

VII. b. Jurisprudencia internacional

VII. b. 1. Estados Unidos

Tribu*nal del distrito de Connecticut, Caso 175 F. Supp. 2d. 367 Estados Unidos v. Ivanov (3:00CR00183-AWT), 6 de diciembre de 2001*

A principios de 2000, el FBI se encargó de investigar a Aleksey Vladimirovich Ivanov y Vasiliy Gorshkov, dos hackers rusos, quienes desde su país de origen llevaron a cabo acceso ilegítimo a varios sistemas informáticos de los Estados Unidos.

Esto afectó a varias compañías, bancos, tarjetas de crédito, ISP (proveedores de servicios de internet), entre otros. Gracias a esto, los

hackers obtuvieron acceso a datos personales mediante los cuales llevaron a cabo diversos fraudes.

Una de las empresas afectadas, OIB (Online Information Buro), que guarda la información de las tarjetas de crédito de los clientes, recibió varios mails extorsivos por parte de los imputados exigiendo dinero a cambio de que estos mejorasen su sistema de seguridad; caso contrario, al tener en su poder la clave de acceso al sistema, borrarían todos los datos de este.

El FBI decidió llevar a cabo un operativo para atraer a ambos hackers y así proceder a su pronta detención y enjuiciamiento. Crearon una empresa de Seguridad Informática y les ofrecieron trabajo invitándolos a los Estados Unidos. Haciéndose pasar por miembros de la compañía ficticia, solicitaron a ambos sospechosos que ingresaran de forma ilegítima al sitio web de una empresa ficticia. La finalidad era engañarlos para que llevaran a cabo delante del FBI todas las maniobras requeridas para cometer el delito. Todos sus movimientos fueron grabados en la computadora, captando como ingresaron desde Estados Unidos a sus sistemas alojados en Rusia y de allí accedieron al *software* necesario para el ingreso ilegítimo. Con esto, el FBI obtuvo la clave de acceso a los servidores en Rusia y detuvo en el acto a Ivanov y Gorshkov.

Las fuerzas del FBI ingresaron a los servidores localizados en Rusia y se llevaron con ellos las pruebas que necesitarían para más tarde condenarlos; todo ello sin mediar ningún mecanismo cooperación internacional o contacto con el país extranjero.

Ivanov y Gorshkov fueron acusados de conspiración, fraude informático, *hackeo* y extorsión. Gorshkov fue encarcelado en Seattle, donde tuvo mayor impacto sus accionar. En tanto, Ivanov fue trasladado a Connecticut, para ser juzgado en el Estado donde tiene sede la OIB.

La defensa de Ivanov argumentó que el tribunal carecía de jurisdicción, puesto que él se encontraba ubicado físicamente en Rusia al momento de cometer los delitos, por ende, no podía ser juzgado por la ley norteamericana. El tribunal rechazó el planteo, motivándose en que sin importar donde estuviese localizado el autor del delito, los efectos de sus actos ocurrieron en los Estados Unidos. Y agregó *las normas y estatutos por las cuales le fueron imputados los delitos se entienden son de aplicación extraterritorial.* Finalmente, Ivanov y Gorshkov fueron condenados utilizando evidencia que se obtuvo mediante un acceso transfronterizo.

Segun*do circuito de la corte de apelaciones de los Estados Unidos, caso 14-2985-cv Microsoft v. Estados Unidos, 14 de julio de 2016*

En diciembre de 2013, en marco de una investigación de tráfico de drogas, un juez del Estado de Nueva York, en virtud de la Ley de Comunicaciones Almacenadas (SCA) emitió una orden judicial, en la que le requería a la empresa Microsoft la entrega de toda la información y correos electrónicos vinculados a una cuenta de email de un cliente de la compañía.

Si bien en principio, Microsoft accedió a entregar los metadatos, se rehusó a entregar aquellos que consideraba "con contenido" bajo los argumentos de que dicho contenido se encontraba alojado en servidores, que, si bien son de Microsoft, su localización física se encuentra en Dublín, en la República de Irlanda, por lo que el acceso a esos datos requeriría autorización de un juez de aquel país.

Si bien el gobierno de EE. UU. consideró que este país tenía jurisdicción sobre esos datos, en tanto se podían acceder de ese país, el juez de primera instancia le dio la razón. Microsoft apeló. El Segundo Circuito de EE. UU. anuló el fallo de primera instancia. El principal fundamento fue la extraterritorialidad de la SCA, fundándose en precedentes de la Corte Suprema en que se resuelve que las normas dictadas por el congreso, salvo excepción, deben aplicarse dentro de la jurisdicción de los Estados Unidos.

El departamento de justicia de los Estados Unidos apeló ante la Corte Suprema, argumentando que la decisión del segundo circuito permitía a empresas como Microsoft negarse a cooperar con los agentes del Estado dificultando la persecución penal, en tanto la información estuviese alojada en el exterior. A esto Microsoft contestó que el gobierno debería tener por procedente la apelación y en cambio es el congreso quien debe actualizar la ley que devino en obsoleta.

En plena decisión de la Corte, el congreso introdujo la CLOUD Act, que modificó la SCA y posee un nuevo procedimiento para obtener evidencia localizada en extraña jurisdicción.

A partir de ella se emitió una nueva orden en los términos de la CLOUD Act y se comunicó a la Corte Suprema que dejara sin efecto el pedido de apelación, puesto que ya no buscaba la resolución de este, y devolviera a los tribunales inferiores. La Corte emitió un dictamen en abril de 2018 declarando el caso inútil y devolvió el caso a los tribunales inferiores desestimando la demanda.

Tribu*nal de distrito de los Estados Unidos para el distrito del este de Pensilvania, orden de allanamiento No. 16-960-M-01 a Google, 19 de octubre de 2017*

En agosto de 2016, el juez del distrito de Pennsylvania emitió dos órdenes de allanamiento requiriendo a la empresa Google inc. entregar al FBI una serie de emails y demás datos electrónicos de dos cuentas usadas por los sospechosos de dos investigaciones penales.

Ante dicha orden la empresa contestó que enviaría la información que está almacenada en los servidores ubicados dentro del territorio de los Estados Unidos; no obstante, rechazó hacer lo mismo con aquellos correos e información que puedan hallarse en servidores en territorio extranjero. Debido a la forma en que Google almacena esta información, los mails de una cuenta pueden encontrarse en servidores a lo largo y ancho del mundo, amparándose en lo fallado hasta entonces en el caso *Microsoft v. Estados Unidos*.

El juez Thomas J. Rueter falló ordenando que Google debía cumplir con todas las exigencias, no solo para con aquellas cuya información se encuentre almacenada en EE. UU. Determinó que la invasión a la esfera privada ocurrirá dentro del territorio y el registro de los datos pedidos será llevado a cabo también dentro del mismo territorio, lo cual hace a una aplicación local de la SCA. Y que, por ende, traer copias desde servidores extranjeros al país no resulta en una violación de la cuarta enmienda.

El tribunal consideró que transferir información desde un sistema informático localizado en el extranjero y llevada hacia los Estados Unidos no reporta incautar porque no se está privando al dueño de disponer de datos o correos. A su vez, estimó que tampoco se está violentando la soberanía de ningún Estado, puesto que la invasión a la privacidad tendrá lugar dentro de los Estados Unidos, aún si los datos son recuperados desde un servidor en el extranjero. Si la orden de registro y secuestro se lleva a cabo dentro del territorio nacional, entonces un igual carácter puede ordenarla.

El tribunal argumentó que de esta forma se pueden evitar resultados absurdos. Puesto que Google no sabe exactamente dónde se encuentra almacenada la información, pero esta puede ser accedida y es recopilada desde California, donde puede copiarlos y enviarlos al FBI; de aplicarse el mismo resultado del fallo Microsoft, implicaría no poder hacerse con la información requerida por ningún medio.

Sobre la base de estos razonamientos, el tribunal del Estado de Pensilvania ordenó que la empresa Google Inc. Cumpla con las órdenes de allanamiento y entregue toda la información solicitada al FBI.

VIII. Utilización de OSINT - Open Source Intelligence en investigaciones penales

VIII. a. Introducción

Es la práctica que implica el uso de un conjunto de técnicas y tecnologías que facilitan la recolección de información que se encuentra disponible públicamente, como pueden ser textos, imágenes, videos, audios, e incluso datos geoespaciales. Consiste en aprovechar la cantidad de información disponible para todo público con el fin de convertirla en inteligencia accionable.

Debemos ponderar, en este punto, que existe un debate respecto de su utilización en materia de prevención del delito (el denominado rastrillaje informático o "ciber patrullaje"), y que se encontraría dentro del ámbito de la inteligencia criminal, que se diferencia del mecanismo de recolección de este tipo de pruebas en el marco de una investigación criminal ya iniciada, lo que no se encuentra específicamente previsto en la legislación procesal.

Como hemos adelantado la utilización de estas prácticas en el marco de investigaciones judiciales no está específicamente prevista en las leyes procesales, aunque su uso ha sido admitido por distintos tribunales, que validan la incorporación al proceso de la información recolectada si fue publicada voluntariamente por la imputada en una plataforma digital que es accesible por terceros,

En materia de prevención del delito, la Resolución 144/2020 del Ministerio de Seguridad de la Nación, Protocolo General para la Prevención Policial del delito con uso de fuentes digitales abiertas deroga la anterior normativa que regía parcialmente la actividad, la 31/2018, y establece *principios, criterios y directrices generales para las tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad que se llevarán a cabo únicamente mediante el uso de fuentes digitales abiertas.*

La Resolución indica que las directrices del Protocolo General serán de aplicación subsidiaria, en lo pertinente, a las tareas de investigación criminal que realizan los cuerpos policiales y fuerzas de seguridad como órganos auxiliares de la justicia, en tanto impliquen una doctrina compatible con las instrucciones que impartan los magistrados y permitan su mejor ejecución.

Tampoco fue hallada en el derecho comparado normativa especial respecto del uso de OSINT en los procesos judiciales. Como en mayor parte ocurre, la utilización de estas nuevas técnicas de investigación es analizada con el prisma de su potencial afectación a garantías constitucionales. Para estas herramientas en particular, la categoría de análisis de relaciona con el resguardo de la garantía que protege la privacidad y el secreto de las comunicaciones, siendo mayoritaria la doctrina que admite la obtención de elementos de prueba *cuando se trata de información de conocimiento público para cualquier usuario de internet y que el propio usuario de la red es quien lo ha introducido en la misma* (en el caso del rastreo de direcciones IP por parte de la Policía Judicial de España) *o cuando se trata de actuaciones equivalentes a una labor de vigilancia convencional.*

En Alemania, debe tenerse en cuenta lo decidido por el Tribunal Constitucional el 15 de diciembre de 1983, al aludir al Derecho a la autodeterminación informativa como el derecho de los ciudadanos a conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos, criterio que fue desarrollado en los años subsiguientes al ritmo del avance tecnológico, hasta llegar a alertar sobre el riesgo de que el uso de la tecnología, a través del acopio y cruce masivo de datos, pueda dar lugar a la creación de los referidos perfiles de personalidad de los

ciudadanos hasta el punto de llegar a influir de manera determinante en el comportamiento de los individuos.[1]

VIII. b. Jurisprudencia argentina

VIII. b. 1. Fuero federal

Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala II, "D.C.N.F.F.X. x/ procesamiento", 3 de febrero de 2020

La encuesta se inició como consecuencia del resultado que arrojaron las tareas de relevamiento en la web que efectuó personal de la División Intervenciones Informáticas Complejas perteneciente a la Superintendencia de Delitos Tecnológicos de la Policía de la Ciudad, el marco de las cuales pudieron advertir que a través del dominio www.mercadolibre.com.ar un usuario identificado como d. se ofrecían para la venta diferentes relojes cuyos valores no guardaban correspondencia con los de plaza para productos de esas marcas

El juez interviniente dispuso diversas diligencias orientadas a individualizar al usuario y a establecer la vigencia del registro marcario –conf. fs. 11, 12/46, 54/5–, agregándole luego el listado que contenía el historial de ofertas –fs. 72/100–. Avanzando, se hicieron tareas de investigación en derredor del domicilio y se identificó al ofertante, posteriormente procesado por infracción al artículo 31, inciso "d" de la Ley 22.362.

La defensa apeló el pronunciamiento apuntando que la investigación debía declararse inválida desde su inicio por haber implicado una intromisión indebida en el ámbito de reserva constitucionalmente protegido.

La Cámara de Apelaciones rechazó el recurso, con fundamento en que no hubo investigación sin orden por parte de la autoridad policial sino tareas de relevamiento cuyos resultados, puestos en conocimiento de la instrucción, dieron inicio recién entonces a esta investigación".

[1] Conf. Ortiz Pradillo, Juan Carlos, "La investigación del delito en la era digital", p. 22.

"Asimismo, dicha actividad en modo alguno puede considerarse como una intromisión indebida dentro del ámbito privado de las personas a poco que se repare en que fue realizada en derredor de un sitio de acceso público que opera como una plataforma para el intercambio bienes y servicios entre los usuarios", concluyó el Tribunal de Alzada.

Cámara *Federal de Casación Penal, Sala IV, caso FSM 10817/2016/TO|/ CFC1 "Herrera, Iván Matías y otros s/ recurso de casación", 14 de febrero de 2019*

En la noche del 27 de marzo de 2016, el imputado Herrera junto a otra persona interceptaron y abordaron el automóvil de Juan Carlos Cachia, un Honda Civic, a quien obligaron a pasarse al asiento trasero. Luego de circular por 10 minutos, pasaron a la víctima a un Renault Sandero Stepway, llamaron a su novia y le exigieron un rescate para la liberación, lo que, tras una negociación, ocurrió.

A su vez, el 25 de marzo de 2017[2], a las 23:50 h, los imputados Herrera, Vera y Córdoba detuvieron el automóvil donde se encontraba el Sr. Esteban Pieretti, lo obligaron a bajarse y subirse a otro vehículo, un Renault Sendero Stepway. Allí adentro, los imputados se comunicaron con la madre de la víctima y le exigieron un rescate por su liberación. Luego de una negociación, se efectuó el pago del rescate y Pieretti fue liberado.

Tras realizar tareas investigativas encubiertas en las zonas vinculadas a los hechos referidos, se obtuvieron indicios acerca de la identidad de los posibles autores de los secuestros. Para avanzar en la investigación, las fuerzas policiales analizaron los perfiles públicos de la red

[2] No queda claro si es 2017 o 2018. El Tribunal de casación transcribió textualmente los hechos descritos en el requerimiento de elevación a juicio. En él se hace referencia a dos hechos, el secuestro de Pieretti, que ocurrió, según surge del requerimiento referido, durante el "año en curso" y el secuestro de Cachia que ocurrió, según ese mismo requerimiento, en 2016. Dado que en el mismo requerimiento se diferencian temporalmente estos dos hechos, se advierte que el secuestro de Pieretti no pudo haber ocurrido en 2016 y, como el juicio oral fue en 2018, se entiende que el hecho ocurrió en 2017 o en 2018. Dado que el juicio oral culminó el 21 de marzo de 2018, se considera más probable que el requerimiento de elevación a juicio haya sido de 2017.

social Facebook de los sospechosos, sin contar con orden judicial. De allí se obtuvieron imágenes de los posibles autores a efectos de que las víctimas determinaran si se trataba de los secuestradores, lo que arrojó resultados positivos.

El Sr. Herrera fue condenado por el Tribunal Oral en lo Criminal Federal N.º 5 de San Martín como coautor de los dos hechos. Los Sres. Vera y Córdoba, como coautores del segundo hecho.

Las defensas apelaron la sentencia por considerar, entre otras cuestiones, que el análisis de los perfiles de Facebook de los imputados constituyó una "excursión de pesca" que implicó una injerencia arbitraria a la privacidad sin la debida orden judicial.

Con cita al fallo "Bejarano, Alexis Ezequiel s/recurso de casación", de la misma Sala IV, los integrantes del Tribunal, en votos separados, consideraron que las investigaciones en los perfiles públicos de la red social Facebook no requieren de una orden judicial para llevarse a cabo. Para fundamentar tal postura consideraron que las publicaciones "públicas" en esa red social conllevan una autorización para su difusión y permiten el acceso a tanto a seguidores como terceros ajenos, dado que carecen de cualquier tipo de restricción de privacidad. Por tal motivo, las tareas realizadas en los perfiles de los imputados en la red social referida no implicaron injerencia alguna en la privacidad de los individuos y, en consecuencia, resultaron válidas.

Juzgado *Nacional en lo Criminal Federal N° 4, Causa CFP 2398/2019, 23 de mayo de 2016*

El área de Cibercrimen de la Policía Metropolitana, en el marco de tareas de ciberpatrullaje que –"rastrillaje en fuentes abiertas" (*sic*)– se realizaban de forma rutinaria con la finalidad de prevenir delitos, contravenciones y faltas, se detectaron mensajes amenazantes contra Mauricio Macri, entonces Presidente de la Nación, y su hija, provenientes del perfil @lamarikaos. Advirtieron esos mensajes por la repercusión que tuvieron en la red social referida.

Posteriormente, las fuerzas de seguridad dieron intervención a la justicia federal para preservar esos mensajes y se inició una investigación para identificar a la autora. A raíz de la información de las conexiones IP del usuario referido informadas por Twitter y de "búsquedas relacionadas" (*sic*) con las publicaciones amenazantes se identificó a

Maribel Anahí Durand como la usuaria del perfil mencionado, desde el cual se publicaron las amenazas.

Sobre la base de eso, se indagó a la Sra. Durand y se la procesó por los delitos de amenazas e incitación al odio y la discriminación.

En el auto de procesamiento no se cuestionó ni analizó la constitucionalidad o legalidad del ciberpatrullaje.

Cámara *Federal de Casación Penal, Sala IV, "BEJARANO, Alexis Ezequiel s/recurso de casación" 4 de diciembre de 2015*

El recurso de casación fue presentado por la defensa de Alexis Bejarano luego de que el Tribunal Oral en lo Criminal N° 20 de la Capital Federal lo condenara por el delito de homicidio calificado por haber sido cometido con alevosía a la pena de prisión perpetua.

En lo que aquí interesa, la defensa solicitó se declare la nulidad de todo lo actuado por haberse incorporado prueba obtenida de un perfil de la red social Facebook sin orden judicial y –a criterio de la defensa– eso violó el derecho la privacidad de su asistido y que la información allí volcada correspondía comunicaciones electrónicas que se encuentra protegida en el art. 153 del CP.

Específicamente, la prueba que criticó su incorporación se trató de unas tareas destinadas a la identificación de los autores del hecho, que habían sido los vecinos quienes sindicaron a un sujeto apodado "Chucky" como autor del hecho. Y que fue luego, a través de una página de "Facebook" que se consiguió atribuir tal apodo a Alexis Ezequiel Bejarano, lo que pudo ser recabado del contenido de la red social, correspondiente a la cuenta propiedad del nombrado.

Se corroboró que se trataba de información pública a la que se accedió desde un navegador. En palabras del tribunal, *La red social "Facebook" es un sitio web que se encuentra disponible para cualquier usuario de la red y se utiliza para que sus usuarios puedan intercambiar comunicación fluida y compartir contenido de forma sencilla a través de internet.*

A partir de sus características públicas la página de Facebook propiedad del imputado no goza de la protección de la privacidad como la clásica vía postal. Ello así, desde que si bien para su funcionamiento y utilización se requiere indispensablemente de un prestador del servicio, el nombre de usuario y clave de acceso destinados a impedir que terceros extraños se entrometan en los datos y contenidos que se emiten y

reciben, lo cierto es que el perfil de BEJARANO en la red social en cuestión era público y casi toda la información que compartía podía ser vista por cualquier persona que accediera a través de internet a la página.

En este sentido, la página de Facebook no puede ser considerada la "correspondencia epistolar" que protege la Constitución Nacional, razón por la cual el modo en que fue obtenida e incluso su incorporación como prueba al juicio, mal puede violar la garantía contenida en el art. 18 de la CN.

A partir de lo expuesto, entiendo que el procedimiento por el cual se obtuvo e incorporó como prueba la página de Facebook mediante la cual se pudo corroborar que el sujeto apodado "Chucky" se correspondía con el nombre y fotografía que figuraban en ese perfil de la red social fue realizado conforme a las disposiciones legales vigentes sin afectar la garantía que prohíbe intromisiones arbitrarias en la intimidad y privacidad del imputado y por ello propongo rechazar el presente agravio.

Así, por unanimidad el máximo tribunal del país considero que la incorporación de información que surge de la búsqueda en fuentes abiertas es válida y no requiere de autorización judicial por tratarse de datos de acceso público.

IX. Agente encubierto digital

IX. a. Introducción

Se trata de una medida para combatir delitos complejos en los que intervienen las nuevas tecnologías como medio para su comisión. Así, el agente encubierto digital es un mecanismo de investigación en las redes cuyo fin consiste en constatar en canales cerrados de la red, la comisión de delitos que se consideran graves e identificar a sus autores que se ocultan en el anonimato que internet les brinda. En algunos casos, resulta necesario, a tal fin, que el agente que desempeñe la tarea cometa algún delito para lograr su objetivo, ej., enviar un archivo con contenido ilícito, como lo es una imagen de explotación sexual infantil, a fin de ser admitido en un foro cerrado de pedófilos.

Así, podríamos definir al agente encubierto digital de la siguiente manera: un empleado o funcionario público –dependiendo la legislación– que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red y que causen una gran repulsa y alarma a nivel social.

Su función consistiría en la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un período de tiempo prolongado en el

mundo en el que los ciberdelincuentes actúan con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales.[1]

En cuanto a los beneficios de su aplicación, y comparándolo con la figura de agente encubierto clásico este trae aparejado ciertas ventajas: en primer lugar, no se estaría poniendo en riesgo la integridad física del agente de seguridad que está llevando adelante la medida, ya que las acciones que va a realizar serán siempre por medios electrónicos. En segundo lugar, el agente encubierto digital permitirá guardar un registro electrónico de su accionar. A modo de ejemplo, se registran las conversaciones mantenidas por el agente, lo que permitirá validar su forma de actuar ante eventuales planteos que lo cuestionen.[2]

Teniendo en cuenta lo expuesto hasta el momento y lo sostenido por la doctrina, podemos delimitar ciertas características y presupuesto que deben existir para hacer uso de esta medida:

- se debe tratar de investigaciones de delitos graves.

- carácter excepcional: debe utilizarse la figura del agente encubierto digital cuando no es posible esclarecer los hechos o identificar al autor de la maniobra investigada mediante otras medidas probatorias menos lesivas (principio de subsidiariedad).

- taxatividad: debe utilizarse para aquellos delitos para cuya investigación se encuentra prevista la figura (al menos, la figura de agente encubierto clásica o tradicional).

- su accionar debe estar delimitado y autorizado judicialmente: se deben establecer las acciones que se encuentra autorizado a llevar a cabo el agente, delimitándose a su vez el período de tiempo mediante el cual podrá operar.

Habiendo así delimitado en qué consiste la medida de agente encubierto digital, y a los fines de este trabajo de investigación, corresponde

---

[1] Bueno de Mata, Federico "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia" en *Los retos del Poder Judicial ante la sociedad globalizada.* Actas del IV Congreso Gallego de Derecho Procesal (I Internacional) A Coruña, 2 y 3 de junio de 2011, Agustín Jesús Pérez-Cruz Martín (dir.), Xulio Ferreiro Baamonde (dir). A Coruña: Universidade, 2012, pp. 295-306.

[2] En este sentido ver Temperini, M. y Macedo, M. "Nuevas Herramientas de investigación penal: el agente encubierto digital" en *Cibercrimen*, Buenos Aires, Bdef, edición 2016, pp. 511 y siguientes.

analizar si esta nueva herramienta se encuentra prevista en las legislaciones procesales que hemos elegido como objeto de análisis.

En este sentido, y en relación con las jurisdicciones a analizar en nuestro país, ni en el Código Procesal Penal de la Nación ni en los Códigos Procesales Penales de CABA (ley Nro. 2.303), provincia de Buenos Aires (ley Nro. 11.922), Mendoza (ley Nro. 6.730), ni Córdoba (ley Nro. 8.123) se encuentra legislada la medida en cuestión.

Sin perjuicio de ello, y volviendo a la medida de agente encubierto clásica, sí contamos en nuestro país, a nivel nacional, con la Ley de Delitos Complejos Nro. 27.319[3] que prevé las figuras de agente encubierto, revelador, informante y entrega vigilada para la investigación, prevención y combate de los delitos vinculados a la Ley Nro. 23.737, secuestro, trata de personas, asociaciones ilícitas, contrabando de estupefacientes, todas las conductas previstas en el art. 128 del Código penal –distribución, facilitación, producción, tenencia, etc., de material de explotación sexual infantil–, entre otras conductas específicamente establecidas en el art. 2º de la citada norma. Al tratarse de una norma de carácter nacional, será aplicable en todo el territorio argentino.

Esta norma, en cuanto al agente encubierto específicamente, establece que serán agentes encubiertos los miembros de las fuerzas de seguridad autorizados a tal fin, quienes deberán estar altamente calificados para dicha tarea (art. 3º). A su vez, se establece que la medida en cuestión deberá ser ordenada por el Juez interviniente de oficio o a pedido del Ministerio Público Fiscal, poniendo en manos del Ministerio de Seguridad de la Nación la designación e instrumentación necesaria para la protección del agente, siempre con control judicial (art. 4º). Un aspecto relevante de esta regulación es que exime de responsabilidad penal a los agentes que deban cometer delitos como consecuencia de la actividad encomendada (art. 9º). Veremos, al analizar las legislaciones comparadas, que no todas adoptan este criterio.

Sin perjuicio de lo expuesto, y advirtiendo que la norma antes citada tiene alcance nacional, en al ámbito de la Ciudad Autónoma de Buenos Aires se introdujeron modificaciones al Código Procesal

[3] Ley 27.319 de Delitos Complejos. Investigación, prevención y Lucha de Delitos Complejos. Herramientas. Facultades. Publicada en el B.O., el 22 de noviembre de 2016.

Penal[4], específicamente en el año 2018 incorporándose la figura del agente encubierto clásica. Así, dentro del capítulo incorporado denominado "medidas especiales de investigación", y específicamente en el art. 153 inc. a) del CPPCABA (conforme texto consolidado por Ley Nro. 6347), se incluyó la figura del agente encubierto, estableciendo que podrá serlo un funcionario de las fuerzas de seguridad o de investigación judicial, siempre requiriéndose para ello autorización judicial.

En cuanto a los delitos para los que podrá emplearse esta medida, se establecen específicamente en el art. 152 del CPPCABA, que se encuentran comprendidos, entre otros, infracciones a la Ley Nro. 23737, los artículos 125 –corrupción de menores– y 128 – explotación sexual infantil– y todos aquellos delitos cuyas penas fueran superiores a tres (3) años de prisión en abstracto y que se justifiquen en la complejidad de la investigación del hecho.[5]

En este caso, y tratándose de un sistema acusatorio, lo dispondrá el Juez de garantías a pedido del Ministerio Público Fiscal, encomendán-

---

[4] Ley Nro. 6020 sancionada el 4/10/2018 y promulgada por decreto Nro. 350/018 del 30/10/2018, publicada en el BOCBA Nro. 5490 del 1/11/2018.

[5] Art. 152. CPPCABA (conforme texto consolidado por Ley Nro. 6347). Implementación de medidas probatorias
Las medidas especiales de investigación serán procedentes únicamente en la investigación sobre la posible comisión de los siguientes delitos: Ley 23737 y modificatorias, en delitos previstos en los artículos 125, 125 bis, 126, 127, 128 y 131 del Código Penal, y delitos cuyas penas fueran superiores a tres (3) años de prisión en abstracto y que se justifiquen en la complejidad de la investigación del hecho, solicitará autorización al/la juez/a por auto fundado, bajo pena de nulidad.
Su aplicación deberá regirse sobre la base de los principios de necesidad, razonabilidad, subsidiariedad y proporcionalidad, con criterio restrictivo, debiendo ponderar en todo momento la gravedad del delito investigado y su complejidad.
El juez resolverá la petición dejando constancia, en acta reservada, la que deberá contar con la solicitud del fiscal, los fundamentos que esgrime, así como también la decisión adoptada, sus fundamentos y bajo pena de nulidad.
En los casos en que el/la Juez/a acepte la solicitud deberá consignar en el acta la duración de la medida, los límites y condiciones bajo las cuales puede desarrollarse y los plazos de seguimiento y revisión de la medida dispuesta. El fiscal podrá solicitar ampliaciones de la medida y prórrogas a su duración en entrevista personal con el/la Juez/a, quien, luego de escuchar las razones que fundamentan el pedido, resolverá dejando constancia en acta en la forma prevista para la primera solicitud.

dose al Ministerio de Justicia y Seguridad su implementación, dejando abierta la posibilidad de que se cree un organismo en el futuro que lo reemplace. Sin perjuicio de qué organismo sea, siempre deberá actuar en forma directa y con noticia al MPF. Por su parte, esta legislación local de la CABA exime también de responsabilidad penal al agente encubierto que, en el marco del desarrollo de la actividad encomendada, incurra en la comisión de un delito (art. 154 CPPCABA conforme texto consolidado por Ley Nro. 6347); claro está, siempre y cuando no se ponga en peligro la vida o integridad física o psíquica de una persona, o la imposición de un grave sufrimiento físico o moral a otro.

Por último, un punto no menor de la legislación de CABA es que establece un plazo de 90 días para llevar a cabo la medida en cuestión, pudiendo ser prorrogada por el mismo término una única vez, por auto fundado, debiendo a su vez registrarse mediante un medio técnico idóneo la información obtenida, para luego poder ser valorada asegurándose su inalterabilidad (art. 155).

En cuanto al Código Procesal Penal de la provincia de Mendoza, también prevé específicamente la figura del agente encubierto clásica en su art. 29.[6] En lo que aquí concierne, podrá utilizarse para la in-

[6] ARTÍCULO 29.- Actuación encubierta. El fiscal de instrucción o el Juez de Garantías, en su caso, podrán, por resolución fundada, de manera permanente o durante una investigación, por un delito con pena mayor de tres años, autorizar que una persona, o agente de policía, actuando de manera encubierta a los efectos de comprobar la comisión de algún delito o impedir su consumación, o lograr la individualización o detención de los autores, cómplices o encubridores, o para obtener o asegurar los medios de prueba necesarios, se introduzca como integrante de alguna organización delictiva, o actúe con personas que tengan entre sus fines la comisión de delitos y participe de la realización de algunos de los hechos previstos en el Código Penal y Leyes especiales de este carácter.
La designación deberá consignar el nombre verdadero del agente y la falsa identidad con la que actuará en el caso, y será reservada fuera de las actuaciones y con la debida seguridad.
La información que el agente encubierto vaya logrando será puesta de inmediato en conocimiento del juez.
La designación de un agente encubierto deberá mantenerse en estricto secreto. Cuando fuere absolutamente imprescindible aportar como prueba la información personal del agente encubierto, este declarará como testigo, sin

vestigación de delitos cuya pena supere los tres (3) años de prisión. Se establece que podrá ordenarlo el Fiscal de Instrucción o el Juez de Garantías, y que podrá ser designado como agente una "persona" o un agente de la policía. Nuevamente, esta regulación exime de responsabilidad penal al agente que incurra en la comisión de un delito en el marco del desarrollo de la actividad encomendada.

Ya a nivel internacional, Alemania tampoco cuenta con una regulación específica del agente encubierto digital. Sin embargo, en el artículo 110 a del Código Procesal Penal alemán (Strafprozeßordnung –StPO– § 110a) se encuentra regulado al agente clásico, delimitando también los delitos para los cuales puede utilizarse la figura, tales como tráfico ilegal de drogas o armas o la falsificación de moneda. Sin perjuicio de ello, también dejan abierta la posibilidad de utilizarlo para la investigación de delitos graves cuando otros medios de investigación no sean útiles para lograr el éxito de la investigación.

---

perjuicio de adoptarse, en su caso, las medidas de protección necesarias.
El agente encubierto que como consecuencia necesaria del desarrollo de la actuación encomendada, se hubiese visto compelido a incurrir en un delito, siempre que este no implique poner en peligro cierto la vida o la integridad física de una persona o la imposición de un grave sufrimiento físico o moral a otro; al momento de resolver sobre su situación procesal, el magistrado interviniente deberá analizar si el agente encubierto ha actuado o no, conforme al Artículo 34 inc. 4) del Código Penal argentino, en virtud de las instrucciones recibidas al momento de su designación; y decidirá en consecuencia.
Cuando el agente encubierto hubiese resultado imputado en un proceso, hará saber confidencialmente su carácter al magistrado interviniente, quien en forma reservada recabará la pertinente información a la autoridad que corresponda.
Si el caso correspondiere a previsiones del primer párrafo de este Artículo, el juez resolverá sin develar la verdadera identidad del imputado.
Ningún agente de las fuerzas de seguridad podrá ser obligado a actuar como agente encubierto. La negativa a hacerlo no será tenida como antecedente desfavorable para ningún efecto.
Cuando peligre la seguridad de la persona que haya actuado como agente encubierto por haberse develado su verdadera identidad, sin perjuicio de las medidas protectivas que para este, y/o su familia, y/o bienes deberán disponerse, tendrá derecho a seguir percibiendo su remuneración bajos las formas que el magistrado interviniente séale tendientes a la protección de la gente. Si se tratare de un particular, percibirá una retribución similar a la de un agente público, conforme al criterio anteriormente expuesto.

A diferencia de lo expuesto hasta el momento, la Ley de Enjuiciamiento Criminal Española sí prevé expresamente la figura del agente encubierto digital –o informático como ellos lo llaman– en su artículo 282 bis, inc. 6, segundo párrafo de la L.E.C.[7] Cierto es que en todo el articulado prevé las condiciones específicas en las que podrá disponerse la utilización de la medida de agente encubierto clásica, la investigación de delincuencia organizada, llevada a cabo por funcionarios de la Policía Judicial, por un plazo de seis meses prorrogable por el mismo término, para la investigación de delitos específicamente determinados (inc. 3), eximiendo también de responsabilidad penal a los agentes que incurran en delitos como consecuencia necesaria del desarrollo de la investigación (inc. 5)–; haciendo referencia únicamente en un párrafo al agente encubierto informático, refiriendo que podrá, con autorización previa, intercambiar o enviar archivos ilícitos, mismo párrafo donde se establece que podrá ser utilizado para actuar en canales cerrados de comunicación.

En Estados Unidos, por su parte, la jurisprudencia hace referencia al llamado *entrapment* ("delito inducido por la autoridad"). En general, la Corte Suprema norteamericana ha convalidado la prueba obtenida a través del *entrapment* para fundar una sentencia condenatoria, siempre y cuando el autor tuviera, previo a esa intervención policial, la predisposición de cometer el delito.[8]

[7] Art. 282 bis de la LEC Española. Ley 41/2015 del 5 de octubre de 2015 que modificó la LEC, publicada en el BOE nro. 239 el 6 de octubre de 2015.

[8] Cfr. Hendler, E. Gullco, H. La utilización de agentes encubiertos en la jurisprudencia de la Corte Suprema de los Estados Unidos, J.A. 1995-1-págs. 713 y ss. (secc. Doctrina).

IX. b. Jurisprudencia argentina

IX.b.1. Fuero de la Ciudad Autónoma de Buenos Aires

Juzgad*o de Primera Instancia en lo Penal, Contravencional y de Faltas N° 18, Caso 13.247-00/17, "Gigatribe Karatekick s/art. 128, párr. 1º CP", 10 de abril de 2018*

En el marco de una investigación por distribución de material de abuso sexual infantil mediante la utilización de una plataforma informática virtual que encriptaba el contenido de los mensajes de extremo a extremo, lo que dificultaba que se pudieran interceptar estos a los fines probatorios, la señora fiscal interviniente solicitó se autorice la utilización de un agente encubierto.

Previo a resolver la medida solicitada por la Sra. Fiscal, el Juez señaló que *la figura del agente encubierto se encuentra prevista por la ley 27.319, la cual en su artículo 2º inc. d), explica la procedencia de las técnicas especiales de investigación para el tipo penal descripto en el artículo 128 del C.P., habilitando a tal efecto la implementación del agente encubierto en el artículo 3 y 4 de la misma.*

Continuó explicando que conforme el texto del art. 3º de aquella ley *será considerado agente encubierto a todo funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultado su identidad, se infiltra o introduce en las organizaciones criminales o asociaciones delictivas, con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación con autorización judicial.*

Asimismo, indicó que la aplicación de esta ley debe ser excepcional y regirse por los principios de necesidad, razonabilidad y proporcionalidad en virtud de la garantía de la no autoincriminación.

En este sentido, cabe destacar que el objeto de la ley de mención, en su artículo 1º, establece que su finalidad es la de [...] brindar a las fuerzas policiales y de seguridad, al Ministerio Público Fiscal y al Poder Judicial, las herramientas y facultades necesarias para ser aplicadas a la investigación, prevención y lucha de los delitos complejos [...]. Es decir, que el avance de las tecnologías utilizadas para la comisión de hechos

delictivos, se ha vuelto de una complejidad tal, que el propio Congreso de la Nación, se vio ante la necesidad de regular las posibles vulneraciones a Garantías Constitucionales de las que goza todo Ciudadano que fuera objeto de investigación a la luz de un Proceso Judicial Penal.

Así, entendió que la solicitud de la Fiscalía resultaba procedente pues *la investigación de este tipo de casos es sumamente compleja y requiere de estas herramientas para lograr la eficiencia que se necesita para corroborar la hipótesis Fiscal y resguardar el derecho de los menores* y, consecuentemente, autorizó la utilización de un agente encubierto.

IX .c. Jurisprudencia internacional

IX. c. 1. España

Tribu*nal Supremo, Sala de lo Penal, Caso 3448/2020, 20 de octubre de 2020*

Se interpuso recurso de casación contra la sentencia dictada por la Sala de Apelación de la Audiencia Nacional. En primera instancia se había condenado a los imputados por el delito de colaboración activa con la organización terrorista Daesh. En la investigación se utilizó un agente encubierto informático. Los imputados le remitieron a éste material relativo al Daesh e intercambiaron conversaciones.

Uno de los argumentos utilizados por los acusados en el recurso de casación fue que el agente encubierto habría provocado el delito. Respecto a esto en la sentencia se dijo que el uso del agente encubierto informático no debía provocar un indeseable efecto de provocación de delito. En este sentido, "el delito provocado aparece cuando la voluntad de delinquir surge en el sujeto, no por su propia y libre decisión, sino como consecuencia de la actividad de otra persona, generalmente un agente o un colaborador de los Cuerpos o Fuerzas de Seguridad, que, guiado por la intención de detener a los sospechosos o de facilitar su detención, provoca a través de su actuación engañosa la ejecución de una conducta delictiva que no había sido planeada ni decidida por aquel, y que de otra forma no hubiera realizado, adoptando al tiempo las medidas de precaución necesarias para evitar la efectiva lesión o puesta en peligro del bien jurídico protegido. Tal forma de proceder lesiona los principios inspiradores del Estado Democrático y de

Derecho, afecta negativamente a la dignidad de la persona y al libre desarrollo de su personalidad, fundamento del orden político y de la paz social según el artículo 10 de la Constitución, y desconoce el principio de legalidad y la interdicción de la arbitrariedad de los Poderes Públicos, contenidos en el artículo 9.3 de la misma, sin que resulte admisible que en un Estado de Derecho las autoridades se dediquen a provocar actuaciones delictivas (STS núm. 1344/1994, de 21 junio). La sentencia agrega que se configuraría una provocación cuando parta del agente provocador, y de tal modo que se incite a cometer un delito a quien no tenía previamente tal propósito, surgiendo así en el agente todo el 'iter criminis', desde la fase de ideación o deliberación a la de ejecución, como consecuencia de la iniciativa y comportamiento del provocador, que es por ello la verdadera causa de toda la actividad criminal, que nace viciada, pues no podrá llegar nunca a perfeccionarse, por la ya prevista "ab initio" intervención policial".

"Esta clase de delito provocado (...) debe considerarse como penalmente irrelevante, procesalmente inexistente y, por todo ello, impune".

Se agregó: "no existe delito provocado, cuando los agentes de la autoridad sospechan o conocen la existencia de una actividad delictiva y se infiltran entre quienes la llevan a cabo, en busca de información o pruebas que permitan impedir o sancionar el delito. En estas ocasiones, la decisión de delinquir ya ha surgido firmemente en el sujeto con independencia del agente provocador, que, camuflado bajo una personalidad supuesta, se limita a comprobar la actuación del delincuente e incluso a realizar algunas actividades de colaboración con el mismo, en la actualidad reguladas (...)".

"La intervención policial puede producirse en cualquier fase del *iter criminis*, en el momento en que el delito ya se ha cometido o se está cometiendo, especialmente en delitos de tracto sucesivo como los de tráfico de drogas, y aun en sus fases iniciales de elaboración o preparación, siendo lícita mientras permita la evolución libre de la voluntad del sujeto y no suponga una inducción a cometer el delito que de alguna forma la condicione. En estos casos, la actuación policial no supone una auténtica provocación, pues la decisión del sujeto activo siempre es libre y anterior a la intervención puntual del agente encubierto (...)".

La sentencia rechazó el argumento diciendo: "si aplicamos esta doctrina al caso concreto aquí enjuiciado, constatamos que cuando interviene el agente encubierto informático ya se ha constatado la radicalización y el peligro que resultaba de su actividad, ya se habían

detectado intercambio de mensajes, la transmisión de informaciones de corte radical y violento, por lo que se dispone su utilización como medio de investigación de una realidad delictiva preexistente y cuyo contenido documentado en las conversaciones y comunicaciones que se mantienen, que aparecen documentadas en el hecho probado la sentencia y la fundamentación, reflejan la expresión de una voluntad de mantenerse en ese adoctrinamiento e indagar las posibilidades de realizar un hecho delictivo, hablando de fechas, de la necesidad de conducir en línea recta en calles de gran aglomeración y la conveniencia de centrar en Madrid los ataques".

Tribu*nal Supremo, Sala de lo Penal, Caso 750/2019, 13 de marzo de 2019*

Los acusados habían sido condenados por los delitos de captación y adoctrinamiento terrorista para lo cual actuaban a través de redes sociales como Facebook para los primeros contactos y luego continuaban a través de la plataforma de WhatsApp. Durante la investigación actuó un agente encubierto informático.

Entre los motivos de agravio esgrimidos por los acusados en los recursos de casación interpuestos, se planteó la nulidad de las actuaciones en relación con la actuación del agente encubierto virtual por afectación al principio de legalidad y de irretroactividad, toda vez que a la fecha en que se autorizó su actuación no existía habilitación legal.

En efecto, teniendo en cuenta que al momento de la investigación de los hechos la normativa procesal española solo preveía la figura del agente encubierto tradicional, la cuestión planteada por la defensa y a resolver por el Tribunal fue si aquella normativa existente amparaba la actuación de un agente policial encubierto para actuar en las redes sociales, o si la ausencia de una previsión legal concreta lo impedía.

Reproduciendo los argumentos de la instancia anterior, el Tribunal señaló: "...la figura del agente encubierto, aparece regulada en el art. 282 bis de la Ley de Enjuiciamiento Criminal, precepto que se introduce *ex novo* en nuestro ordenamiento jurídico a través de la Ley Orgánica 5/1999, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, con la nueva redacción del precepto por la LO 185/2010, de 22 de junio, que introdujo al nº4, y la modificación operada a raíz de la LO 13/2015, a través de la introducción de los nuevos apartados seis y siete".

"La incorporación de este medio de investigación no significa que no se hubiera utilizado nunca anteriormente, con plena garantía de legalidad. No siempre las leyes colman vacíos sino que vienen a sancionar, regulándolas adecuadamente, técnicas de investigación que ya contaban con un genérico soporte normativo, pero que es conveniente que tengan una adecuada regulación legal".

Indicó que el concepto de agente encubierto es un concepto legal previsto en el art. 282 bis LECrim y que "en nuestro ordenamiento será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operando, así como obtener pruebas sobre la ejecución de hechos delictivos".

Continuó describiendo los aspectos centrales de la figura del agente encubierto. Así, en lo que respecta al posible ámbito de actuación, el apartado 1 del art. 282 bis LECrim requiere que lo sea en el marco de investigaciones de actividades propias de la delincuencia organizada y que en el apartado 4 se establece qué se entiende por delincuencia organizada. Señaló que: "segundo aspecto a tener en cuenta, es la necesidad de que medie una autorización judicial. Ello se debe a que nos encontramos de nuevo ante una figura que, a través de su actuación, puede afectar a derechos fundamentales, tales como el derecho a la intimidad, a la inviolabilidad del domicilio o al secreto de las comunicaciones. La limitación de estos derechos fundamentales, llevada a cabo por la autoridad pública, debe obedecer a un fin legítimo, ser proporcional y estar amparada legalmente, lo cual es previsto por el legislador a través de esta exigencia de autorización judicial previa, autorización que debe estar motivada y ser precisa (...)". Y, finalmente, la otra característica de esta figura "es el deber de información exigido al agente encubierto, el cual deberá poner la información que vaya descubriendo a disposición de quien autorizó la investigación, a la mayor brevedad posible" siendo la jurisdicción competente quien establezca los plazos y forma en que deberá realizar esa comunicación.

Prosiguió explicando que la "reforma de LO 13/2015 ha introducido los apartados 6 y 7 del art. 282 de la LECrim. El apartado 6 introduce la novedosa figura del agente encubierto informático, tratando el legisla-

dor, una vez más, de adaptar el texto legal a la sociedad digitalizada en la que nos encontramos inmersos".

En consecuencia, el Tribunal, con cita a una sentencia del Tribunal Constitucional español en la que también se discutía la ausencia de normativa específica pero en relación con la imposición de medidas cautelares, entendió: "...la insuficiente adecuación del ordenamiento a los requerimientos de certeza cera para los hipotéticos destinatarios de las medidas un peligro en el que reside dicha vulneración, no implica por sí misma necesariamente la ilegitimidad constitucional de la actuación de los órganos jurisdiccionales, siempre que estos hubieran actuado en el caso concreto respetando las exigencias dimanantes del principio de proporcionalidad..." y que en el presente caso el agente encubierto informático actuó no solo con autorización del Fiscal y del Juez, sino además dando cumplimiento a las exigencias que le fueron impuestas para llevar adelante su cometido (enunciación de las redes en las que debía actuar, duración de la medida –6 meses–, deber de informar mensualmente toda actividad web del perfil, necesidad de requerir autorización judicial expresa para diligencia que impliquen la limitación de un derecho fundamental como ser intervención de comunicaciones orales o del correo postal, etc.).

Se rechazó el submotivo de agravio.

Tribu*nal Supremo, Sala de lo Penal, Caso 345/2019, 7 de febrero de 2019*

En el transcurso de chequeos en redes sociales, agentes policiales identificaron un perfil que exhibía una bandera de una organización terrorista en la parte de su perfil que era de acceso público. De esa forma una vez que el agente informático ganó la confianza del acusado, pudo acceder al material que este último distribuía.

A fin de profundizar la investigación se solicitó autorización judicial para la actuación de un agente encubierto informático a quien el acusado invitó y admitió entre su grupo de amigos en las redes sociales.

Se determinó que el acusado a través de distintas redes sociales, entre ellas Facebook, difundía la ideología de una organización terrorista para atraer potenciales partidarios. Para ello procedió a la apertura en dichas redes sociales a cuentas bajo el nombre de "Baltasar" y acudía a un foro de acceso cerrado donde le era suministrado el material que luego distribuía por la red.

El acusado fue detenido tiempo después, momento en el que se procedió al secuestro de diversos dispositivos electrónicos con material relevante para la investigación.

Se lo condenó por el delito de colaboración en organización terrorista y fue absuelto por los delitos de integración en organización terrorista, autoadoctrinamiento y enaltecimiento y justificación del terrorismo.

La defensa impugnó la sentencia condenatoria.

Entre las distintas cuestiones puestas a consideración, en el fallo se analizó la validez de la figura del agente encubierto virtual en las investigaciones penales, su diferencia con el agente provocador y el alcance del requisito de organización criminal exigida por la norma procesal.

La defensa alegó que en este caso el agente encubierto informático había sobrepasado su misión investigadora para convertirse en un agente provocador. Al respecto, el Tribunal Superior indicó que la diferencia con el agente provocador radicaba en que la intervención del agente encubierto no provoca el delito, sino que el delito ya se ha cometido o se está cometiendo y la actuación del agente se limita a conseguir pruebas acerca de la comisión del delito.

Asimismo, señaló que en el caso concreto no fue el agente encubierto quien tomó la iniciativa enviando una solicitud de amistad al acusado, sino que fue este último quien lo hizo invitándolo a conocer y compartir no solo sus ideas sobre la organización violenta sino también su actividad distribuidora para captar partidarios a su causa.

Destacó también el Tribunal Superior que en el caso del agente encubierto, a diferencia de los supuestos en los que el agente actúa como provocador, el dolo en el autor ya existía antes de la designación del agente encubierto.

En definitiva, y sobre la base de las distinciones efectuadas por la doctrina, indicó las siguientes diferencias entre el agente encubierto y el agente provocador:

- El agente provocador no se infiltra en la organización criminal, sino que tiene un contacto limitado con esta o con algún delincuente;
- El agente provocador no utiliza una identidad ficticia, sino que se limita a ocultar su condición de agente de policía, engañando así a los delincuentes;
- Al ser el engaño menor y la relación con los delincuentes más corta, el riesgo de la vulneración de derechos fundamentales es mucho menor en la actuación del agente provocador que en la del agente encubierto; y

- La finalidad de la actuación del agente provocador es detener al delincuente en el instante, impidiendo el agotamiento del delito, mientras que el agente encubierto recaba información, ya que por encima de la incautación de efectos del delito o detenciones concretas está la desarticulación de una organización criminal.

Finalizó afirmando: "(e)l Tribunal declara válida la intervención del agente encubierto, que tenía cobertura judicial, y en este caso tiene una mera participación investigadora y no incitadora a la comisión del delito, y cuya necesidad se convierte en absoluta al proceder el ilícito en un torno privado informático al que solo se accede en un círculo reducido, que en este caso lo es en virtud de acciones de acceso a propaganda terrorista y en un segundo plano su distribución, para lo que se exige un acceso privado al círculo propio e interno del autor del delito".

Cuestionó la defensa que en el caso se hubiera verificado el requisito de organización criminal para la habilitación de la actuación del agente encubierto, toda vez que se trató de la actuación individual del acusado. Al respecto, el Tribunal Superior expresó que en el escenario del organigrama de una organización terrorista, "...el reparto de funciones es amplio y ocupa, también, a quienes desempeñan su "campo de batalla" en la actuación online para promover el terrorismo. Y ello se integra en el término de la propia organización criminal, lo que permite atraer el uso del art. 282 bis LECRIM para la participación del agente encubierto en las investigaciones, dada la ocultación de los autores tras equipos informáticos, lo que lleva a un punto de la investigación que la dificulta...".

En definitiva, el Tribunal Superior sostuvo que, al contrario de lo manifestado por la defensa, no se trató de una actuación individual en la comisión de los delitos, sino que dicha actuación debía enmarcarse en una estructura colectiva propia de la organización terrorista, en el que cada una actúa su rol y realiza su aporte.

En virtud de esas consideraciones el Tribunal Superior desestimó los motivos invocados por la defensa y no hizo lugar al recurso de casación interpuesto.

Tribu*nal Supremo, Sala de lo Penal, Caso 4038/2018, 26 de noviembre de 2018*

Se interpuso recurso de casación contra la sentencia dictada por la Sección de Apelación de la Sala Civil y Penal del Tribunal Superior de Justicia de Cataluña. En la investigación se había utilizado un agente en-

cubierto que se hizo pasar por agente corrupto de aduanas para recibir información de quiénes traerían cargamentos con cocaína a Barcelona. Algunos de los intercambios ocurridos entre este y los sospechosos se realizaron mediante la carpeta borradores de un correo electrónico.

La defensa se agravió de la falta de autorización judicial específica al agente encubierto para que accediera al correo electrónico (carpeta borradores) que utilizaban para comunicarse con los acusados. En la sentencia se dijo: *el derecho a la intimidad en ningún caso ha sido vulnerado, pues la cuenta a la que se accede por el agente encubierto con la debida autorización es una cuenta creada para la ocasión, pero lo que más importa es que son los propios investigados los que le dan al agente encubierto la dirección y las claves de esa cuenta para acceder y comunicarse, es en ella donde se recibirán los avisos, es donde se depositará (bandeja borrador) las documentaciones de los posibles viajeros para ver si estaban "limpios" es decir sin antecedentes, y por ello podrían ser "correos" idóneos, y es de esta bandeja borrador de donde se extraen los pantallazos (...).*

En definitiva, rechazamos las denuncias relativas a que se viola el secreto de las comunicaciones, pues no se trata de comunicaciones en el sentido traslativo, sino que la bandeja borrador de la cuenta era el lugar donde se depositaba información, no eran llamadas telefónicas, que sí hubieran requerido autorización judicial, ni tampoco eran intervenciones informáticas especializadas para adentrarse en espacio de comunicación privados excluyentes de otras personas sin su conocimiento, o entrar en las redes sociales lo que también requeriría autorización judicial. Aquí ellos (los investigados) le dieron la cuenta y las claves de acceso, haciéndole usuario de la misma, sin que hubiera expectativa alguna de privacidad (...).

Por ello, *no hay injerencia alguna en el secreto de las comunicaciones, sino libre disposición de las mismas por el ahora recurrente cuando cuestiona un acceso al que se le facilita libre entrada, por lo que no hay la pretendida vulneración de un derecho sobre el que la parte provoca y efectúa una libre cesión del sistema de acceso a la información mediante la cual el fin era la comisión de un hecho delictivo, y el agente ya estaba investido de la autoridad que le otorgaba su condición de agente encubierto, sin que, por ello, este haya llevado a cabo ninguna injerencia, sino compartir acceso a una información con el propio autor del delito.*

Con respecto a la necesidad de la articulación de la vía del agente encubierto informático del art. 282 bis.6 LECRIM debe descartarse la

necesidad de poner en marcha el mecanismo autorizante de esta vía, porque (...) el hecho de que esa forma de comunicación se instaurara por los investigados desde el principio de sus reuniones con el agente encubierto en nada incide en la corrección de la autorización, ni hacía necesario dar inmediata cuenta de ello al Ministerio Fiscal autorizante, porque no afectaba a derechos fundamentales y no precisaba, pues, de confirmación judicial.

Agregó respecto del agente encubierto informático: *(...) su función esencial prevista es la de actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación. Y es aquí donde, con claridad, se desvela la innecesariedad del agente infiltrado informático que, a juicio del apelante, se ofrece indispensable en estos autos: no asistimos a una incorporación del agente encubierto a una red cerrada de comunicación entre usuarios; antes al contrario, el agente es invitado por los titulares de la cuenta de mail a participar en ella, intercambiándose mutuamente información y facilitando, para ello, la contraseña que, con el consentimiento, por tanto, de los investigados, le permite acceder al mail. Por tanto, asistimos a un interlocutor (los investigados) que de forma activa y voluntaria han consentido la introducción en su canal de comunicación de un tercero (el agente encubierto) que, por tanto, participa con normalidad en el intercambio de información.*

Tampoco las facultades reconocidas por el artículo al agente encubierto informático tienen encaje en la actuación que llevó a cabo el agente encubierto: el legislador prevé que pueda intercambiar o enviar archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de esos archivos. Y nada de eso hizo el agente de autos. En definitiva, ninguna razón justificaba la incorporación a la investigación de un agente encubierto informático. Se desestimó este submotivo de recurso.

Tribu*nal Supremo, Sala de lo Penal, caso 1385/2018, 11 de abril de 2018*

En el marco de la cooperación internacional en la lucha contra la prostitución y corrupción de menores, la Policía de Nueva Zelanda había puesto en funcionamiento un foro denominado "Pedoleaks", encubierto y controlado por ella misma. Durante las tareas de control, detectó a un usuario que afirmaba producir su propio material y mantener encuentros sexuales con su hija menor de edad. La Policía de aquel país,

ante la urgencia y el riesgo que la situación implicaba para la menor, localizó la IP determinando que la conexión provenía de España y procedió a informar a través de Europol a la Policía Judicial Española de la situación quien solicitó orden judicial para identificar al titular de la conexión y proceder al registro del domicilio.

Concluida la investigación, el acusado fue juzgado por haber realizado actos de contenido sexual con sus dos hijas gemelas de cuatro años en el domicilio familiar y haber tomado fotografías de esas prácticas sexuales, como también de otras fotografías resaltando el carácter infantil de las víctimas, que distribuía en un servidor de internet denominado PEDOLEAKS dentro de la red TOR. El servidor estaba reservado a un reducido círculo de pedófilos y era de muy difícil acceso, donde los participantes no buscaban un lucro económico sino el intercambio de material "de alta calidad" entre ellos.

El acusado fue condenado por dos delitos continuados de abuso y agresiones sexuales a menores de trece años cometido en las personas de sus dos hijas y distribución de pornografía infantil.

Tanto la acusación particular como el acusado interpusieron recursos de casación contra la sentencia

Uno de los motivos esgrimidos por la defensa radicó en cuestionar el origen de la investigación y la afectación al derecho de las comunicaciones, toda vez que la policía de Nueva Zelanda *se habría inmiscuido en unas comunicaciones realizadas a través de la red sin contar con la preceptiva autorización judicial.*

En su decisión, el Tribunal Superior señaló en primer lugar, que en el caso no era posible afirmar la existencia de una intromisión en las comunicaciones entre terceros pues uno de los comunicantes había sido el propio agente policial que se encontraba suplantando o simulando ser otro usuario que se había auto atribuido una identidad en la red.

En cuanto al requisito de la autorización judicial, afirmó que no era una exigencia necesariamente constitucional, sino más bien legal y que solo era exigida en determinados supuestos. Entre las razones que fundan esa exigencia mencionó las posibles injerencias en derechos fundamentales amparadas en un engaño o simulación. Sin embargo, en este aspecto realizó una distinción cuando en el engaño o simulación intervenía un agente encubierto tradicional o un agente encubierto informático.

Así explicó: *en el mundo de la red el empleo de una identidad supuesta es la regla: todos se asoman a ese mundo usando un* nick. *En*

este punto, el ciber agente encubierto se aparta del agente encubierto convencional en un dato: la asignación de identidad supuesta es una de las vertientes que impulsa a la conveniencia de una autorización. En la red no se produce engaño por la utilización de pseudónimo. Todos lo utilizan: es una regla de ese espacio de comunicación.

Y concluyó: *El derecho comparado muestra modalidades muy diversas de regulación. Doctrinalmente, se diferencia entre lo que se conoce como ciber patrulleo (el agente realiza exploraciones o indagaciones por canales abiertos de comunicación) y el estricto agente encubierto online que opera en canales cerrados. Solo en este segundo caso la legislación reformada en 2015 requiere autorización judicial, lo que no inexorablemente habría de proyectarse a casos como el ahora examinado en que no estamos ante una inflitración policial en la red, sino ante el uso por la policía del canal creado por quien ha sido detenido, valiéndose de su* nickname.

En consecuencia, el Tribunal Superior desestimó este motivo de agravio.

Juzga*do de lo Penal, Caso SJP 39/2016, 06 de julio de 2016*

En este caso, el Ministerio Fiscal acusó a tres hombres de formar parte del grupo "Anonymous" con el objeto de cometer de forma concertada uno o varios delitos y, en ocasión de la celebración de elección locales en España con la finalidad de entorpecer el proceso electoral, de haberse puesto de acuerdo y dirigido, organizado y ejecutado ataques de Denegación de Servicio Distribuido (DDoS) a diversas páginas web que hubieran afectado de forma importante el normal funcionamiento del correo electrónico obstaculizando los trámites previos al proceso electoral y ocasionado el bloqueo de la página web de la Junta electoral central y contra las páginas web de determinados partidos políticos.

Las defensas de los imputados solicitaron su absolución alegando cuestiones relativas a la vulneración de derechos fundamentales y a la irregularidad de las pruebas practicadas. Entre ellas, cuestionaron la intervención de un agente que, actuando bajo un pseudónimo se ganó la confianza de alguno de los acusados. Asimismo, adujeron en relación con la prueba documental relativa a las conversaciones mantenidas, que se trató de un supuesto de delito provocado o, en su caso, que el agente encubierto había actuado sin autorización judicial.

En cuanto a si la actuación del agente configuraba un supuesto de agente encubierto o agente provocador, la Magistrada con referencia a

diversos precedentes del Tribunal Superior, señaló la diferencia entre ambas herramientas de investigación:

- En el delito provocado hay una actuación engañosa del agente policial que supone una apariencia de delito, ya que desde el inicio existe un control absoluto por parte de la policía.
- El delito provocado se integra por tres elementos, a saber: a) un elemento subjetivo constituido por una incitación engañosa a delinquir por parte del agente a quien no está decidido a hacerlo; b) un elemento objetivo teleológico consistente en la detención del sujeto provocado que comete el delito inducido y c) un elemento material consistente en la inexistencia de riesgo alguno para el bien jurídico protegido y, como consecuencia, de la atipicidad de la acción.
- En cambio, no es posible hablar de delito provocado cuando los agentes sospechan o conocen la existencia de una actividad delictiva y se infiltran entre quienes la llevan a cabo para verificar la comprobación del delito y ponerle fin. Es decir, que en estos casos no se provoca nada que no estuviera ya en la ideación del sujeto activo, sino que se trata de comprobarlo.

Sostuvo que si bien en teoría la diferenciación entre ambos supuestos era clara, en la práctica podían darse situaciones ambiguas que deberían resolverse atendiendo a las particularidades de cada caso concreto.

Por otra parte, también señaló que conforme sentencia del 6/11/13 del Tribunal Superior "al referir que las actividades criminales por su complejidad tiene ritmos y tiempo que pueden dilatarse en el tiempo y que demandan un seguimiento previo al objeto de contrastar los datos y evitar actuaciones precipitadas. Y que el acercamiento, contacto y diálogo para ganar confianza no son gestiones que necesiten autorización judicial" ni que en principio vulneren garantías constitucionales.

En efecto, sostuvo que en lo que respecta a actuaciones dirigidas a la vigilancia, prevención y evitación de ilícitos en redes informáticas donde la evidencia se encuentra en fuentes abiertas en la web o en canales no cerrados de comunicación, se venía sosteniendo que la actuación de un agente policial haciéndose pasar por un usuario más en la red, en principio no requería autorización judicial.

Concluyó, que en el presente caso entonces *no puede considerarse que los hechos objeto de enjuiciamiento se hubieran desarrollado a consecuencia de la iniciativa o sugerencia del agente cuestionado, ni que su actuación hubiera requerido anteriormente de autorización judicial,*

al tratarse de actuaciones encaminadas a efectuar averiguaciones y a abortar actividad delictiva, habiendo intervenido en todo caso en zonas públicas en las redes sociales, chats públicos en los que todos participan con identidades supuestas, pudiendo por ello participar los agentes en los chats públicos y no necesitando autorización para intervenir y controlar zonas públicas de internet sino en su caso para comunicaciones privadas.

Fue así como, una vez confirmadas las sospechas de los agentes y ante la inminencia de los ataques informáticos, solicitaron las correspondientes autorizaciones judiciales.

En consecuencia, la Magistrada desestimó el planteo efectuado por las defensas en este sentido. Sin embargo, todos los acusados fueron absueltos por la titular del Juzgado de lo Penal a cargo del proceso por considerar que no existían elementos probatorios que acreditaran la participación de los acusados en los hechos investigados.

Tribu*nal Supremo, Sala de lo Penal, Caso 767/2007, 03 de octubre de 2007*

Un agente de la Guardia Civil, mientras mantenía una conversación en el canal IRC (Internet Relay Chat), tomó conocimiento de manera casual de que una persona había remitido a otro usuario de ese canal material de abuso sexual infantil. El agente, mediante la utilización de un apodo ("nick"), entabló conversaciones con aquella persona quien le envió material con imágenes y videos de abuso sexual infantil y le comentó acerca de la existencia de un foro en el que un grupo de personas mayores de edad fijaban encuentros con la participación de sus hijos menores para mantener con ellos relaciones sexuales.

Frente a la posible comisión de un delito, se inició la investigación policial y el agente en cuestión fue autorizado a actuar como agente encubierto por el Fiscal y el Juzgado.

El hombre fue condenado por el delito de corrupción de menores consistente en la distribución y facilitación de material pornográfico para cuya producción se utilizaron menores de edad.

Tanto el Ministerio Fiscal como el acusado interpusieron recursos de casación contra la sentencia.

En lo que aquí respecta, el acusado impugnó la sentencia alegando que la intervención del agente encubierto no cumplió con los requisitos exigidos por el art. 282 bis de la L.E.Cr. sobre la base de los siguientes motivos:

- que el agente actuó sin autorización judicial,
- que tampoco procedía su designación como agente encubierto

por no tratarse de un caso de delincuencia organizada, y
- que se tuvo por válida una prueba obtenida irregularmente atento a que se trató de un delito provocado por la actuación del agente.

La importancia de este antecedente jurisprudencial radica en que en este caso la actuación del agente policial fue analizada bajo los parámetros de la figura del agente encubierto tradicional, pues cabe recordar que el agente encubierto informático fue introducida en la L.E.Crim. con la reforma por la Ley Orgánica 13/2015 del 5 de octubre de ese año.

En cuanto a la esgrimida ausencia de autorización judicial con la que habría actuado el agente de la guardia civil, el Tribunal Superior sostuvo: *...los agentes de la autoridad, cuando realizan las labores habituales de vigilancia para prevenir la delincuencia informática tuvieron noticia casual de la existencia de un posible delito de difusión de pornografía infantil. Realizaron las investigaciones oportunas y, solo cuando tuvieron la convicción de estar efectivamente en presencia de hechos presuntamente delictivos, confeccionaron el oportuno atestado que remitieron a la Fiscalía de la Audiencia Provincial donde se instruyeron las pertinentes diligencias informativas...* y el Fiscal procedió a la designación del agente de la guardia civil como agente encubierto, lo que fue ratificado por la autoridad judicial.

Es decir, el Tribunal Superior consideró a la actuación inicial del agente, en este caso, como una práctica propia de los agentes policiales para hacer su labor de investigación.

Por otra parte, la defensa esgrimió que no se estaba ante un caso de delincuencia organizada y que, en consecuencia, resultaba improcedente la utilización del agente encubierto como herramienta procesal para la investigación, por ausencia de uno de los requisitos exigidos por la normativa procesal.

El Tribunal Supremo luego de señalar que el acusado había remitido archivos informáticos con material de abuso sexual infantil y comentado la existencia de un foro en el que un grupo organizado de personas mayores de edad fijaban encuentros con la participación de sus hijos menores para mantener relaciones sexuales con estos, señaló: *la difusión e intercambio de pornografía supone la confección previa del material pornográfico, circunstancia que sugiere la intervención de otras personas.*

Finalmente, también se descartó que el agente encubierto haya actuado como agente provocador pues para afirmar su existencia se exige que la provocación provenga de parte del propio agente, de forma

tal que de ella se incite a otra persona a cometer el delito. Supuesto que, afirmó, no ocurrió en este caso donde fue el propio acusado quien había cometido el delito de forma libre y espontánea respecto a otra persona (envío de material de abuso infantil), circunstancia que llegó a conocimiento del agente policial, y ese primer delito suponía que el recurrente era poseedor de material pornográfico que facilitó a un tercero.

X. Utilización de *software* a distancia

X. a. Introducción

El denominado *software* judicial a distancia, comúnmente conocido como "allanamiento remoto" se trata de una medida de investigación en el marco de un proceso penal tendiente a registrar y, de ser necesario, secuestrar (o copiar) datos informáticos alojados en cualquier tipo de sistema informático, mediante la utilización de programas informáticos que actúan de manera subrepticia, sin necesidad de obtener o acceder físicamente al dispositivo de almacenamiento de datos que es objeto de investigación.[1]

Sin perjuicio de que se la asimila al allanamiento tradicional en el espacio físico, su dinámica dista de ser equiparable a esa medida de investigación, por lo que entendemos que sería dificultoso utilizar las reglas previstas para esta medida de prueba en las leyes procesales (art. 228 CPPN; Art. 111 CPPCABA; art. 220 CPPBA), debido a que cuenta con elementos diferenciadores que hacen imposible constitucionalmente implementar este tipo de medio de prueba sin violentar el principio *de*

[1] Salt, M. "Allanamiento remoto: ¿un cambio de paradigma en el registro y secuestro de datos informáticos?".

nulla coactio sine lege. Asimismo, cierta parte de la doctrina considera que, más que allanamiento, se trata de una medida asimilable a la intervención de comunicaciones telefónicas.

Algunos de los elementos diferenciadores del allanamiento remoto con el tradicional, y sin ser un análisis exhaustivo, consisten en que el remoto necesita del engaño del sospechoso o del titular del sistema informático por la aplicación del *software* malicioso; la movilidad de los dispositivos donde se aloja la información, que puede generar problemas de competencia y jurisdicción a la hora de disponer de esta medida ante supuestos de acceso transfronterizo de datos; lo que hace materialmente imposible asimilar al tradicional allanamiento de morada.

La medida no se encuentra específicamente regulada en el Convenio para la Ciberdelincuencia de Budapest. En el sistema argentino, las provincias de Neuquén y Tucumán poseen una disposición que podría ser asimilable a este instituto, pero que no comprende ni captan su la complejidad.

En efecto, la provincia de Neuquén, en el Código Procesal Penal reformado en 2011 se establece en el art. 153 lo siguiente:

> Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia.
>
> También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota.

En el Código Procesal Penal de la provincia de Tucumán, reformado en 2016, se introdujo en el art. 199 una disposición similar. Dichas disposiciones no regulan el marco básico de implementación, autoridad que puede ordenarla y aplicarla, duración, metodología, control, ni su carácter excepcional. Asimismo, se han presentado distintos proyectos a tal fin.[2]

El allanamiento remoto se encuentra regulado en países como Estados Unidos, Alemania, España, Italia, Holanda o el Reino Unido.

---

[2] Mensaje n° 111/16: con un apartado para la regulación de medios especiales de investigación que no fue aprobado; o la iniciativa que cuenta con media sanción en Mendoza que admite para la investigación de ciertos delitos el acceso a un dispositivo o sistema para ser registrados los datos informáticos allí contenidos, y, de ser posible, la realización previamente de una copia forense de este).

En los Estados Unidos se aplicó por analogía las normas y criterios jurisprudenciales que regulan el registro y secuestro tradicional. Incluso se realizó una modificación a la Regla Procesal 41, autorizando a un juez de una jurisdicción en la que ocurrió un delito a emitir una orden de acceso remoto a otras jurisdicciones.

En Alemania la medida se encuentra legislada enmienda de la Ley para hacer procedimientos penales más efectivos y prácticos, sancionada por el parlamento el 17 de agosto de 2017 que amplió las facultades previstas en el Código Procesal Penal de los organismos encargados de hacer cumplir la ley para realizar búsquedas en línea y vigilar las telecomunicaciones.[3]

En España se encuentra legislada la medida desde el año 2015. Con la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal, que en su artículo 588 *septies* dispone:

> 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un *software*, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos (...) siempre que persiga la investigación de los delitos individualizados en la misma norma.

X. b. Jurisprudencia internacional

X. b. 1. Alemania

Bverf*G, Judgment of the First Senate, 370/07, 27 de febrero de 2008 BvR 370/07 – – 1 BvR 595/07 (2008)*

En este caso se trató de un planteo no efectuado en el marco de un proceso penal, sino que se trató de una acción judicial impulsado por un periodista, de un miembro del partido DIE LINKE de Renania del

[3] Salt, ob. cit.

Norte-Westfalia y tres abogados contra las disposiciones de la Ley de Protección de la Constitución estadual, que autorizaba a que los servicios de inteligencia, en su rol en la lucha contra el terrorismo, a realizar acciones como monitoreo e intercepción de datos en tiempo real de comunicaciones electrónicas y el "registro remoto" de sistemas informáticos mediante programas troyanos.

Los demandantes aseguraron que esas potestades chocaban con garantías fundamentales que protegen la confidencialidad e integridad de los sistemas de tecnología de la información. Por su parte, el Estado Provincial sostuvo que la garantía que estaba en juego en ese tipo de medidas era el derecho a la privacidad de las telecomunicaciones, mientras que el Estado Federal encuadró la disputa dentro de los alcances de la garantía de inviolabilidad del domicilio.

Sin embargo, el Tribunal Constitucional consideró que estaba en juego una nueva garantía a la "confidencialidad e integridad de la información en sistemas informáticos", entendido como el "interés del usuario en garantizar que los datos que son creados, procesados y almacenados por los sistemas informáticos tengan un ámbito de protección confiable".

"El derecho general de la personalidad en la manifestación aquí tratada, en particular, proporciona protección contra el acceso secreto, mediante el cual los datos disponibles en el sistema pueden ser espiados en su totalidad o en gran parte", expresó el fallo.

X. b. 2. Estados Unidos

Para abordar la jurisprudencia en la materia en lo que resulta conveniente citar el caso paradigmático en donde se debatió si el uso *software* judicial a distancia puede afectar garantías constitucionales. Se trata de las diferentes resoluciones dictadas en el marco de los múltiples procesos nacidos por una investigación de las fuerzas federales de los Estados Unidos sobre la web "Playpen", un sitio creado en 2014 al que solo podía accederse mediante por la red "TOR" con sofisticados mecanismos de anonimización. La web, que llegó a tener más de 200 mil usuarios activos y 1500 visitas diarias hasta que el F*ederal Boreau f Investigation (FBI)* dispuso su bloqueo en marzo de 2015, fue conocida como el servicio oculto de contenido de material de abuso sexual infantil más grande a nivel global.

La génesis de la investigación fue en 2014 cuando por un supuesto error de su administrador, Seven W. Chase, la dirección IP de Playpen fue advertida por una fuerza de seguridad fuera de los Estados Unidos, que inmediatamente notificó los sucesos al FBI, que llegó a la conclusión de que el sitio web de Playpen estaba alojado en un servidor en Lenoir, Carolina del Norte, tras lo cual se logró el dictado y ejecución de una orden de registro para incautar el servidor.

Tras la ejecución de la orden y la detención de Chase, los investigadores colocaron una copia del servidor incautado en un servidor controlado por el gobierno estadounidense ubicado en Newington, Virginia. Con posterioridad a ellos, solicitaron el libramiento de una orden judicial para el uso de una 'Técnica de investigación en red' (NIT) para identificar a los usuarios de Playpen, orden concedida por el Tribunal de Distrito de EE. UU. Para el Distrito Este de Virginia el 20 de febrero de 2015.

A través del NIT, el gobierno de los Estados Unidos colocó un código en el servidor del sitio web para que cada usuario que ingrese al sitio web lo descargue y así permitir que el FBI pueda recopilar información de identificación de las computadora de cualquier usuario o administrador que inicie sesión en Playpen ingresando un nombre de usuario y contraseña. Con esa técnica, la computadora de activación, "donde sea que se encuentre", transmitió la información, incluida su dirección IP y nombre de host, a la instalación gubernamental en Virginia.

A raíz de esa investigación se abrieron distintos procedimientos contra los usuarios y administradores del sitio en los cuales se debatieron los alcances de distintas órdenes dictadas por magistrados para poder realizar el registro y secuestro de datos mediante el envío de un malware a los dispositivos de los sospechosos que ingrese de manera subrepticia a estos para así hacerse con la información.

Tribu*nal de Apelación del Noveno Distrito, Caso 17-40097-DDC, "United States of America v. Wesley Wagner", 12 de febrero de 2019*

Esta causa tuvo su origen cuando un usuario de Playpen, "soldiermike" inició sesión en el sitio web el 28 de febrero de 2015. El NIT identificó el nombre de host de la computadora del usuario y su dirección IP. Tras ello, los agentes de investigación obtuvieron una orden de allanamiento la residencia del imputado en el Estado de Kansas, donde se ejecutó una orden de registro y secuestro de datos informáticos por la que se

halló evidencia de material de abuso sexual de menores en una computadora portátil. El Sr. Wagner fue posteriormente acusado de tenencia y distribución de material de abuso sexual de menores.

La defensa de Wagner buscó que se excluya la identificación del NIT de su dirección IP, la evidencia secuestrada en su casa y sus declaraciones a los agentes. El fundamento contra la acusación fue que la génesis de la investigación se obtuvo a través de una conducta que afectó el debido proceso y fue dictada por un juez que no tenía jurisdicción. Sin embargo, el tribunal de distrito negó sus mociones y tras un debate de tres días, un jurado lo condenó por ambos cargos. El Tribunal del Noveno Circuito rechazó todos los planteos, al considerar que no se estaba ante un supuesto en el que procediera la regla de exclusión.

El Cuerpo contempló aplicable la doctrina de la Corte Suprema de Justicia de los Estados Unidos en el caso "United States v. Leon" según la cual cuando las fuerzas confían de "buena fe objetiva" en una orden judicial, aunque haya sido invalidada posteriormente, no existía un proceder ilegítimo. Por lo tanto las pruebas son admisibles.

El fallo apuntó que, aun cuando se considerase que la orden de la jueza de Virginia excedía su jurisdicción porque autorizó la búsqueda de computadoras ubicadas fuera del Distrito Este de Virginia, los agentes ejecutores se basaron en la orden de buena fe porque tenían conocimiento de que el NIT se instalaría en servidores en el Distrito Este de Virginia, donde se encontraba la magistrada que dictó la orden

Juzga*do de Distrito del Oeste de Washington, Caso 3: 15-cr-05351-RJB, United States of America v. Jay Michaud, 26 de enero de 2016*

En este precedente, la defensa del imputado cuestionó que existió una violación a la cuarta enmienda, que protege a los individuos ante registros irrazonables, alegando también que el registro sobre el domicilio del imputado violó la denominada Regla 41 anteriormente descrita.

En un primer momento, el juez Robert Bryan rechazó la defensa apuntando que la orden que se dictó debido a los datos obtenidos por el NIT fue respaldada por una "causa probable" y describió particularmente los lugares que se registrarán y las cosas que se incautarán. "Aunque la orden de NIT violó la Regla 41 (b), la infracción fue de naturaleza técnica y no justifica la supresión", aseguró el juez.

Sin embargo, las defensas exigieron tomar conocimiento del código fuente del *spyware* utilizado. En ese contexto, el FBI les brindó el

módulo de "carga", pero no el "lanzador", lo que fue rechazado por la defensa, que pidió los códigos de ambas.

La defensa de Michaud buscaba, mediante el conocimiento de los códigos, determinar de forma independiente el alcance total de la evidencia obtenida de los dispositivos del imputado cuando implementó el NIT... si las declaraciones del gobierno sobre cómo funciona el NIT, pero el gobierno federal se negó a otorgar la información. De esa forma, el defensor de Michaud pidió que se excluya esa evidencia por existir una colisión con la garantía de defensa en juicio.

De tal modo, el juez de Circuito de Washington Bryant excluyó parte de la evidencia, tras lo cual, el FBI pidió que se desestime el caso.

Tribu*nal de Apelaciones del Noveno Circuito, Caso 17-30117 D. C. N° 3:16-cr-05110-RB-1, United States v. Tippens, 17 de mayo de 2019*

Poco después del caso "Michaud" en otro de los incidentes surgidos de la investigación "Playpen", iniciado por la defensa de David Tippens, el juez Bryant revisó su decisión y avaló la incorporación de la evidencia obtenida gracias al uso del NIT pese a que el FBI no quiso develar todos los códigos.

Según detallan artículos especializados[4] un posterior análisis de expertos y la empresa Mozilla –autora del código explotado por el gobierno para introducir el *malware*– dejó en claro que el contenido de dicho programa solo hubiese sido relevante en caso de comprobarse que el FBI deliberadamente lo había programado para exceder el alcance de la autorización judicial. Basándose en ello, el juez enfrentó la siguiente serie de casos con más y mejor información, lo cual lo llevó a rechazar la pretensión de la defensa.

El fallo fue apelado por la defensa de Tippens y el Tribunal de Apelaciones ratificó la decisión por entender que había una "causa pro-

[4] Hennessey, Susan (2017): "The elephant in the room: Addressing child exploitation and going dark", Aegis Paper Series, Hoover Institution, Stanford University, N° 1701, citado por Blanco, Hernán "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre", disponible en https://indret.com/wp-content/uploads/2021/01/1593-.pdf, última visita marzo de 2021.
Asturias, Miguel Ángel, *Estupefacientes,* Buenos Aires, Hammurabi, 2019, p. 470.

bable" para registrar la residencia de Tippens en Washington basándose en la totalidad de las circunstancias que incluían, entre otras cosas, que Playpen era un sitio ilegal de material de abuso sexual infantil, que Tippens creó una cuenta en Playpen en Hawái, lo mantuvo durante más de tres meses e inició sesión activamente en el sitio durante 26 horas, la evidencia que se podía recuperar la información mediante la recopilación de las actividades del usuario en internet, por lo que podía inferirse de manera lógica que Tippens probablemente llevó, en lugar de enviar, una computadora o computadora portátil cuando se mudó de Hawái a Washington, y que el material que lo incriminaba podía estar alojado en su dispositivo.

XI. Entrega vigilada digital

XI. a. Introducción

Tradicionalmente, la entrega vigilada es una técnica de investigación que consiste en permitir la circulación de bienes y ganancias delictivos, con autorización judicial y conocimiento de las autoridades, bajo su vigilancia, con el objeto de identificar a los partícipes del delito y/o obtener pruebas para la investigación. Ha sido utilizada, especialmente, en los delitos vinculados al narcotráfico, en los términos estipulados por el art. 11 de la Convención de Naciones Unidas sobre el tráfico ilícito de estupefacientes y sustancias psicotrópicas (Viena, 1988; aprobada por ley Nro. 24.072).[1] En el derecho comparado se la ha denominado también "remesa controlada", "entrega controlada" y "circulación y entrega vigilada".[2]

Esta técnica investigativa tuvo tradicionalmente como objetivo "descubrir y desbaratar la intrincada cadena del tráfico ilegal de es-

[1] Artículo 2.i, de la Convención de Palermo de 2000 y 2.i, de la Convención de Mérida de 2003.

[2] Asturias, Miguel Ángel, *Estupefacientes,* Buenos Aires, Hammurabi, 2019, p. 470.

tupefacientes –como sistema delictivo cuyas acciones se multiplican en tiempo y espacio–, otorgándole al juez la facultad de postergar la detención de personas en caso de que la ejecución inmediata de la medida pudiera comprometer un éxito mayor en la investigación".[3]

En ese sentido, se puede pensar teóricamente en una modalidad de entrega vigilada digital que conlleve la misma técnica aplicada en el ámbito de internet, lo cual le generaría modificaciones sustanciales. La Convención de Budapest no posee mención alguna respecto de esta posibilidad para la investigación, así como tampoco fue hallada ninguna normativa especial en el ámbito de referencia del presente proyecto.

En principio y a grandes rasgos, cualquier regulación debe considerar las particularidades que tiene la aplicación de esta técnica al ámbito digital; podemos pensar en dos universos de casos: a) la de aquellos bienes que efectivamente pueden concretar su entrega de forma digital (p. e., pornografía infantil); b) la de cosas físicas cuya entrega puede ser monitoreada digitalmente. A diferencia de la entrega en el mundo físico, surge otro nivel de dificultad en cuanto a la trazabilidad del objeto en la red (en la entrega clásica basta con un exhaustivo seguimiento físico y contacto permanente del sujeto) y la identificación de quién es el receptor (p. e., no hay un sujeto que "firme por el paquete recibido" en el sentido tradicional).

Así se ha sostenido que *muchos de los delitos vistos hasta ahora, se llevan a cabo a través de este método tecnológico, como, por ejemplo, delitos cibernéticos, extorsiones, el conocido actualmente como ciberterrorismo utilizado por grupos organizados como el ISIS para captar "fieles", o la pornografía infantil. Se utilizan herramientas tecnológicas como softwares o "virus espías", que rastrean los rincones de internet buscando material delictivo como, por ejemplo, movimientos y transferencias de dinero, telecomunicaciones habidas entre las personas relacionadas con el delito que hayan podido realizar en el pasado, reservas de viajes o estancias, o entradas y salidas en aeropuertos, etc., que sirvan de aportación de pruebas a la investigación contra los sospechosos investigados. El problema en estos casos surge, en que (...) en el campo informático, existe la dificultad de que los agentes policiales no*

[3] Cornejo, Abel, Cornejo, Abel, *Estupefacientes*, 4ta. edición ampliada y actualizada, Santa Fe, Rubinzal Culzoni, 2018, p. 616.

pueden asegurar el control de la circulación, entre las organizaciones criminales, que realicen por la red, pues no es lo mismo seguir la circulación de un kilo de droga que se desplace entre dos ciudades, que un fichero de contenido pedófilo que circule por internet, sobre todo, por la rapidez con la que circulan estos debido a los avances tecnológicos.[4]

También, esta modalidad se encuentra relacionada, a menudo, con el agente provocador y/o encubierto; así también, en el delito del *grooming* podemos encontrarnos con el "particular provocador", encarnado en los padres que descubren al *groomer* de sus hijos y comienzan a escribirle por las redes sociales con la identidad del menor.

Dado que no existe regulación sobre la forma digital de entrega vigilada, realizaremos un breve delineamiento de la normativa existente de la entrega tradicional en los ámbitos de referencia.

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (aprobada por ley Nro., 25.632) sugiere la incorporación de técnicas de investigación a los países parte, como la "entrega vigilada y, cuando lo considere apropiado, la utilización de otras técnicas especiales de investigación, como la vigilancia electrónica o de otra índole y las operaciones encubiertas, por sus autoridades competentes en su territorio con objeto de combatir eficazmente la delincuencia organizada" (art. 20.1). Del mismo modo y con semejante redacción lo estipula la Convención de las Naciones Unidas contra la Corrupción (ley Nro. 26.097), que agrega que los Estados prevean lo necesario "como para permitir la admisibilidad de las pruebas derivadas de esas técnicas en sus tribunales" (art. 50.1).

En nuestro país, a nivel nacional, la ley de Delitos Complejos Nro. 27.319 establece las figuras de agente encubierto, revelador, informante y entrega vigilada para la investigación, prevención y combate de los delitos vinculados a la ley 23.737, secuestro, trata de personas, asociaciones ilícitas, contrabando de estupefacientes, entre otros señalados

[4] Folgado Gallego, Sergio, "La diligencia de entrega vigilada en el proceso penal español", tesina Facultad de Derecho, Universidad de la Laguna, curso 2017/8. https://riull.ull.es/xmlui/bitstream/handle/915/9498/La%20diligencia%20de%20entrega%20vigilada%20en%20el%20proceso%20penal%20espanol..pdf?sequence=1.

por el art. 2 de la norma. La novedad respecto del sistema anterior es que se puede utilizar en mayor cantidad de delitos.[5]

Con relación a la entrega vigilada, los arts. 15 y 16 le otorgan la facultad al juez de postergar la detención de personas o secuestro de bienes en pos del éxito de la investigación, tanto de oficio como a pedido del MPF y en audiencia unilateral. Incluso, puede suspender la interceptación en el territorio del país de "una remesa ilícita" destinada a otro país, y permitir que circule sin interferencia de las autoridades competentes y bajo su control y vigilancia, con el objeto de identificar a los partícipes o reunir pruebas para la investigación, siempre y cuando tuviere la seguridad de que será vigilada por las autoridades del país de destino.[6]

Así también la normativa faculta al juez a disponer la suspensión de la entrega vigilada en cualquier momento y ordenar la detención de los intervinientes y el secuestro de los elementos correspondientes, en caso de peligro para la vida o integridad de las personas o la aprehensión posterior de los partícipes del delito.[7]

Por su parte, el CPPF en sus arts. 193 y 194 estipula también la figura de entrega vigilada, de manera muy similar a la dispuesta en la citada ley Nro. 27.319, pero, en consonancia con el espíritu del nuevo ordenamiento procesal, se establece que el juez puede ordenarla ante el pedido del representante del MPF.

---

[5] Cornejo, Abel, Estupefacientes, cuarta edición ampliada y actualizada, Santa Fe, Rubinzal Culzoni, 2018, pg. 616.

[6] "Consagrada mediante la introducción que hizo el artículo 11 de la ley 24.424 –como segundo párrafo– al artículo 33. Así, un juez federal puede suspender la interceptación en territorio argentino de un cargamento de droga y permitir su salida del país, cuando tuviere la certeza –seguridades, dice la norma del artículo 11 de la Ley 24.424– de que será vigilada por las autoridades judiciales del país de destino. Dicha medida debe ordenarse por resolución fundada, haciéndose constar, en cuanto fuese posible, la calidad y cantidad de la sustancia vigilada como también su peso". Grisetti, Ricardo Alberto, "Ley n° 27.319 de investigación, prevención y lucha de los delitos complejos. Herramientas y facultades", La Ley Online, AR/DOC/336/2017.

[7] Sin perjuicio de que los funcionarios públicos puedan aplicar las normas de detención para el caso de flagrancia (art. 16 de la ley 21.319).

Ni en el CPPN, ni en los Códigos Procesales Penales de CABA (ley Nro. 2.303), Buenos Aires (ley Nro. 11.922), Mendoza (ley Nro. 6.730), ni Córdoba (ley Nro. 8.123), se menciona la técnica en cuestión.

Por otro lado, España cuenta con la Ley de Enjuiciamiento Criminal, que en el art. 263 bis estipula la entrega vigilada de drogas mediante autorización judicial; en su apartado 2 define: *se entenderá por circulación o entrega vigilada la técnica consistente en permitir que remesas ilícitas o sospechosas de drogas tóxicas, sustancias psicotrópicas u otras sustancias prohibidas, los equipos, materiales y sustancias a que se refiere el apartado anterior, las sustancias por las que se haya sustituido las anteriormente mencionadas, así como los bienes y ganancias procedentes de las actividades delictivas tipificadas en los artículos 301 a 304 y 368 a 373 del Código Penal, circulen por territorio español o salgan o entren en él sin interferencia obstativa de la autoridad o sus agentes y bajo su vigilancia, con el fin de descubrir o identificar a las personas involucradas en la comisión de algún delito relativo a dichas drogas, sustancias, equipos, materiales, bienes y ganancias, así como también prestar auxilio a autoridades extranjeras en esos mismos fines.*[8]

La nueva regulación del art. 588 bis LECrim, realizada por la LO 13/2015, de 5 de octubre, también se aplica en el caso. Es así que, *con*

[8] En tanto el apartado 1 sostiene: "1. El Juez de Instrucción competente y el Ministerio Fiscal, así como los Jefes de las Unidades Orgánicas de Policía Judicial, centrales o de ámbito provincial, y sus mandos superiores podrán autorizar la circulación o entrega vigilada de drogas tóxicas, estupefacientes o sustancias psicotrópicas, así como de otras sustancias prohibidas. Esta medida deberá acordarse por resolución fundada, en la que se determine explícitamente, en cuanto sea posible, el objeto de autorización o entrega vigilada, así como el tipo y cantidad de la sustancia de que se trate. Para adoptar estas medidas se tendrá en cuenta su necesidad a los fines de investigación en relación con la importancia del delito y con las posibilidades de vigilancia. El Juez que dicte la resolución dará traslado de copia de la misma al Juzgado Decano de su jurisdicción, el cual tendrá custodiado un registro de dichas resoluciones. También podrá ser autorizada la circulación o entrega vigilada de los equipos, materiales y sustancias a los que se refiere el artículo 371 del Código Penal, de los bienes y ganancias a que se hace referencia en el artículo 301 de dicho Código en todos los supuestos previstos en el mismo, así como de los bienes, materiales, objetos y especies animales y vegetales a los que se refieren los artículos 332, 334, 386, 399 bis, 566, 568 y 569, también del Código Penal".

la diligencia de entrega vigilada a través de internet, lo que se persigue, como se puede deducir del nombre, no son envíos físicos, sino archivos, ficheros, correos electrónicos, en definitiva, material informático susceptible de incurrir en actividades delictivas. Esto es, lo que los agentes de la Policía Judicial permiten que se transfiera o circule, con la finalidad de aprehender al mayor número de partícipes, y retirar de la red la cantidad máxima posible de archivos en circulación. Se trata de aprovecharse de los avances tecnológicos que utilizan los delincuentes, para llevarlos al campo de la lucha contra el crimen. De igual manera que ocurre en las investigaciones físicas convencionales, los agentes pueden llevar a cabo esa diligencia "con sustitución del material, interceptar ese material informático y sustituirlo por otro de su interés, ante la posibilidad de perderle el rastro en la red, y que el delito se consuma. Ocurre, por ejemplo, en el caso de la pornografía infantil o el ciberterrorismo, donde se puede sustituir las fotografías o videos por otros que no sean dañinos, o por esos archivos o *softwares* que una vez abiertos, delaten al infractor".[9] Se expone en el art. 588 bis a.1 LECrim que, para llevar a cabo esta diligencia se requerirá "autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida".

Alemania, por su parte, cuenta con las Directrices para procedimientos penales y multas (RiStBV), que definen el "tránsito controlado" como "el transporte ilegal de narcóticos, armas, bienes robados, bienes robados, etc., monitoreado por las agencias policiales, desde el extranjero a través del país a un tercer país"; que distinguen entre exportación controlada –el transporte ilegal monitoreado desde el exterior– y la importación controlada, realizado desde el extranjero al interior del país.

En Estados Unidos de América, la jurisprudencia utiliza ampliamente el "controlled delivery" Para evitar peligros de las demoras en el otorgamiento de una orden judicial en situaciones de entrega vigilada, conforme lo dispuesto por la Suprema Corte en United States v. Grubbs (2006), las fuerzas de seguridad pueden obtener una orden de registro anticipada, que se basa en la declaración jurada mostrando causa probable que evidencia cierto delito, que se cometerá en un futuro

[9] Folgado Gallego, Sergio, "La diligencia de entrega vigilada en el proceso penal español", tesina Facultad de Derecho, Universidad de la Laguna, curso 2017/8.

señalado; ello, siempre que en la maniobra no se instigue a la comisión del delito mediante la figura del "entrapment", lo que torna a la técnica ilegítima (Jacobson v. United States, 1991).

XI. b. Jurisprudencia

XI. b. 1. Ciudad Autónoma de Buenos Aires

Juzga*do de Primera Instancia en lo Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires N° 20, caso "I.E.L. s/ abuso sexual simple", 30 de enero de 2020*

El juez Norberto R. Tavosnanska resolvió en la audiencia correspondiente dictar la prisión preventiva solicitada por el Ministerio Público Fiscal, respecto del imputado E. L. I. por los delitos de *grooming* y abuso sexual.

El fiscal imputó a E. L. I. que el 26 de enero del corriente año en el inmueble de la calle XXXX, de la Ciudad Autónoma de Buenos Aires intentó abusar sexualmente del menor T. V. C. de 11 años; así también que, para convencerlo de un encuentro sexual, lo contactó y le envió durante un lapso prolongado desde el 20 de enero de 2020 en horas de la tarde hasta el domingo 26 de enero del mismo año mensajes a través de la red social Instagram. Al principio le profería frases tales como "te quiero y a ver cuándo me prestás un bóxer" a lo que el menor respondía "no amigo te van a quedar chicos" sin perjuicio de que I. insistía en que le diera uno igual. Cuando el niño le preguntaba cómo pasárselo el imputado le decía "para ver, qué sé yo", "regalame si querés yo te doy la plata", "qué sé yo bro".

Posteriormente, el acusado comenzó a solicitarle que no contara nada de lo que hablaban y le dijo frases tales "cuando me invitás a tu casa", "tenés que venir un día aunque sea", "yo no te voy a hacer nada", y "amigo necesito un hermanito como vos". Luego de todas sus conversaciones le proponía que borrase todo después; le decía: "te hago la paja por plata", "borra todo después", "yo pago todo y pago bien", "yo siempre pago", "pero no digas nada a nadie", "queda todo acá", "y si pinta algo qué sé yo"; "si querés juga vos y yo te la chupo", "yo te la toco nada más no va a pasar nada turro, qué sé yo vos jugás con el celu o la

play. Que te la toque un ratito queda acá. En serio no voy a decir nada a nadie ahh re" "te la toco y si pinta qué sé yo", "bueno obviamente coger no, pero pete o paja te hago. Estate en bóxer así te la toco. Jajá".

La fiscalía fundó su pedido de prisión preventiva en el riesgo del entorpecimiento del proceso, en los términos del artículo 171 del CPPCABA; también que por la magnitud de la pena potencial podría no ser de ejecución condicional. También consideró relevante el temor manifestado por el menor en la audiencia de Cámara Gesell, justamente por el área del barrio y los lugares a donde concurren el imputado y el menor. Agregó que se encontraba en la etapa de producción de prueba, de los dispositivos informáticos secuestrados en el allanamiento realizado.

A lo dicho añadió que nunca hay consentimiento del niño, independientemente de si entiende o no la actividad, incluso cuando no muestre signo de rechazo. Señaló que el contacto sexual puede configurar abuso cuando hay aprovechamiento intencional de la diferencia de edad, y que el imputado tenía 23 años y el menor 11. También que existieron actitudes inapropiadas, comentarios lascivos respecto a la intimidad sexual de los niños, y que eso se vio en el intercambio de mensajes. Para la fiscalía se encontraba probado el delito de *grooming*.

Resaltó que entre las tácticas de seducción de los agresores existe la compra de regalos y que el menor en la Cámara Gesell habló de acercamientos que T. tenía con I. y con sus amigos. Dijo que les hacía regalos, golosinas, les daba plata y hasta los invitaba a Mc Donald's.

Debido a los argumentos descritos, por toda la prueba que faltaba recabar, solicitó que se dictase la prisión preventiva por el plazo de noventa días.

Por su parte, la defensora solicitó el rechazo de la prisión preventiva por no encontrarse probada la materialidad del hecho. Indicó que la fiscalía se limitó a imputarle la tentativa y refirió a las conversaciones que su asistido habría tenido por la red social Instagram diciendo que el hecho sucedió en la calle XXX de esta Ciudad en donde intentó abusar del menor T. V. C. de 11 años, pero que no hizo mención del modo comisivo, ni explicó cuándo habría un principio de ejecución por parte de su asistido. Indicó que solo se dijo que fue en la puerta del domicilio del menor, pero no se especificó qué hizo. Postuló que nuestro derecho penal liberal y de acto exige la descripción de un acto concreto.

Añadió que el delito de abusar, según la doctrina, requiere un contacto físico entre el autor y la víctima. Que si bien es cierto que se

discute que puede haber actos de acercamiento de una parte pudenda al cuerpo de la víctima, que no se puede comprender en el caso cuál fue el acto en concreto. Relacionado con la tentativa y la consumación, sostuvo que la mayoría de la doctrina no admite la tentativa del abuso sexual simple, solo para casos de que exista violencia. Postuló que solo hubo meros actos preparatorios sin dolo.

Respecto del delito de *grooming* afirmó que, si bien pueden ser repudiables las acciones que realizó su asistido, tampoco se confirmó ese delito. Dividió la conducta de su asistido en dos etapas.

La primera sería la conversación que mantiene con T., en la que le dice "gracias amigo, me voy a comer que IPhone es" no hay tipicidad, pero hay un mensaje en el que le dice "a ver cuándo me prestás un bóxer". Sostuvo que el dolo se puede llegar a presentar después, pero no en el chat con el niño.

Una segunda etapa fue aquella en la que empieza a hablar con un mayor de edad, el padrastro de T, que se hace pasar por el menor, lo cual no está controvertido. Afirmó entonces que en el caso no estaba presente el tipo subjetivo, ya que la persona con la cual se intercambiaron los mensajes era mayor de edad y, por ende, no había delito de *grooming*.

Con relación a los riesgos procesales, sostuvo que las penas permitirían una condena de ejecución condicional, y que se realizó un allanamiento en el que se le secuestraron los dispositivos electrónicos a su asistido, por lo que no podría entorpecer el proceso.

Pidió el rechazo de la prisión preventiva y, en todo caso, una medida restrictiva.

Asimismo afirmó que el miedo que manifestó el menor en la Cámara Gesell fue impuesto por la secuencia en la que le contaron el procedimiento realizado por los padres, en el que los padres se transformaron en agentes provocadores para hacer ir al imputado a donde estaba el menor, siendo dicha circunstancia lo que perturbó al menor.

A su turno, la fiscal rechazó las medidas restrictivas propuestas por la defensa.

Del cuestionamiento sobre la validez de las comunicaciones de los padres del menor con el imputado, indicó que no se trató de una diligencia judicial o un acto que deba ser realizado con control judicial y sobre la base de las normas de procedimiento. Señaló que fue una medida que tomaron los padres para resguardar al menor, y que en el diálogo que mantuvo el padre del menor con el imputado se limitó a

mantener la conversación sin utilizar diálogos con contenido sexual, lo que sí hizo el imputado.

Por su parte, la asesora tutelar coincidió con el criterio de la fiscalía, y refirió que quizás se encontraban ante un abuso calificado, pues no estaba claro cuál era el rol que ocupaba el imputado en el gimnasio donde concurría el niño. Agregó que se podría estar en presencia de delitos conexos, ya que podría haber otras víctimas.

También remarcó que, cuando la psicóloga le preguntó al menor si hubo un encuentro con el imputado, allí el niño realizó una manifestación con el cuerpo en la que ocultó sus manos, se protegió haciéndose una bolita y dijo que no; por lo que iba a solicitar una pericia psicológica para establecer si hubo abusos sexuales.

Indicó que la víctima que vive en un barrio cercano a donde vive el imputado, que podría aportar mayor prueba y que a su vez aportó dos nombres de dos posibles víctimas.

Destacó que el imputado no solamente manifestó en el chat que quería tener relaciones sexuales con el menor, sino que fue a hasta el palier, ingresó al lugar con preservativos en la mochila, con un líquido y una jeringa. Hizo hincapié en que también faltaban medidas de prueba para ver qué efectos tenía la droga incautada, que podría ser un estimulante anabólico y con efectos colaterales a nivel sexual. Y puntualizó que el imputado quería subir al departamento, aunque el niño le decía que esperasen allí porque hacía calor.

El juez ingresó en el análisis de las cuestiones controvertidas. Indicó que las partes no cuestionaron la materialidad de los hechos ni los diálogos entre el menor y el imputado, así como tampoco que el imputado concurrió al domicilio del menor, que tenía conocimiento de que se encontraba solo. Mencionó que el imputado claramente le dijo: "y si pinta yo te doy plata, no te preocupes te quiero amigo" y "si querés jugás vos mientras yo te la toco", "de que te la toque un ratito queda acá y no decimos nada"; "estate en bóxer así yo te la toco". Sostuvo que no solo habla de tocamiento y de otros vínculos sexuales, sino que hace referencia a la posibilidad de que haya penetración más allá de la realización de sexo oral.

Respecto del argumento de la defensa de que los diálogos fueron entre dos adultos, indicó que en el momento en que se estaban llevando a cabo esas conversaciones el imputado no sabía que se encontraba hablando con un adulto, ya que creía que estaba conversando con T.; recién con posterioridad a dicha situación esa cuestión pudo ser adver-

tida por el imputado. Manifestó que allí radica una diferencia sustancial para resolver la situación fáctica del *iter criminis*.

También introdujo una cuestión sustancial no expuesta por las partes: que en la Cámara Gesell, T. dijo que en el momento en el cual I. quiso entrar a su domicilio hubo una hábil pero contundente resistencia del menor, ya que el imputado todo lo que quería era subir a su hogar.

Por otra parte, remarcó que el menor no se encontraba en soledad, ya que estaba presente una vecina además de su madre. Por ello, entendió que dicha cuestión resulta relevante a la hora de delimitar los actos preparatorios no punibles de los actos que integran el principio de ejecución los cuales resultan punibles, y son integrantes de la base de la tentativa.

A su vez, explicó que se encontraron presentes tres testigos: una vecina, la madre y el padrastro. Y que luego el padrastro convocó a personal policial, que detuvo al imputado. Remarcó que la policía no lo estaba esperando, sino que llegó con posterioridad y sobre la base de la convocatoria realizada por el padrastro del menor, motivo por el que descartó la teoría del agente provocador.

Respecto de la tipicidad, sostuvo que tanto en el *grooming* como en el abuso existen distintas teorías respecto de las diferencias entre los actos preparatorios no punibles y el principio de ejecución punible.

Primero indicó el plan o el comienzo del *iter criminis*, en el que a su entender el incuso había ingresado, debido al tenor de los mensajes intercambiados y a que el imputado concurrió al domicilio con preservativos, dinero y con una jeringa llevando droga. Así también indicó que no hubo desistimiento voluntario por parte del Sr. I., ya que el delito no fue consumado por la presencia de terceros.

Finalmente, por los argumentos descritos, dispuso la prisión preventiva por noventa días para el imputado, por la posibilidad de entorpecimiento de la investigación, en virtud de la cantidad de prueba pendiente de producción.

XII. Uso de drones

XII. a. Introducción

La existencia de drones, cuya tripulación a distancia permite una mayor capacidad de intromisión en recintos domiciliarios abiertos y su utilización en el marco de investigaciones criminales, no se encuentra específicamente regulado en nuestra legislación. Vehículo Aéreo No Tripulado (VANT), comúnmente denominado dron, es considerado un vehículo aéreo destinado a volar sin piloto a bordo, y es controlado desde una estación de pilotaje a distancia

En ese contexto, su uso no ha sido admitido por parte de tribunales argentinos –que decretaron la nulidad de elementos de prueba obtenidos por VANT por no contar con previa autorización judicial– aunque tampoco ha sido descartado de lleno, al recomendarse un uso especialmente prudente y cuidadoso de esos elementos (como medios de investigación), procurando –de ser posible– una activa participación de los órganos judiciales y jurisdiccionales en la efectivización de las diligencias, a fin de garantizar una efectiva tutela de los derechos constitucionales (cfr. NN s/estupefacientes –siembra o cultivo– art. 5º ley 23.737. Sala I de la Cámara de Apelación y Garantías en lo Penal Departamental de Bahía Blanca. Investigación penal preparatoria 17.673).

La única legislación existente en la materia es el Reglamento provisional de los vehículos aéreos no tripulados de la Administración Nacional de Aviación Civil, que brinda definiciones sobre estos dispositivos, y precisa su uso en materia de prevención de delitos, no así a su utilización como herramienta en el marco de un proceso penal. Es así como el reglamento indica que el uso del VANT o SVANT con el propósito de prevenir delitos o detener hechos ilícitos en ejecución, que es ejercido en forma exclusiva por las fuerzas de seguridad federales o locales en virtud de las funciones asignadas en sus normas constitutivas o en cumplimiento de una manda judicial.

Como se ha mencionado, la utilización de VANT no se encuentra específicamente regulada en el Convenio para la Ciberdelincuencia de Budapest ni en nuestras leyes de procedimientos. En lo que hace a la legislación local, cabe apuntar que la Ley 27.319 que introduce las nuevas Técnicas especiales de investigación al proceso penal no hace mención específica a este tipo de elementos.

En el ámbito del derecho comparado tampoco se encuentran regulaciones específicas, sino que las distintas normas procedimentales regulan las nuevas técnicas de investigación de forma más genérica, a fin de que la legislación no quede en desuso ante el avance de la tecnología.

Así, en España, la ley orgánica 13/2015 que reforma la Ley de Enjuiciamiento Criminal prevé en su artículo 588 *quater* a) la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados; mientras que en su artículo 588 *quinquies* a) la captación de imágenes en lugares o espacios públicos.

De un primer análisis de la problemática, se observa que, si bien este tipo de mecanismos no tiene una regulación específica, tampoco existe una prohibición expresa para su uso, y en líneas generales la admisibilidad de prueba obtenida mediante VANT gira en torno a la autorización judicial previa que respete las garantías constitucionales que resguardan a la privacidad y la inviolabilidad del domicilio.

Tampoco en los Estados Unidos se prevé legislación específica para el uso de drones para registro de personas, domicilios o documentos, y su implementación en casos penales se revisa dentro de los marcos de protección de la cuarta enmienda, y la jurisprudencia que versa

sobre prueba obtenida por medio Aviones tripulados (vrg. California v. Ciraolo; Dow Chemical v. United States o Florida v. Riley).

XII. b. Jurisprudencia argentina

XII. b. 1. Fuero federal

Juzgado Federal N° 1 de Azul, Caso N° 1110/2017, "Incidente N° 4. Salaberry, Giselle y Otro s/ Incidente de Nulidad", 28 de febrero de 2018

El expediente se inició con una la denuncia anónima en la Subdelegación Olavarría de la Policía Federal Argentina, ocasión en la que dejó constancia acerca de un llamado telefónico por parte de una persona que no quiso identificarse, mediante la cual puso en conocimiento de que en una vivienda sus moradores tendrían plantas de marihuana.

En la causa previno anteriormente una Unidad Funcional de Instrucción (UFI) con competencia ordinaria: "dispuso que se proceda a realizar tareas investigativas en relación con los domicilios aportados con el fin de proceder a la individualización de los moradores y verificar la veracidad de la denuncia", tras lo cual se solicitó una orden de allanamiento en el lugar, donde efectivamente se secuestraron estupefacientes.

La causa, posteriormente radicada en sede federal, concluyó con la nulidad de la orden dictada, luego de que la defensa oficial de los imputados lo solicitara, luego de denunciar "que se realizaron tareas investigativas consistentes en espiar a los ciudadanos mediante objetos voladores no tripulados –drones– un día antes a la denuncia. Por ello entiende que la policía jamás podría haber dirigido una investigación dirigida contra un individuo fundada en una denuncia ocurrida posteriormente".

La defensa aseguró: *el registro de una propiedad a distancia, mediante un dispositivo robótico afecta el derecho a la intimidad de quien reside en esta y debe ser ordenado por un juez competente mediante acto fundado, no habiéndose cumplido con estas formalidades el registro de la propiedad de mis asistidos es nulo.*

La fiscalía, al contestar la vista, rechazó los argumentos al sostener que *la utilización del dron fue efectuado con el simple objeto de obtener*

las vistas fotográficas obrantes en autos, las cuales se asemejan a las que podrían haberse obtenido en internet. En tal sentido advierte que no se ha invadido el ámbito privado ni la intimidad de los moradores de la vivienda observada.

El juez federal Martín Bava dijo: *la orden de allanamiento dispuesta no satisface el deber de fundamentación exigido, pues el magistrado no solo no efectuó ninguna consideración que justifique la medida, sino que mencionó extremos que no fueron señalados por la prevención (los elementos que presumía que allí había o podían hallarse).*

Además de ello tampoco realizó mención alguna en relación con la fecha de la denuncia anónima recibida en sede policial (15 de febrero de 2017), la cual es posterior a la realización de las tareas de investigación por parte del personal de la prevención sobre el domicilio en cuestión (un día antes), extremos por los cuales podrían inferirse también una grave irregularidad en el actuar policial, y que conllevaría también a dejar sin sustento a la decisión judicial tachada de nula por la Defensa Oficial.

XII. b. 2. Provincia de Buenos Aires

Cámara de Apelación y Garantías en lo Penal del Departamento Judicial Bahía Blanca. Sala I "NN s/ estupefacientes –siembra o cultivo– artículo 5 Ley 23.737"

La Sra. Jueza a cargo del Juzgado de Garantías nro. 3 Departamental dispuso la exclusión probatoria de la declaración testimonial y de las placas fotográficas acompañadas en la causa, que habían sido obtenidas mediante el uso de un dron, y –en consecuencia– denegó el allanamiento requerido, por no contarse con elementos de convicción suficientes que justifiquen la intromisión.

Según la magistrada, los medios de convicción ofrecidos han afectado los derechos constitucionales a la privacidad e intimidad, por "invadir un espacio privado sobre el que cualquier injerencia solo puede ser decidida con intervención de los órganos judiciales y jurisdiccionales".

Dicha decisión fue apelada por la Fiscalía, asegurando: "ni el personal policial, ni el dron ingresaron al domicilio investigado" y que "el levantamiento de un dron en forma vertical no resulta violación de domicilio". En apoyo a su postura, el fiscal indicó: *el dron se alzó sobre*

la esquina del inmueble pudiendo divisar que el patio del domicilio de esta persona hay una construcción de chapas y ladrillo, la cual tiene como techo una red color naranja, a través de la cual se puede observar plantas similares alas de la especie cannabis sativa.

La Cámara revisó la imagen y concluyó: "fue tomada desde un ángulo lateral horizontal y con una gran cercanía al objeto que captó, lo que indica que el uso del equipo tecnológico utilizado no se limitó a un ascenso vertical exterior", por lo que "la intromisión del dron como se llevó adelante requería algo más que la difusa testimonial del personal policial que inicia las actuaciones".

Finalmente, la Cámara recomendó "un uso especialmente prudente y cuidadoso" de los dispositivos digitales como medio de investigación ante "las posibilidades de intromisiones ilegítimas en la privacidad de los ciudadanos que puede derivarse del uso de nuevas tecnologías".

XII. c. Jurisprudencia internacional

XII. c. 1. España

Tribu*nal Supremo de España, Sala de lo Penal, STS 329/2016, de 20 de abril de 2016*

Miembros de la Brigada Provincial de Seguridad Ciudadana tuvieron conocimiento a través de distintos anónimos, comunicaciones personales e incluso de una pintada, a cerca de la actividad de venta y distribución de sustancias estupefacientes que se desarrollaba en el restaurante Tres Torres y en el que realizaba funciones de encargado, el acusado D. Evelio, de 32 años, y sin antecedentes computables en esta causa. Por ello, se estableció un dispositivo de vigilancia del referido local, así como de la vivienda del Sr. Evelio.

En el ejercicio de sus funciones investigativas, integrantes de las fuerzas de seguridad, valiéndose de unos prismáticos, observaron a través de uno de los dos ventanales que daban a la calle, correspondiente al salón y el cual carecía de ningún obstáculo que dificultase o impidiese ver el interior, como Evelio e Ildefonso –el otro de los investigados– *manipulaban una sustancia de color marrón y la envolvían en un plástico negro, así como la presencia de otra sustancia contenida*

en una bolsa termo sellada. Rosana abandonó el salón y regresó portando una bolsa de color rojo, sin anagramas, la cual entregó al Sr. Evelio quien introdujo en la misma los paquetes previamente preparados e hizo entrega de la misma a Ildefonso.

Ambos imputados fueron condenados por la Audiencia Provincial de Ourense, Sección Segunda a cuatro años de prisión por tenencia y distribución de estupefacientes. Ambas defensas presentaron recurso de casación. La de Evelio, entre otros puntos, denunció que existió una vulneración al derecho constitucional a la inviolabilidad del domicilio, proclamado en el art. 18.2 de la Constitución Española.

Los jueces de la audiencia provincial habían rechazado oportunamente los planteos nulificatorios en el entendimiento de que la *actuación de los agentes, derivada de la inmediatez del curso de los hechos, no supone la vulneración del derecho a la intimidad de los acusados en cuanto estos no establecieron obstáculo alguno que impidiese la visión del salón, como se desprende de la precisa información facilitada por los agentes, la cual sería inviable de haberse dispuesto obstáculos que impidiesen esa visión.*

Llegado el caso a la Sala en lo Penal del Tribunal Supremo de Justicia, se admitió el recurso y se declaró la nulidad del procedimiento y la absolución de los imputados.

El fundamento fue: "la protección constitucional de la inviolabilidad del domicilio, cuando los agentes utilizan instrumentos ópticos que convierten la lejanía en proximidad, no puede ser neutralizada con el argumento de que el propio morador no ha colocado obstáculos que impidan la visión exterior".

Asimismo, "el domicilio como recinto constitucionalmente protegido no deja de ser domicilio cuando las cortinas no se hallan debidamente cerradas. La expectativa de intimidad, en fin, no desaparece por el hecho de que el titular o usuario de la vivienda no refuerce los elementos de exclusión asociados a cualquier inmueble. Interpretar que unas persianas no bajadas o unas cortinas no corridas por el morador transmiten una autorización implícita para la observación del interior del inmueble, encierra el riesgo de debilitar de forma irreparable el contenido material del derecho a la inviolabilidad domiciliaria".

El fallo además cita el art. 588 *quinquies* a), introducido por la reforma de la LO 13/2015, 5 de octubre, que en su apartado 1º dispone: "la Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar

o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos", agregando que "sin embargo, el art. 588 *quater* a) somete a autorización judicial la utilización de dispositivos electrónicos orientados a la grabación de imágenes o de las comunicaciones orales directas entre ciudadanos que estén siendo investigados, ya se encuentren aquellos en un recinto domiciliario, ya en un lugar público".

Para el Supremo, si bien es cierto que la reforma no contempla de forma específica el empleo de prismáticos *la intromisión en la intimidad domiciliaria puede encerrar similar intensidad cuando se aportan al proceso penal las imágenes grabadas o cuando uno o varios agentes testifican narrando lo que pudieron observar, valiéndose de anteojos, en el comedor del domicilio vigilado*, máxime cuando en el caso tampoco existió autorización judicial.

Finalmente, el Alto Tribunal concluyó: *la protección constitucional frente a la incursión en un domicilio debe abarcar, ahora más que nunca, tanto la entrada física del intruso como la intromisión virtual. La revolución tecnológica ofrece sofisticados instrumentos de intrusión que obligan a una interpretación funcional del art. 18.2 de la CE. La existencia de drones, cuya tripulación a distancia permite una ilimitada capacidad de intromisión en recintos domiciliarios abiertos es solo uno de los múltiples ejemplos imaginables. Pero incluso para el caso en que se entendiera que los supuestos de falta de presencia física por parte de los agentes en el domicilio investigado deben ser protegidos conforme al concepto general de intimidad que ofrece el art. 18.1 de la CE, lo cierto es que en el presente caso no consta la existencia de ningún fin constitucionalmente legítimo que, por razones de urgencia, permitiera sacrificar la intimidad del sospechoso.*

XIII. Acceso a comunicaciones electrónicas desarrolladas a través de plataformas de mensajería instantánea y a correos electrónicos laborales en el marco de políticas de *compliance*

XIII. a. Introducción

La evolución de las comunicaciones, a la par del progreso tecnológico, ha extendido los ámbitos de interacción al escenario digital. Esto supone, no solo el avance de la tecnología sobre las comunicaciones personales sino también, su avance sobre las interacciones que tienen lugar en los ámbitos laborales.

Desde luego que el surgimiento de estos entornos digitales de interacción supuso un desafío para la normativa jurídica, dado que no contemplaba la específica protección de estos nuevos espacios de comunicación informática.

Hasta la sanción de la Ley de Delitos Informáticos (Ley N° 26.388), que introdujo modificaciones en el Código Penal, gozaban de protección las comunicaciones epistolares y los papeles privados, cuya inviolabilidad consagra del artículo 18 de la Constitución Nacional.[1]

[1] Específicamente el texto de dicho artículo establece: "(...) El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a

Frente a la nueva realidad tecnológica y a su innegable impacto sobre las comunicaciones personales –junto con la consecuente expansión de la esfera de privacidad–, la citada ley significó la introducción en la legislación argentina, de disposiciones que, específicamente, procuran extender el ámbito de protección penal, a las comunicaciones electrónicas, sancionando a quien ilegítimamente accediere a ellas.[2]

Como bien señala Carlos Christian Sueiro: *Las razones que han impulsado esta ampliación y redefinición del bien jurídico protegido, muy probablemente obedezcan a que en las últimas décadas el acelerado e irrefrenable avance de las tecnologías de la información y la comunicación, a través del empleo de computadoras conectadas a Internet, el empleo de teléfonos celulares, el uso del chat, comunicaciones por Voz IP, han expuesto y hecho cada vez más vulnerable la intimidad y privacidad de las personas.*[3] Continúa añadiendo que *por ello, a los efectos de proteger y tutelar eficientemente el derecho de reserva e intimidad de los ciudadanos es que se ha ampliado y redefinido el bien jurídico protegido con el objeto de qué conductas cotidianas que se realizan mediante el empleo de nuevas tecnologías de la información no se vean desprovistas de protección estatal. (...) El derecho a la intimidad o privacidad*

---

su allanamiento y ocupación (...)".

[2] Así, el nuevo artículo 153 del Código Penal prevé: "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

[3] Sueiro, Carlos Christian, *Criminalidad Informática. La eficacia de la reforma al Código Penal en materia de delitos informáticos – Análisis de las leyes 26.388, 26.685 y 26.904*, Buenos Aires, Editorial Ad-Hoc, 2016, pág. 97 y sgtes.

es un derecho personalísimo que encuentra sustento en el respeto a la dignidad humana y que posee su plataforma legal y normativa en la interpretación armónica de los arts. 18, 19 y 33 de la C.N. y de los arts. 11, incs. 2° y 3° de la CADH, 17 del PIDCP, 12 de la DUDH y 10 de la DADDH.[4]

Por su parte, Gustavo Aboso –citando a Germán Bidart Campos– señala: *las acciones privadas están definidas de modo negativo por el art. 19 de nuestra constitución y ampara tan solo un aspecto de la esfera de intimidad personal referida a las conductas autorreferenciales, pero a ello debe agregarse que la tutela constitucional se extiende a la expectativa de privacidad o confidencialidad de dichas conductas solipsistas como las intersubjetivas.*[5]

Advierte, además, el referido autor: *el derecho a la expresión de ideas y su libertad de comunicación engarzan de manera directa con el ámbito de tutela penal provisto por este art. 153 del Código Penal argentino.*

En este sentido agrega, siguiendo a Hilgendorf: *en la actualidad los medios existentes de acuerdo con el grado de evolución alcanzado por nuestra sociedad tecnológica obligan al intérprete a adoptar una postura cautelosa que permita ampliar las zonas de privacidad en lugar de restringir su espacio.*

Pues bien, desde ya que el abanico de nuevas formas de comunicación que trajo aparejado el avance de la tecnología ha tenido un impacto significativo y transversal, sobre cada uno de los ámbitos en los que se manifiesta y desarrolla la personalidad, incluyendo el laboral.

Así, la incorporación de este tipo penal reavivó la discusión a propósito de la posibilidad de los empleadores de acceder a las comunicaciones de sus dependientes, debido a que no contamos con una regulación legal específica que la contemple expresamente.

Vale la pena hacer aquí la siguiente aclaración. Esos debates a los que hemos hecho referencia no abarcan a las cuentas de correo electrónico privadas de los empleados y al control que sobre estas pudieran ejercer los empleadores, puesto que, acerca de la imposibilidad de

[4] Sueiro, Ob. cit., pág. 98.

[5] Aboso, Gustavo, "Acceso indebido a las comunicaciones electrónicas en el ámbito laboral (art. 153 del Código Penal)" en Dupuy, Daniela y Kiefer Mariana. *Cibercrimen*. Buenos Aires, Editorial Bdef, 2017, pág. 191.

autorizar tales intromisiones, en función de su equiparación con la correspondencia epistolar, protegida por mandato constitucional, no existirían controversias.

En particular, la discusión que surge en nuestro país gira en torno de las facultades que tendría el empleador para acceder y/o controlar las comunicaciones mantenidas a través del correo corporativo. A ello se suma que, si consideramos que el empleador, en determinado caso, no puede acceder al correo corporativo de sus empleados; si lo hiciera, estaría cometiendo un delito y podría ser juzgado penalmente. Es decir, si en un pronunciamiento dado se declara inválido un acceso a un correo, se estaría frente a la comisión del delito de acceso indebido a las comunicaciones.

En efecto, se observa en estos casos, un conflicto de intereses, que pone en tensión al derecho de propiedad empleador sobre las herramientas de trabajo –incluidos los correos corporativos que proporciona a sus dependientes para que puedan llevar adelante sus labores– y las facultades de organización y de control que le confiere la Ley de Contrato de Trabajo (arts. 64, 65 y 70 de la ley 20.477), con la normativa penal que veda el acceso indebido a las comunicaciones electrónicas.

Por un lado, en la legislación laboral no encontramos una regulación que, específicamente, contemple la posibilidad de acceso y control a los correos electrónicos corporativos de los empleados, por parte del empleador; y ninguna salvedad al respecto prevé la normativa penal que –lisa y llanamente– prohíbe el acceso a las comunicaciones electrónicas.

Sumado a ello, debe tenerse en cuenta la aparente colisión de derechos que nace a partir de la sanción de la ley de Responsabilidad Penal de las Personas Jurídicas (Ley N° 27.401), dicha ley reconoce la posibilidad de adjudicar responsabilidad penal a las personas jurídicas privadas, respecto de la comisión de una serie de delitos taxativamente enumerados en la referida normativa.[6]

[6] Ley 27.401, "ARTÍCULO 1°.– Objeto y alcance. La presente ley establece el régimen de responsabilidad penal aplicable a las personas jurídicas privadas, ya sean de capital nacional o extranjero, con o sin participación estatal, por los siguientes delitos: a) Cohecho y tráfico de influencias, nacional y transnacional, previstos por los artículos 258 y 258 bis del Código Penal; b) Negociaciones

Pues bien, dentro de las previsiones de la citada ley –específicamente en sus arts. 22 y 23– se prevé la posibilidad de dictar e implementar *Programas de Integridad, consistentes en el conjunto de acciones, mecanismos y procedimientos internos de promoción de la integridad, supervisión y control, orientados a prevenir, detectar y corregir irregularidades y actos ilícitos comprendidos por esta ley*. De hecho, la implementación y cumplimiento de estos programas de *compliance* por parte de las personas jurídicas puede influir tanto en la graduación como en la exención de la pena.

Resulta relevante traer a colación lo señalado en el primer párrafo del art. 8 de esta: *Para graduar las penas previstas en el artículo 7° de la presente ley, los jueces tendrán en cuenta el incumplimiento de reglas y procedimientos internos; la cantidad y jerarquía de los funcionarios, empleados y colaboradores involucrados en el delito; la omisión de vigilancia sobre la actividad de los autores y partícipes; la extensión del daño causado; el monto de dinero involucrado en la comisión del delito; el tamaño, la naturaleza y la capacidad económica de la persona jurídica; la denuncia espontánea a las autoridades por parte de la persona jurídica "como consecuencia de una actividad propia de detección o investigación interna"; el comportamiento posterior; la disposición para mitigar o reparar el daño y la reincidencia. (...)* (el destacado pertenece a esta obra).

En este sentido, resulta ilustrativo señalar lo indicado por Francisco Castex en relación con las investigaciones internas: *Dentro de la facultad de la empresa de fiscalizar al trabajador podría trazarse una distinción entre el registro de la persona, su taquilla y sus efectos personales, por un lado; y la supervisión de los medios que el empresario pone a disposición del trabajador para la producción (teléfono, ordenador, cuentas de correo electrónico, etc.). La intervención en los medios productivos de la empresa permitiría una interpretación más amplia, ya que el basamento es la relación contractual que existe entre ambos, de*

---

incompatibles con el ejercicio de funciones públicas, previstas por el artículo 265 del Código Penal; c) Concusión, prevista por el artículo 268 del Código Penal; d) Enriquecimiento ilícito de funcionarios y empleados, previsto por los artículos 268 (1) y (2) del Código Penal; e) Balances e informes falsos agravados, previsto por el artículo 300 bis del Código Penal".

la que se desprende el deber del trabajador de desarrollar correctamente su actividad laboral y el de la facultad de la empresa de controlar que ello sea efectivamente así. De ahí que permitiría el control de computadoras, cuentas de correo electrónicas corporativas (ya que al ser medios de producción se consideran idóneos para albergar información del trabajador).[7]

Concluye Castex: *En el caso de los mails, en principio habrá que diferenciar si se trata de una casilla cooperativa que provee la propia empresa o no. En ese primer supuesto, siempre y cuando lo haya advertido previamente y notificado de manera fehaciente a los empleadores, la empresa tendría un derecho de supervisión sobre el contenido de los mails con el fin de que sean utilizados respetando los fines éticos para los cuales se proveyó la cuenta.*[8]

Siguiendo con las posturas doctrinarias, Pablo Palazzi indica: *En doctrina existen diferencias acerca de cuáles son los límites legales vigentes. Para un sector mayoritario, cuya opinión compartimos, es posible que el empleador revise los correos electrónicos del trabajador si se trata del corporativo y se hace dentro del reglamento de la empresa. Para otro sector doctrinario, más reducido, la revisión no puede tener lugar, salvo cuando el trabajador ha prestado su consentimiento. Algunos incluso van más lejos y exigen que este consentimiento sea por escrito.*[9]

Finalmente, Aboso sostiene al respecto: *...la ley constitucional resguarda el derecho a la intimidad y a la privacidad de un modo amplio. La intimidad puede ser definida a partir de una contextualización meramente autorreferencial basada en el derecho de estar solo, pero ella resulta claramente insuficiente en la actual era de la información y la comunicación digitales. Las condiciones de posibilidad de ampliar el horizonte de nuestra esfera de privacidad a partir de los adelantos técnicos nos enseñan que la privacidad se extiende sin duda alguna a aquellas relaciones intersubjetivas no dañinas para terceros de parte de sujetos responsables. En este marco de ejercicio de esta autonomía personal el*

---

[7] Castex, Francisco *Responsabilidad penal de la persona jurídica y compliance*, Buenos Aires, Ad-Hoc, 2018, pág. 200 y sgtes.

[8] Castex, ob. cit., pág. 209.

[9] Palazzi, Pablo, *Los delitos informáticos en el Código Penal – Análisis de la ley 26.388*, Buenos Aires, Editorial Abeledo Perrot, 2016, pág. 89.

Estado tiene el deber de no practicar injerencias indebidas en el ámbito de la vida personal de cada uno de los integrantes de la comunidad organizada, al mismo tiempo que debe prevenir y reprimir los atentados por parte de funcionarios públicos o particulares contra esa zona de autonomía personal. (...) La privacidad como interés jurídicamente tutelado no se restringe al ámbito personal o familiar, sino que también incluye otros ámbitos sociales, en especial el de las relaciones laborales. En el marco de la moderna sociedad de la información, hoy ya se ha acuñado el término de ´autodeterminación informática´ para designar el derecho de toda persona de controlar el sentido y alcance de los datos sensibles que circulan por las redes telemáticas. No existe causal alguna de justificación que pueda legitimar en el estado actual de cosas la vigilancia informática de los dependientes, menos aún bajo el ropaje de un presunto derecho de control de la actividad empresarial. Si bien la privacidad es un bien jurídico disponible por parte de su titular, debe existir un marco regulatorio adecuado para evitar caer en excesos, en particular, cuando las relaciones laborales están signadas por una marcada desigualdad entre el empleador y el empleado. Cualquier medida de injerencia en el ámbito personal del afectado debe estar autorizada judicialmente al mismo tiempo que dicha medida debe guardar relación de necesidad, idoneidad y proporcionalidad con lo injusto cometido y sospechado. Cualquier infracción al derecho de privacidad personal debe ser resarcida económicamente de manera adecuada, mientras que al Estado le corresponde el deber de adoptar las medidas necesarias para evitar que la intimidad de las personas en un Estado social y democrático de derecho sea objeto del escrutinio público.[10]

Por otro lado –recientemente–, se sancionó la Ley N° 27.555, dicha ley establece el régimen legal del teletrabajo, y regula genéricamente la cuestión de la privacidad de los trabajadores con respecto a los datos generados en su actividad laboral. En su artículo 15, obliga a los empleadores a: "los sistemas de control destinados a la protección de los bienes e informaciones de propiedad del empleador deberán contar con participación sindical a fin de salvaguardar la intimidad de la persona que trabaja bajo la modalidad de teletrabajo y la privacidad de su domicilio".

[10] Aboso, ob. cit., pág. 215.

A continuación, en el art. 16, también se establece: *el empleador deberá tomar las medidas que correspondan, especialmente en lo que se refiere a* software*, para garantizar la protección de los datos utilizados y procesados por la persona que trabaja bajo la modalidad de teletrabajo para fines profesionales, no pudiendo hacer uso de* software *de vigilancia que viole la intimidad de la misma.*

A nivel nacional, la falta de una legislación que determine con toda claridad cómo deben afrontarse y resolverse estas colisiones de derechos, obliga con frecuencia a los interesados a acudir a los tribunales, en busca de respuestas y soluciones. En la práctica y como se verá más adelante, los problemas que genera ese vacío normativo son resueltos por la jurisprudencia, que en algunas ocasiones viene a zanjar los planteos de empleados y empleadores.

En el derecho comparado, también ha sido abordada esta problemática desde las distintas aristas que ofrece y se han ensayado, en consecuencia, soluciones de diversa índole con el propósito de resolverla.

España se encontraba en una posición similar a la de nuestro país, y el debate relativo a la posibilidad de acceso a las comunicaciones de los dependientes no se encuentra claramente abordado por la normativa, siendo las cortes, las llamadas a resolver, en caso de conflicto.

Tan es así, que desde la doctrina se señala: *...son varias las teorías y argumentos esgrimidos por nuestros tribunales para posicionarse a favor o en contra de los ´registros´ informáticos. 2. a) Teoría de la prevalencia del poder de control y vigilancia Los pronunciamientos judiciales que admiten con carácter general la validez de las pruebas obtenidas por medio de la monitorización de los ordenadores de la empresa sin necesidad de previa autorización judicial parten de la premisa de que los equipos informáticos son herramientas de trabajo propiedad del empresario (Sentencia del Tribunal Superior de Justicia de Murcia de 15.6.1999, AS.2504). Al empleador le asiste, al amparo de lo previsto en el artículo 20.3 ET, un derecho a supervisar la recta utilización de tales instrumentos, así como la correcta ejecución del trabajo por parte de sus empleados. De ahí que el empresario pueda adoptar las medidas que estime pertinentes para vigilar la correspondencia electrónica de sus empleados. Las sentencias que optan por esta interpretación, como es el caso de la del Tribunal Superior de Justicia de Cataluña de 9.7.2002 (AS.2811), y 5.7.2000 (AS.3452) niegan el carácter de correspondencia privada a los e-mails recibidos y/o enviados por los trabajadores y, por tanto, excluyen los mismos del ámbito de aplicación del artículo 18.3*

de la Constitución. 2. b) Tesis de la extensión del secreto de las comunicaciones. En otros casos, los tribunales han defendido tajantemente la naturaleza del correo electrónico como comunicación a la que resulta extensivo el Derecho constitucional al secreto de las mismas. De lo que resultaría que "solo con autorización judicial podrá violarse el secreto de tales comunicaciones" (sentencia del Juzgado de lo Social nº 3 de Vigo de 29.4.2001, AS.3563) Puesto que las pruebas que pudieran obtenerse violentando los derechos o libertades fundamentales no surtirían efecto alguno (artículo 11.1 de la Ley Orgánica del Poder Judicial), defender la falta de legitimidad del empresario para acceder al correo electrónico de los trabajadores, por atentar contra el Derecho al secreto de las comunicaciones, lleva aparejado que las pruebas así obtenidas carezcan de eficacia en juicio. En este sentido se pronuncian las sentencias de los Tribunales Superiores de Justicia de Andalucía 25.2.2002 (AS.562); y de Madrid de 31.1.2002 (AS.916). 2. c) Teoría ecléctica. No faltan ejemplos tampoco de pronunciamientos judiciales que, aun negando que el artículo 20.3 ET faculte al empresario para llevar a cabo indiscriminadamente controles de los e–mails de sus empleados, admiten la licitud de los mismos sin mediar previa autorización judicial siempre y cuando concurran una serie de requisitos. Esta es la solución por la que se decantan la sentencia del Juzgado de lo Social nº 3 de Vigo de 29.4.2001 (AS.3563) y de la sentencia del Tribunal Superior de Justicia de Galicia de 4.10.2001 (AS.3366), que aplicando los criterios sentados por el Tribunal Constitucional en su sentencia 186/2000, de 10 de julio, consideran que para que el empresario pueda registrar el correo electrónico de sus empleados es preciso "que se dé una triple característica de idoneidad, necesidad y proporcionalidad" en cuanto a las medidas de control y vigilancia adoptadas por el empresario. Concurriendo tales requisitos, el correo electrónico de los empleados podrá ser supervisado sin incurrir en vulneración de Derecho Fundamental alguno y, por tanto, las pruebas así obtenidas podrán ser admitidas en juicio.[11]

[11] Sánchez-Rodas Navarro, Cristina, "Información y Derecho: Restricciones en el uso del correo electrónico e Internet por parte de los trabajadores por cuenta ajena", en Información, Libertad y Derechos Humanos. La enseñanza de la Ética y el Derecho de la Información, 2° Congreso Internacional de Ética y Derecho de la Información, disponible en https://eprints.ucm.es/id/

Sin perjuicio de lo anteriormente señalado, pareciera haberse producido una evolución a nivel legislativo que ha inclinado la balanza hacia una postura en particular.

En primer lugar, desde el punto de vista normativo, el punto 3° del artículo 18 de la Constitución Española establece: *se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*

Independientemente de ello, pareciera que las modificaciones jurisprudenciales –como se verá oportunamente– y normativas en cuanto a las facultades del empleador respecto los mails corporativos, vienen acompañadas de la entrada en vigor en el marco de la Comunidad Europea del Reglamento General de Datos Personales (que entrara en vigencia el 25 de mayo de 2018 y fuera sancionado por el Parlamento Europeo y el Consejo, el 27 de abril de 2016 – Reglamento (UE) 2016/679).

Este contiene previsiones con respecto al tratamiento de los datos personales de los empleados que impactan, de alguna manera, en la temática en tratamiento.

Así, el artículo 88 de dicho Reglamento prevé: *Tratamiento en el ámbito laboral: 1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral. 2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales*

---

eprint/6128/1/definitivo2.pdf. Valencia, 2005.

dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo. 3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.[12]

De la mano de esta normativa comunitaria, España incluyó modificaciones en la Ley del Estatuto de los Trabajadores en la cual se previeron normas que otorgan a los empleadores facultades de control y organización de sus dependientes, para observar el cumplimiento desus obligaciones u para otros fines.[13] Esta disposición se encuentra limitada por el art. 20 bis de dicho Estatuto, el cual menciona que: *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión. Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de*

[12] Texto disponible en https://eur–lex.europa.eu/legal–content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1617124275737
from=EN#d1e3596–1–1

[13] Boletín Oficial del Estado, Real Decreto Legislativo 2/2015, Ley del Estatuto de los Trabajadores (BOE–A–2015–11430). "Artículo 20. Dirección y control de la actividad laboral. 1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien este delegue. 2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquel en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe. 3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad. 4. El empresario podrá verificar el estado de salud del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones".

dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.[14]

Por su parte, la Ley de Protección de Datos Personales y Garantías de los Derechos Digitales[15] –LOPD– contiene, en su artículo 87 especificaciones respecto las facultades del empleador. Dicha normativa reza: *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. 1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador. 2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos. 3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.*

En cierta medida, estas nuevas líneas normativas han impactado en las decisiones jurisprudenciales –como se verá al momento de analizar los fallos relevantes– difiriendo los límites al control empresarial, dependiendo de la naturaleza o condición otorgada por el empresario a los dispositivos digitales (esta diferencia radica en si se da o no autorización para el uso privado de estos).

Alemania, por su lado, abordó esta temática analizada de una manera similar, haciéndolo a través de su normativa y especificando en

[14] Ley del Estatuto de los Trabajadores, añadido por la disposición final 13 de la Ley Orgánica 3/2018 del 05/12/2018. BOE-A-2018-16673.
[15] Ley Orgánica 3/2018 consultar en EDL 2018/128249

qué circunstancias el empleador cuenta con las facultades de control sobre el correo electrónico corporativo de los empleados y bajo qué pautas debe procederse, debiendo analizarse la cuestión, a la luz de dos normas distintas.

La normativa específica de la materia traída a estudio parte de los derechos básicos reconocidos en la Ley Fundamental para la República Federal de Alemania, de la cual se desprende el derecho a la *autodeterminación informática* como constitutivo del derecho a la privacidad –conforme el art. 2°, par. 1 en consonancia con el art. 1°, par. 1°[16]–, derecho base de la normativa que especifica las facultades del empleador y del empleado en relación con el control de la actividad laboral.[17]

De acuerdo con la normativa específica aplicable, hay que diferenciar –por un lado– aquellos supuestos en los que el empleador autoriza el uso personal de internet o el mail corporativo a sus empleados, de aquellos supuestos en los que dicho uso no se encuentra permitido.

Así pues, en el primer supuesto, las agencias de protección de datos alemanas consideran al empleador como un proveedor de servicios de telecomunicaciones y se ven alcanzados no solo por el Acta Federal de Protección de Datos (*Bundesdatenschutzgesetz*[18], en adelante BDSG), sino también, por el Acta de Telecomunicaciones

[16] Ley Fundamental: "I. Derechos básicos Artículo 1. Dignidad humana – Derechos humanos – Fuerza jurídica de los derechos fundamentales. (1) La dignidad humana es inviolable. Respetarla y protegerla es el deber de toda autoridad estatal. (2) Por ello, el pueblo alemán reconoce los derechos humanos inviolables e inalienables como base de toda comunidad, de la paz y de la justicia en el mundo. (3) Los siguientes derechos fundamentales obligan al poder legislativo, al ejecutivo y al judicial como derecho directamente aplicable. Artículo 2. Libertades personales. (1) Toda persona tiene derecho al libre desarrollo de su personalidad siempre que no atente contra los derechos de los demás o contra el ordenamiento constitucional o la ley moral. (2) Toda persona tiene derecho a la vida y a la integridad física. La libertad de la persona será inviolable. Estos derechos solo podrán ser vulnerados en virtud de una ley". Ver https://www.gesetze–im–internet.de/englisch_gg/englisch_gg.html#p0023.

[17] Kamman, Janis, "Germany: Employment & Labour: Laws and Regulations 2021". Consultar en https://iclg.com/practice–areas/employment–and–labour–laws–and–regulations/germany.

[18] Consultar en https://www.gesetze–im–internet.de/bdsg_2018/

(*Telekommunikationsgesetz*[19], en adelante TKG) y el Acta de *Telemedia* (*Telemediengesetz*[20], en adelante TMG).

Asimilándose, entonces, a un proveedor de servicios, el empleador no cuenta con facultades de monitoreo –como regla general– y se encuentra sujeto al principio legal de inviolabilidad de las telecomunicaciones, siendo, en caso de que se determinara que hubo una violación a este, pasible de sanciones penales.[21] En este sentido, la TMG específi-

[19] Ver en https://www.gesetze–im–internet.de/tkg_2004/

[20] Disponible en https://www.gesetze–im–internet.de/tmg/

[21] Artículo 206. Violación del secreto postal o de las telecomunicaciones: "(1) Quien, sin estar autorizado para ello, comunique a otra persona hechos que estén sujetos al secreto postal o de telecomunicaciones y que hayan llegado a su conocimiento en calidad de propietario o empleado de una empresa que se dedique a la prestación de servicios postales o de telecomunicaciones, incurrirá en una pena de prisión de hasta cinco años o en una multa. (2) Quien, en calidad de propietario o empleado de una empresa indicada en el apartado (1), sin estar autorizado para ello. 1. abra un envío de correo precintado que haya sido confiado a dicha empresa para su entrega o tenga conocimiento de su contenido utilizando medios técnicos y sin romper el precinto, 2. suprima un envío confiado a dicha empresa para su entrega o 3. permita o fomente una de las actividades descritas en el apartado (1) o en los números 1 o 2 incurrirá en la misma pena. (3) Los apartados (1) y (2) también se aplican a las personas que 1. realicen tareas de supervisión sobre una de las empresas designadas en el apartado (1) 2. sean encargadas por dicha empresa o con su autorización de prestar servicios postales o de telecomunicaciones o 3. tengan encomendada la producción de instalaciones que sirvan al funcionamiento de dicha empresa o la realización de trabajos en la misma. (4) El que, sin estar autorizado para ello, comunique a otra persona hechos de los que haya tenido conocimiento en su calidad de funcionario público que trabaja fuera del servicio postal o de telecomunicaciones en virtud de una violación autorizada o no del secreto postal o de telecomunicaciones, incurrirá en una pena de prisión de hasta dos años o en una multa. (5) Los demás datos relativos al correo recibido por personas concretas, así como el contenido de los envíos postales, están sujetos al secreto postal. El contenido de las telecomunicaciones y sus detalles, en particular el hecho de que alguien haya participado o esté participando en un proceso de telecomunicaciones, están sujetos al secreto de las telecomunicaciones. El secreto de las telecomunicaciones se extiende también a los detalles relativos a los intentos infructuosos de establecer una conexión" – Código Penal de la República Federal de Alemania consultar en https://www.gesetze–im–internet.de/englisch_stgb/englisch_stgb.html#p1854

camente impide que los proveedores de servicios de telecomunicaciones –en este caso, los empleadores–, procesen información relacionada con los accesos de los individuos a los sitios web, por ejemplo.

Bien, la situación difiere en los casos en los que el empleador no autoriza el uso de internet o mail corporativo para fines privados. En este supuesto, está facultado a realizar actividades de monitoreo, pero dentro de los parámetros especificados por el marco normativo dado por la BDSG, la Agencia Federal de Protección de Datos y, en su caso, las agencias regionales (estas últimas como agentes gubernamentales de control, formulan consideraciones y guías de interpretación que, si bien no son obligatorias, sirven como pautas de entendimiento).

Al igual que sucede en el supuesto español, las previsiones del Acta Federal de Protección de Datos (BDSG) se encuentran alienadas con la normativa del Reglamento General de Protección de Datos de la Comunidad Europea (RGPD). Así, el artículo 26 de la BDSG proporciona las claves fundamentales para comprender los alcances de las facultades que tiene el empleador, a la hora de recolectar y procesar la información personal de los empleados con el fin de efectuar un monitoreo.

En este sentido, la BDSG permite al empleador recolectar, procesar y utilizar los datos personales del empleado a los fines de la relación de trabajo, cuando sea necesario para decidir su contratación, bien para su despido o la finalización del contrato laboral.

Asimismo, el empleador solo podrá recolectar, procesar y utilizar la información personal de sus empleados a fin de detectar la comisión de algún delito, cuando se de la siguiente condición: haya una razón documentada para creer que el empleado cometió un delito mientras se encontraba bajo la relación laboral, siempre que la recolección, procesamiento y uso de esos datos sean necesarios para investigar el crimen y –siempre y cuando– no exista un interés superior del empleado que se imponga al del empleador. A su vez, esta normativa exige que el tipo de información y su extensión deben guardar la debida proporción con el propósito buscado al procurar su obtención.

No obstante, esta facultad se ve limitada por el mismo art. 26 del BDSG, el cual especifica que no se aplica para justificar el monitoreo del empleado, si este no es necesario para la contratación, el desempeño o la finalización del contrato de trabajo o bien, para investigar un delito ya cometido.

Sin perjuicio de ello, en el supuesto de que este artículo no se aplicara, el empleador puede –en ciertos casos– justificar el monitoreo del

empleado bajo las previsiones del art. 6 del RGPD. Este último permite entre otras medidas– el procesamiento de los datos cuando sea necesario para salvaguardar el interés legítimo del empleador, siempre y cuando, las circunstancias particulares no lleven a que se deba imponer el derecho a la privacidad del empleado por sobre el derecho del empleador.

En estos supuestos en los que el principio es la facultad de monitoreo del empleador, la normativa germana no exige que el empleado preste un consentimiento al respecto; no obstante, como se indicó, cuando el principio se invierte y el empleador autoriza el uso privado de los servicios –y la normativa a aplicar es aquella que emerge de la TMG y de la TKG–, aun en ese supuesto, el empleado puede prestar consentimiento y en este caso, continuar haciendo uso del sistema de telecomunicaciones y sujeto ello a las condiciones establecidas por el empleador o bien, no prestar su consentimiento y absteniéndose de dar un uso personal al sistema de telecomunicaciones.

Como se mencionó, el Acta de Protección de Datos alemana se complementa con lo dispuesto por la normativa de la Comunidad Europea. En relación con ello, específicamente, el RGPD indica que tanto los empleados como aquellas personas ajenas a la relación laboral pero que se ven afectadas, de alguna manera, por el monitoreo que efectúa el empleador, cuentan con diversos derechos ante la situación de control de los datos personales, entre otros: previa notificación de esta circunstancia, la oportunidad de objetar el monitoreo bajo ciertos supuestos, la oportunidad de restringir el procesamiento de sus datos personales, en determinados casos, el acceso a los registros de monitoreo y la oportunidad de solicitar su rectificación o borrado.

Particularmente, en relación con estos puntos, la jurisprudencia alemana ha abordado nuestra temática en forma circunstancial, analizando supuestos que van más allá del mero acceso del empleador a los mails corporativos.

En cuanto aquí interesa, en un fallo[22] dictado por la Suprema Corte Regional de Trabajo de Baden–Wurtemberg, en junio de 2018, se con-

[22] LArbG Baden–Württemberg Urteil vom 6.6.2018, 21 Sa 48/17http://lrbw.juris.de/cgi–in/laender_rechtsprechung/document.py?Gericht=bw&GerichtAuswahl=Arbeitsgerichte&Art=en&Datum=2018–6&n-

sideró válida la evidencia digital recolectada que acreditaba un incumplimiento a la relación contractual por parte del empleado, aun cuando dicho incumplimiento fue descubierto por accidente durante una búsqueda en los dispositivos utilizados por este mismo.

En el caso bajo estudio, el empleador (demandado) finalizó el contrato de trabajo con el empleado (demandante) basado en una fuerte sospecha de fraude en torno a la provisión de nafta que el empleado utilizaba para el automóvil que la compañía le había puesto a su disposición. Esta sospecha se originó en datos encontrados en la *laptop* de la compañía utilizada por el empleado –que fuera voluntariamente entregada por este para que pudiera ser inspeccionada– mientras se llevaba adelante una investigación interna respecto de otro empleado que había enviado a terceros un email que contenía información confidencial de la demandada.

La Corte Regional entendió que el empleador no tenía *per se* una causa probable para justificar la búsqueda en la *laptop* de la compañía, dada la esfera de privacidad del demandante –más teniendo en cuenta que dicho empleado tenía permitido el uso para fines particulares del dispositivo que le proveyó la compañía y el empleador no tenía el consentimiento del empleado para efectuar la búsqueda–, lo cual entrañaba una violación a la antigua Ley de Protección de Datos alemana (vigente al momento de los hechos), no pudiendo tomarse como un consentimiento válido –a los fines de la investigación del fraude de la nafta– el hecho de que el demandante indicara que prestaría colaboración, a los fines de la investigación interna seguida contra el otro empleado.

Pero, sin perjuicio de ello, la Corte entendió que el demandado podía hacer uso de la información encontrada accidentalmente en las medidas legales tomadas en contra del demandante.

Para resolver así, los jueces sostuvieron que los datos recolectados solo pueden ser invalidados como evidencia en la Corte, si su recolección constituye una interferencia injustificada en el derecho a la privacidad del demandante. Si se está o no ante este supuesto, deberá determinarse en casa caso particular, balanceándose los intereses de la persona afectada con los de la necesidad de que exista un buen funcionamiento en la administración de justicia.

---

r=25844&pos=3&anz=4.

En el caso analizado, la corte entendió que el derecho a la privacidad del demandante se presentaba de forma subsidiaria a la necesidad de contar con una buena administración de justicia. Particularmente, esta decisión se basó en el hecho de que el demandante había entregado su *laptop* de manera incondicional, había manifestado su voluntad de colaborar y proveer de la información necesaria aportando los *passwords* y la búsqueda se llevó a cabo de forma abierta, sabiendo el demandante que cualquier dato que había en su dispositivo podía ser descubierto.

Otra pauta tenida en cuenta para convalidar el uso de la evidencia obtenida fue que el derecho a la privacidad del empleado se encontraba protegido por el código de uso de los dispositivos IT del empleador y las guías allí contenidas; asimismo, se entendió que cualquier dato privado personal podría haber sido resguardado por el empleado de una forma tal que podría haber evitado al empleador acceder a él.

En otro orden de ideas, y en relación con las facultades de control del empleador sobre los dispositivos de los empleados (y, por ende, lo allí contenido), el Tribunal Federal del Trabajo (BAG), en un fallo[23] dictado el 27 de julio de 2017, resolvió que la instalación y el uso de un *software "keylogger"* viola la normativa de protección de datos alemana y el derecho constitucional del empleado a la autodeterminación.

En el caso, el Tribunal destacó que las previsiones del art. 32 (1), segundo párrafo del Acta Federal de Protección de Datos no puede justificar la recolección, procesamiento y el uso de la información personal del empleado obtenida a través de un *software keylogger*; esta norma permite la recolección y el uso de datos de los empleados si existen hechos fácticos y documentados vinculados con la comisión de un delito mientras prestaban funciones laborales, siempre y cuando la recolección, el procesamiento y el uso de los datos sea necesario para la investigación de ese delito y cuando el interés legítimo del empleado no prevalezca.

En el caso bajo estudio, el empleador no tenía ninguna indicación ni fáctica ni documentada –antes del uso del *software*– que pudiera

[23] BUNDESARBEITSGERICHT Urteil vom 27.7.2017, 2 AZR 681/16 ECLI:DE:BAG:2017:270717.U.2AZR681.16.0 disponible en https://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&Datum=2017-7&nr=19516&pos=2&anz=34.

haberle dado una sospecha suficiente de que el empleado estaba cometiendo una grave violación a sus deberes contractuales. Por lo cual, se resolvió desestimar la evidencia presentada obtenida a partir de este *software*, teniendo en cuenta el respeto por el derecho constitucional a la autodeterminación del empleado (Art. 2.1 en conjunción con el art. 1 de la Ley Fundamental alemana).

Por último, vale la pena mencionar un fallo del Tribunal Regional de Trabajo de Berlín-Brandemburgo[24], donde se sostuvo que un empleador tenía derecho a controlar el uso de internet de un empleado sin su consentimiento y que el uso personal excesivo de la web por parte del empleado justificaba el despido inmediato.

En el caso, el dependiente tenía a su disposición una computadora laboral que, según la política de la empresa, solo podía utilizarse para fines laborales. No obstante, el empleado estaba autorizado a utilizar internet con fines privados en casos excepcionales y durante sus descansos.

A partir de información recibida por parte de otro dependiente, el empleador tomó conocimiento de que el empleado hacía un uso privado excesivo de esta autorización excepcional. Así las cosas, al constatar el enorme volumen de datos implicado en ese uso irregular de la herramienta informática, el empleador despidió con causa al empleado

Tras el despido, el empresario evaluó el historial de navegación del empleado sin su consentimiento y descubrió que aquel había utilizado internet con fines privados durante aproximadamente 40 horas en solo 30 días laborables, abriendo páginas web más de 16 000 veces.

El empleado impugnó el despido alegando que su historial de navegación no podía ser controlado sin su consentimiento y que, por tanto, ese registro debía ser excluido del juicio.

El Tribunal Superior de Trabajo dictaminó que el despido con causa era legalmente efectivo dada la extrema violación de los deberes del empleado.

Sostuvo que, si bien, el dependiente no dio su consentimiento para evaluar el historial de navegación como datos personales en el sentido de la Ley Federal de Protección de Datos (*Bundesdatenschutzgesetz*), las pruebas podían utilizarse en el caso en cuestión. La Ley permite

[24] Fallo que puede consultarse en https://openjur.de/u/872845.html.

básicamente almacenar y evaluar los historiales de navegación para controlar cualquier conducta abusiva –incluso– sin el consentimiento del empleado.

En opinión de los jueces, la justificación concreta del accionar del empleador se encuentra en el art. 32 de la Ley Federal de Protección de Datos, según el cual, los datos personales de los empleados pueden ser recogidos, procesados y utilizados para fines concernientes a la relación laboral, entre otras cosas, si es necesario para tomar la decisión de ponerle fin a ese vínculo.

Si bien la relación laboral ya había finalizado cuando el empresario evaluó el historial de navegación, esta justificación era aplicable –según el Tribunal de Justicia– para el supuesto en que el empleador debiera recabar, dar tratamiento y hacer uso de datos personales a los fines de demostrar y probar el uso incorrecto, durante el procedimiento de despido.

A su vez, se ponderó que el empleador no tuvo otro medio igualmente eficaz pero menos lesivo para comprobar el uso abusivo de internet por parte del empleado. En el caso que nos ocupa, el empresario no tenía otra opción que acceder a la información del *browser*.

Finalmente, debemos referirnos a la situación que se plantea en los Estados Unidos de Norteamérica, en torno de las cuestiones que venimos abordando.

En primer lugar y desde el punto de vista normativo, debe tenerse presente la Cuarta Enmienda[25], la cual protege el derecho a la intimidad y a las comunicaciones privadas de los ciudadanos.

Para ampliar un poco el panorama normativo, deben traerse a colación las disposiciones de la *Electronic Communications Privacy Act*[26] –en adelante ECPA– la cual, a primera vista, veda la posibilidad de interceptar las comunicaciones de los empleados por parte del empleador.

---

[25] Amendment IV: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seize".

[26] Texto disponible en https://www.congress.gov/bill/99th–congress/house–bill/4952.

No obstante, debe repararse en algunas excepciones allí contenidas, porque pueden tener impacto en el tema analizado.

En primer lugar, está la excepción de *negocios*, que permite al empleador interceptar las comunicaciones electrónicas de sus dependientes, siempre que haya un motivo comercial o de negocios legítimo para hacerlo.

En segundo lugar, está la excepción *por consentimiento*, en virtud de la cual el empleador puede interceptar esas comunicaciones electrónicas, si el empleado le da su consentimiento para hacerlo.[27]

Un detalle no menor es el hecho de que el ECPA define a las comunicaciones electrónicas como cualquier mensaje electrónico que se está transmitiendo, y si bien dicha normativa no define el término "interceptar", se entiende que se hace referencia a la captación en tiempo real de una comunicación, a diferencia de aquella que implica acceder a una comunicación que se encuentra almacenada.

En este último supuesto debe recurrirse a la *Federal Storage Communications Act* para encontrar regulaciones referidas a las facultades del empleador con respecto a las comunicaciones almacenadas.[28]

Como supuesto de excepción, dicha normativa no sanciona el acceso a las comunicaciones que fueran almacenadas, en los casos que el empleador le hubiera proporcionado el servicio de comunicaciones, siempre y cuando estas no sean almacenadas en otro sistema que no sea el del empleador.[29]

Por otro lado, existen previsiones normativas particulares, que exigen el monitoreo de las comunicaciones de ciertos empleados, dependiendo de lo sensible de la información a la cual pueden acceder. Algunos ejemplos de obligaciones de monitoreo que surgen de otras leyes y regulaciones, pueden hallarse en aquellas correspondientes a la Agencia Federal de Comercio –en este caso, incluso se dispone el control sobre las comunicaciones de los empleados que hacen uso de las redes sociales del trabajo para conectarse con posibles clientes–, o

[27] Ver https://www.americanbar.org/news/abanews/publications/youraba/2018/january–2018/how–much–employee–monitoring–is–too–much–/.

[28] Ver en https://www.law.cornell.edu/uscode/text/18/part–I/chapter–121

[29] Información disponible en https://mcdonaldhopkins.com/Insights/April–2018/Employment–Law–QA–May–I–monitor–an–employees–email

en la Autoridad de Regulación de la Industria Financiera, que establece la posibilidad de monitorear las comunicaciones de los *brokers* con el público, ya sea vía email, mensajería instantánea o a través de las redes sociales.

Paralelamente, existen regulaciones locales. Algunos estados como Arkansas, Illinois, Michigan, Missouri, Carolina del Norte, Oklahoma, Carolina del Sur y Dakota del Sur han impuesto la obligación –a través de normas estatutarias– de requerir a los trabajadores de las tecnologías de la información, que se reporten comunicaciones a través de las cuales se hubiese cursado información relacionada con pornografía infantil y que fuera encontrada en computadoras que ellos están atendiendo.

Se procederá, a continuación, a analizar las decisiones jurisdiccionales más destacadas de los antecedentes normativos traídos a análisis.

XIII. b. Jurisprudencia argentina

XIII. b. 1. Fuero Federal

Juzgado Federal No. 12. Sala I. Causa N° 753, caratulada "Caballero, Florencio Oscar s/rechazo de nulidad". 6 de agosto de 2009

El presente caso resuelto por la Cámara Federal de Apelaciones en lo Criminal y Correccional de la Capital Federal, donde convalidó la nulidad decretada por el juez de grado y que fuera apelada por la querella. El caso penal se inició a raíz de que se presentaran como prueba de cargo una serie de e-mails –supuestamente– pertenecientes al imputado que fueron acercados en forma anónima sin consentimiento y/o autorización de este.

La Cámara, en primer término, resaltó que no se podía afirmar que los contenidos plasmados en los supuestos correos hayan constituido comunicaciones privadas vía correo electrónico, ni que en caso de que trataran de tales, se las haya obtenido de forma ilegítima. Esto, debido a que la prueba presentaba se trataba de transcripciones –de tipo copiar y pegar– que ni siquiera contaban cuerpo de correo electrónico.

Asimismo, adujo que *aun en el caso de que pueda verificarse que se trató de información obtenida a través de alguna "cuenta" de correo*

electrónico, no puede descartarse que haya sido aportada por alguno de los interlocutores del imputado, sin que la referencia del apelante en torno a su gran cantidad lleve de por sí a descartar esa hipótesis. Adviértase que lo contrario implicaría la posibilidad de supeditar la validez de un proceso penal a un juicio conjetural o hipotético relativo a eventuales actividades ilegítimas de las cuales no se tiene prueba.

XIII. b. 2. Fuero nacional

Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VII. Causa N° 35.369. caratulada "ABREGU, Carlos Alejandro s/ nulidad". 09 de octubre de 2008

La parte querellante articuló un recurso de apelación con el fin de impugnar la decisión del juez de grado, quien había dictado el sobreseimiento de la persona acusada, tras decretar la nulidad de la incorporación de un acta notarial relacionada con distintos correos electrónicos enviados y recibidos por aquella, los cuales entrañaban el supuesto desvío de información confidencial de la sociedad anónima que se consideraba damnificada.

Los jueces señalaron, con remisión a dos precedentes jurisprudenciales de esa Cámara de Apelaciones: *a partir de sus características propias, el correo electrónico goza de una protección de la privacidad más acentuada que la clásica vía postal, desde que para su funcionamiento y utilización se requiere indispensablemente de un prestador del servicio, el nombre de usuario y clave de acceso destinados, sin duda alguna, a impedir que terceros extraños se entrometan en los datos y contenidos que se emiten y reciben (de esta Cámara, Sala VI, causa ´Lanata, Jorge´, del 4-3-1999 y de esta Sala, causa en 33.649, ´Falik, Flavia´, del 7-4-2008).*

Luego indicaron que, independientemente de que los correos electrónicos revisados hubiesen sido remitidos a través del servidor del empleador del imputado, no era posible soslayar que todos ellos lo habían tenido a él como emisor o destinatario –indistintamente–, y que la propia querella se refirió al correo personal del acusado, cuando quiso aludir a la dirección de correo electrónico que le había sido asignada dentro de la compañía.

Por este motivo consideraron: *...con la incorporación de las probanzas relativas a los correos electrónicos del imputado se transgredió el ámbito de su privacidad con la consecuente afectación de su dignidad y autodeterminación*, amparados por los artículos 18 y 19 de la Constitución Nacional.

Al igual que cuanto sucede con las comunicaciones telefónicas, la Sala sostuvo –con cita de otro de sus precedentes (causa n° 31.743, *"Robles, Fernando y otros"*, del 6 de julio de 2007)– que su protección *...encuentra andamiento en las previsiones contenidas en los instrumentos de derechos humanos relativas al derecho de toda persona a la vida privada y a la inviolabilidad de su correspondencia*, en los términos establecidos en los artículos X de la Declaración Americana de los Derechos y Deberes del Hombre, 12 de la Declaración Universal de Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos y 11.1 y 11.2 de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), en función de lo dispuesto en el inciso 22, del artículo 75 de nuestra Carta Magna.

El tribunal confirmó que, ninguna duda cabía acerca de que la correspondencia electrónica que estaba siendo analizada, había sido emitida o bien destinada al imputado, su intimidad se había visto invadida por un particular –en este caso, su empleador–, valiéndose de un método que no se encontraba legitimado por el Estado, es decir, fuera de los excepcionales supuestos, taxativamente previstos en que una injerencia semejante puede ser autorizada por alguna de sus agencias, procurando asegurar la protección del bien común.

En esas condiciones y no contándose en el legajo con un cauce válido e independiente que permitiese continuar la investigación, los jueces confirmaron la decisión del juez de la instrucción del sobreseimiento del acusado.

Cámara de Apelaciones en lo Criminal y Correccional de la Capital Federal. Sala VI -Causa N° 39.427, caratulada "R., R y otros s/nulidad – archivo–costas". 14 de junio de 2010

El hecho que originó esta resolución de la Cámara dio inicio en un procedimiento de *back–up* de las computadoras de los empleados de la empresa, en las que observaron que dos empleados –imputados– captaban proyectos de la empresa y los comercializaban como propios a través de otra sociedad. La actividad que realizaban en esta empresa

era idéntica a la de su empleador. Los empleados fueron imputados por administración fraudulenta y violación de secretos, pero fueron absueltos en primera instancia por decretarse la nulidad de correos como prueba de cargo y la querella apeló dicha decisión.

Antes de resolver la apelación la Cámara sostuvo: *La naturaleza de la denuncia impone que fijemos determinados conceptos. El primero es que a un empleado se le asignan distintas "herramientas laborales" dentro de las que se encuentran computadoras personales, portátiles y cuentas de correo electrónico, entre otras que no interesan en el tratamiento del tema que nos ocupa. Junto a ellos se le proporciona una clave o "password" que le garantiza confidencialidad en sus comunicaciones y archivos personales, lo cual ya sugiere su carácter privado. Por tal motivo el ingreso a su contenido y su eventual utilización como prueba puede conculcar elementales garantías individua les, fundamentalmente de raigambre constitucional, que ya se han extendido a estos nuevos soportes aportados por la tecnología moderna.*

En este sentido, agregaron: *Solo cuando los controles sobre tal privacidad cuentan con el consentimiento previo del trabajador, el procedimiento puede tener validez jurídica (así se ha interpretado el artículo 70 de la Ley de Contrato de Trabajo). Se agregan otras exigencias a través de la jurisprudencia laboral pues, de obrarse subrepticiamente, se agredirá la intimidad sin razón anterior que la justifique. En el caso que nos ocupa tal exigencia parece estar claramente ausente.*

Asimismo, añadieron que la querella había admitido que en la empresa no existían reglas sobre el manejo de la información de tal manera de que el empleado no era notificado formalmente de que podían ser revisados, con lo existía una razonable expectativa a la privacidad. Así la Cámara afirm: *Acá no hay duda de que se violó esa expectativa de privacidad. Nada sabía el empleado de cuál era la posibilidad de invasión en su intimidad ni la modalidad de control que sobre sus tareas su empleador pretendía y que finalmente practicó al obtener, u acceder, al* backup *de la información contenida en los ordenadores de los imputado.*

Finalmente, confirmaron la sentencia apelada y agregaron: *A nuestro criterio entonces, los elementos de juicio aportados por la querella para dar sustento a la imputación fueron obtenidos a través de una intromisión en la privacidad, fundamentalmente porque nada se había establecido en relación con tal extremo como política de la empresa y que hubiese permitido a los empleados conocer, con la claridad que las normas citadas exigen, cuáles eran los límites a su intimidad.*

Cámara de Apelaciones de la Capital Federal. Sala I, Causa N° 41816 caratulada "Gotlib Rodolfo Saul y Otros". 13 de febrero de 2015

El caso que se analiza surge a raíz de la apelación presentada por querella en virtud de una sentencia de primera instancia que resolvió declarar la nulidad de una prueba obtenida de la correspondencia de un empleado. Así, se introdujeron al proceso como prueba de cargo los correos electrónicos del imputado, que fueron aportados por la querella, su empleador.

La Cámara –por mayoría con el voto de Bunge Campos al que otros de los camaristas adhirió– convalidó la sentencia de primera instancia, por cuanto entendió: *toda vez que se les asigna un usuario y una clave personal de ingreso, abandona el estado público y lo convierte en privado, impidiendo que los mensajes obtenidos a través de la intervención en el servidor del dominio puedan, al menos como se plantea en el caso, constituir prueba en contra de alguno de los propietarios del mensaje; es decir, de su remitente o su destinatario; pues ello no está permitido, incluso, en el ordenamiento civil (art. 1036 CC).*

La Cámara continuó argumentando que *el empleador tiene prohibido, en principio, leer e–mails enviados o recibidos por sus empleados. Y el contenido de tal prohibición no es otro que la violación del derecho de privacidad del trabajador, facultad que no comporta un elemento configurador del débito contractual y que, por ello, hace a la indiscutible e impenetrable dignidad y autodeterminación que como sujeto titulariza". (*in re*: Sala IV, causa 25.065, "Redruello, Fabián L. y otros", rta. 15/11/2004)*

En este sentido, el voto mayoritario afirmó *la averiguación de la verdad no puede erigirse como bastión del avasallamiento de derechos reconocidos por la Constitución Nacional, ni por parte de los particulares, ni del poder público, pues precisamente y como hilo conductor del principio de juicio previo, se despliega un abanico de garantías que limita al poder punitivo, en la materialización de ese cometido. Ello implica que la parte acusadora no puede justificar su actuación, por encima de las garantías, en el éxito de la investigación, pues allí entra en juego su propio interés... (in re: Sala I, causa 21.387, "Calleja, Marta Haydeé y otros", rta. 18/05/2005).*

Finalmente, el juez Bunge Campos restó importancia a los llamados códigos de ética firmados por el empleado afirmando: *en cuanto al mencionado código de ética que los empleados de la firma debían*

suscribir, conforme lo afirmaron las partes en la audiencia, debo decir que se trata, a mi juicio, de una típica cláusula de adhesión en la que el consentimiento no ha sido brindado de un modo libre y espontáneo, pudiendo resultar abusiva. En ese orden de ideas, debemos preguntarnos cuál es la validez a la luz del art. 18 de la CN de un consentimiento anticipado que, potencialmente, podría resultar en una autoincriminación. La hermenéutica en materia de derechos individuales nos obliga a adoptar la más amplia interpretación, por aplicación del principio pro hominem, por lo que no le asignaré virtualidad alguna.

En este sentido, la conclusión a la que arribó fue: *al momento de revisar los correos electrónicos del personal, la empresa carecía del "caso" por lo que tal intromisión carece de justificación alguna. Ello no quiere decir que se convalide la posición de la defensa de que se trató de una excursión de pesca, sino que se limita a la intromisión en los mails señalados. He dicho que "toda medida que implique un avance sobre los derechos individuales debe estar justificada primero por un caso* (cf."-Panóptico sin fronteras", en *Informática y delito*, INFOJUS-Asociación Internacional de Derecho Penal, 2014, p 153).

Asimismo, esta resolución tuvo una disidencia escueta en la que se sostuvo: *del debate producido en la audiencia es dable concluir que no se encuentra controvertido que todos los correos electrónicos aludidos fueron remitidos desde o dirigidos a casillas corporativas (con la extensión "pcda" por "[Marca de la firma]")*. Además, que de acuerdo con el código de ética de la compañía dichas casillas corporativas solo podían ser utilizadas para cuestiones laborales y su contenido estaba sujeto a supervisión de la dirección. Por último, que el imputado Grant conocía que debía notificarse formalmente del contenido de dicho código, el que se encontraba a disposición de todos los empleados en la intranet de la empresa.

El marco reseñado permite afirmar que las comunicaciones cursadas por esta vía carecían de una expectativa razonable de privacidad que pueda fundar válidamente la anulación recurrida.

Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala I, caratulada "Grant, Federico Guillermo s/incidente de nulidad". 13 de febrero de 2015

Interviene la Cámara del fuero a raíz del recurso de apelación interpuesto tanto por la defensa del imputado Grant, como así también por la querella contra la resolución del juez de grado que resolviera recha-

zar, por un lado, parte de las nulidades articuladas por la defensa y, por el otro, conceder la nulidad ordenando la exclusión del catálogo probatorio de los correos electrónicos aportados por la querella, sobre la base de los cuales la acusación privada sostenía que el imputado habría procedido a cerrar un negocio que un proveedor, en provecho propio, abusando de la confianza depositada en él.

Para así resolver, la Sala I entiende que carece de relevancia el proveedor de la cuenta de correo electrónico, ya que al momento de asignar al empleado un usuario y una clave personal de ingreso, abandona el estado público y lo convierte en privado, impidiendo de esta manera que los mensajes obtenidos a través de la intervención en el servidor del dominio puedan constituir prueba en contra de alguno de los propietarios del mensaje; es decir, su remitente o su destinatario.

Asimismo, se agrega que el código de ética –puesto en conocimiento al empleado– carece de relevancia dado que no dista demasiado a una cláusula de adhesión, en la que el consentimiento no se brinda libre y espontáneamente. Lo cual, a la luz del artículo 18 de la Constitución Nacional, podría resultar en una autoincriminación.

A esto último, se suma que el avance sobre los correos electrónicos que no se efectuó en el marco de un "caso", traza una analogía con el registro de las telecomunicaciones y refiere la necesidad de contar con la previa autorización de juez para llevar a cabo esa injerencia sobre los correos.

En el caso en cuestión se trata el correo electrónico laboral o corporativo, es decir, aquel suministrado por el empleador.

Es así que resulta relevante lo resaltado por el juez Luis María Bunge Campos quien, al momento de tratar la validez de los correos electrónicos aportados por la querella a la causa, refirió: *En este sentido, cabe preguntarse si el empleador, en el caso la parte querellante, tiene autorizado la intromisión en las cuentas de correo electrónicas que como parte de la actividad laboral proveyera al empleado y valerse del producto de esa intromisión para formular una denuncia, sin que ello resienta la garantía de inviolabilidad de la correspondencia prevista en el art. 18 de la Constitución Nacional, al carecer del control indispensable del órgano jurisdiccional.* Consideró: *no tiene relevancia quien sea el proveedor de la cuenta de correo electrónico, pues toda vez que se les asigna un usuario y una clave personal de ingreso, abandona el estado público y lo convierte en privado, impidiendo que los mensajes obtenidos a través de la intervención en el servidor del dominio pueda, al menos como se plantea en el caso, constituir prueba en contra de*

alguno de los propietarios del mensaje; es decir, de su remitente o su destinatario; pues ello no está permitido, incluso, en el ordenamiento civil (art. 1036 CC).

Sustentó tal postura con jurisprudencia propia de la Sala, la cual mencionaba: *…frente al argumento del querellante de que la documentación fuera encontrada en el lugar de trabajo de los imputados, cuadra inferir que en función de las previsiones normativas de los artículos 18 y 19 CN, no ofrece mayores reparos para una correcta resolución interpretativa: el empleador tiene prohibido, en principio, leer e-mails enviados o recibidos por sus empleados. Y el contenido de tal prohibición no es otro que la violación del derecho de privacidad del trabajador, facultad que no comporta un elemento configurador del débito contractual y que, por ello, hace a la indiscutible e impenetrable dignidad y autodeterminación que como sujeto titulariza (in re:* Sala IV, causa 25.065, …, rta. 15/11/2004).

En tal sentido, agregó: *la averiguación de la verdad no puede erigirse como bastión del avasallamiento de derechos reconocidos por la Constitución Nacional"; ya que, a partir del principio de juicio previo, se abre un abanico de garantías que ponen límite al poder punitivo. Motivo por el cual, la parte acusadora no puede justificar su actuación, por encima de las garantías, en el éxito de la investigación, pues allí entra en juego su propio interés…* (*in re*: Sala I, causa 21.387, "Calleja, Marta Haydeé y otros", rta. 18/05/2005).

Así las cosas, el Magistrado expresó: *si bien el empleador puede utilizar la información obtenida de los correos electrónicos ubicados en los servidores de una sociedad integrante del mismo* holding *empresario; lo cierto es que tal prueba debe ser incorporada –en materia penal– a la luz de un criterio riguroso de modo tal de no avanzar indebidamente sobre la privacidad del ciudadano.*

En relación con el código de ética que los empleados de la firma debieron suscribir, el camarista entendió que se trató de una cláusula de adhesión, en la que el consentimiento no fue brindado de forma libre y espontánea, pudiendo ser abusiva. Asimismo, se preguntó si tal consentimiento anticipado podría resultar en una autoincriminación a la luz del artículo 18 de la Constitución Nacional. Por lo cual, en aplicación del principio *pro hominem*, descartó la validez de aquel.

Posteriormente, señaló que el avance sobre el derecho a la privacidad no fue realizado en el marco de un caso, sino para determinar su existencia o no. Se valió –en tal sentido– de la falta de precisión de las

irregularidades manifestadas en el escrito de la denuncia, y que fueron las que originaron el ingreso del empleador a los servidores de correo electrónico de la empresa y consecuente accedo al de los empleados.

Sobre este punto, citó parte de la conclusión arribada en el fallo "Halabi" dictado por Corte Suprema de Justicia de la Nación, puntualmente: *este Tribunal ha subrayado que solo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen* (Fallos: 306:1892; 316:703, entre otros).

Seguidamente, refirió: *Es en este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado (confr. art. 236, segunda parte, del Código Procesal Penal de la Nación, según el texto establecido por la ley 25.760), de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas. Esta norma concuerda con el artículo 18 de la ley 19.798 que establece que 'la correspondencia de telecomunicaciones es inviolable. Su interceptación solo procederá a requerimiento de juez competente.'* Agregando el considerando siguiente que: *El Tribunal tiene dicho que los motivos que determinan el examen de la correspondencia en el caso de un delincuente, pueden diferir de los referentes a un quebrado, a un vinculado al comercio, a un sujeto de obligaciones tributarias, etc.; por ello ha interpretado que el art. 18 de la Constitución no exige que la respectiva ley reglamentaria deba ser única y general* (Fallos: 171:348; 318:1894, entre otros). Cabe recordar que en el precedente de Fallos: 318: 1894 (en el voto de los jueces Fayt, Petracchi y Boggiano) se afirmó: *para restringir válidamente la inviolabilidad de la correspondencia, supuesto que cabe evidentemente extender al presente, se requiere: a) que haya sido dictada una ley que determine los casos y los justificativos en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia; b) que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión; c) que la aludida restricción resulte un medio compatible con el fin legítimo propuesto y d) que dicho medio no sea más extenso que lo indispensable para el*

aludido logro. A su vez, fines y medios deberán sopesarse con arreglo a la interferencia que pudiesen producir en otros intereses concurrentes.

Por lo expuesto, el Magistrado concluyó que la intromisión careció de justificación. Para ello, se basó en la falta del "caso" por parte de la empresa, al momento de revisar los correos electrónicos. Asimismo, aclaró ello que no convalida la posición de la defensa en cuanto a que se trató de una excursión de pesca, sino que se limitó *a la intromisión en los mails señalados.* Y, agregó: *toda medida que implique un avance sobre los derechos individuales debe estar justificada primero por un caso" (cf. "Panóptico sin fronteras*, en *Informática y delito, INFOJUS–Asociación Internacional de Derecho Penal, 2014, p 153).*

Finalmente, resolvió que resultan válidas las declaraciones testimoniales –cuestionadas por la defensa– como así también lo sostenido por el juez de grado en los puntos I y II de su decisorio, en cuanto hizo lugar parcialmente a la nulidad de la inclusión de los correos electrónicos aportados por la querella.

Por otro lado, en su voto, el Juez Jorge Luis Rimondi manifestó su disenso con la opinión emitida por el Dr. Bunge Campos y declaró la validez de la incorporación de los correos electrónicos aportados por la querella.

El magistrado sostuvo: *es dable concluir que no se encuentra controvertido que todos los correos electrónicos aludidos fueron remitidos desde o dirigidos a casillas corporativas (con la extensión "pcda." por "[Marca de la firma]"). Además, que de acuerdo al código de ética de la compañía dichas casillas corporativas solo podían ser utilizadas para cuestiones laborales y su contenido estaba sujeto a supervisión de la dirección. Por último, que el imputado Grant conocía que debía notificarse formalmente del contenido de dicho código, el que se encontraba a disposición de todos los empleados en la intranet de la empresa.*

En el mismo orden de ideas, agregó que tales comunicaciones *carecían de una expectativa razonable de privacidad que pueda fundar válidamente la anulación recurrida; pues, al tratarse de casillas de correo corporativas, la información se encontraba alojada en servidores dependientes de la compañía. Por tal circunstancia, los empleados tuvieron conocimiento que su uso era solo para comunicaciones laborales –sujetas a supervisión superior– y, asimilable su contenido al concepto de papeles privados constitucionalmente tutelados.*

En este sentido, expuso el camarista: *es dable afirmar que hubo una renuncia tácita a cualquier mínima expectativa de privacidad que pu-*

dieron haber guardado en su ánimo los imputados; y, concluye –respecto a la hipótesis delictiva en cuestión– que *el hecho no habría acaecido tal y como ocurrió si las comunicaciones hubiesen salido desde casillas particulares de los imputados; así, si albergaban alguna infundada expectativa de privacidad habrían debido de renunciar tácticamente a ella a efectos de la realización del plan criminal que se habrían propuesto.*

Así las cosas, frente a las posturas adoptadas por los magistrados intervinientes, en cuanto a la disidencia parcial en sus votos, la Sra. Juez Mirta L. López González adhirió al voto del Sr. juez Bunge Campos.

La magistrada señaló: *pese a que los mails fueron provistos por el empleador, la circunstancia de habérseles asignado a cada uno de los imputados un usuario y contraseña, implica reconocer en ello un ámbito de privacidad que no puede ser objeto de intromisión sin los recaudos legales pertinentes...*

Sumado a ello, concluyó: *más allá de no estar especificadas las serias irregularidades detectadas en el manejo de la empresa*, tampoco se dio intervención a la justicia e, incluso, se encomendó una investigación privada a cargo del director de la empresa Vesuvio S.A.; quien, a su vez, obtuvo los correos electrónicos depositados en el servidor de la compañía. Motivo por el cual, tal circunstancia *no puede ser avalada en el marco de un proceso penal.*

Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VII. Causa N° 27.462/14, caratulada., H. C.". 25 de noviembre de 2015

La parte querellante interpuso un recurso de apelación contra el decisorio de la jueza de la instrucción, quien había decretado la nulidad de la incorporación de los correos electrónicos que esta acompañara.

El juez Juan Esteban Cicciaro se inclinó por homologar la decisión en todos sus términos, señalando que compartía los fundamentos que la juzgadora había plasmado en su resolución.

Comenzó por recordar que oportunamente había sostenido que el correo electrónico debía equipararse a la correspondencia epistolar (causa Nº 33.649, "F., F.", del 7-4-2008), indicando que aquel goza de una protección de la privacidad aún mayor, pues *...su funcionamiento y utilización requiere indispensablemente de un prestador del servicio, el nombre de usuario y una clave de acceso destinados a impedir que terceros se entrometan en los datos y contenidos que se emiten y reciben (causa Nº 35.369, "A., C.", del 9-10-2008).*

Sostuvo que si bien no habría controversias acerca de que la protección que emerge de los artículos 18 y 19 de la Constitución Nacional, 11, puntos 1 y 2 de la Convención Americana sobre Derechos Humanos y 17, puntos 1 y 2 del Pacto Internacional de Derechos Civiles y Políticos, alcanza a los correos electrónicos personales, no sucede lo mismo cuando se trata de los correos electrónicos corporativos que son provistos por el empleador: *...pues en tal caso es preciso armonizar la expectativa de privacidad que, como se vio, cuenta con protección constitucional, con el lógico ejercicio de facultades que la ley otorga al empleador en orden al normal funcionamiento de la empresa, bien entendido que los propios controles personales a que está facultado el empleador deben ejercerse con razonabilidad y respetando la dignidad del trabajador (art. 70 de la Ley de Contrato de Trabajo 20.744).*

Teniendo en cuenta esta problemática, desde la necesidad de hallar un razonable equilibrio entre las posiciones extremas, que van desde la posibilidad de revisión sin restricciones para el empleador, hasta la más absoluta imposibilidad de ejercerla con una falta de una legislación específica que expresamente regule la cuestión, el juez puso el acento la idea del consentimiento, a partir del previo conocimiento de pautas claras por parte del empleado, relativas a las facultades de inspección con que contaría su empleador, para acceder al contenido de su correspondencia electrónica. En ese sentido, recordó que el artículo 318 del Código Civil y Comercial de la Nación prevé: *La correspondencia, cualquiera sea el medio empleado para crearla o transmitirla, puede presentarse como prueba por el destinatario, pero la que es confidencial no puede ser utilizada sin consentimiento del remitente. Los terceros no pueden valerse de la correspondencia sin asentimiento del destinatario, y del remitente si es confidencial* y que la Ley de Contrato de Trabajo dispone en su artículo 86: *El trabajador debe observar las órdenes e instrucciones que se le impartan sobre el modo de ejecución del trabajo...*

De una interpretación armónica de ambas disposiciones, estimó que podía concluirse: *si el empleador cuenta con fehacientes facultades de control para el funcionamiento de la empresa, debidamente conocidas por el empleado, no se aprecian dificultades para la incorporación de prueba al respecto.*

Sin embargo, en el caso bajo estudio no se presentaba esa hipótesis y de la circunstancia de que fuese el empleador quien asignara a su empleado un nombre de usuario y una clave personal –lo cual obedecería a elementales razones de seguridad–, no se sigue, necesariamente,

que el dependiente conociera de la legítima posibilidad que el primero tendría de acceder a sus correos.

Distinguió el magistrado, entre los correos que daban cuenta de un intercambio de comunicaciones entre los encausados, de aquellos otros relacionados con las comunicaciones de uno de estos con terceros, contándose en el legajo con la expresa voluntad de estas últimas de no autorizar el uso de sus correos. Y sostuvo que no era posible tampoco convalidar la incorporación de los correos electrónicos que habrían sido recibidos por la querellante, incluida entre los destinatarios como "copiada", puesto que aquellos habrían sido obtenidos de la casilla privada de una de las personas acusadas.

Por último, el juez de cámara mencionó que, a la hora de considerar la validez o invalidez de la prueba analizada, y en la medida en que lo prohibido es el acceso, no resulta relevante que los datos que contengan los correos electrónicos se relacionen exclusivamente con el empleador y no con aspectos de la personalidad de quien los emite o recibe.

Por su parte, el juez Mariano A. Scotto añadió otras consideraciones, coincidiendo con el juez que lo precedió en el acuerdo, en punto a: *...no habiendo previsión legal ni autorización que faculte a la compulsa del correo laboral por parte del empleador sin conocimiento del trabajador al que le fue asignada la casilla respectiva, no puede aquel ingresar al mismo para conocer su contenido, pues el hecho de que se le haya entregado al empleado una clave personal de su exclusivo conocimiento, le ha generado una expectativa de privacidad que tiene primacía y protección.*

Sin embargo, no fue de la misma opinión con relación a los correos electrónicos aportados por la parte querellante y que recibiera de los imputados como "copiada" ("CC:"), dado que la decisión de incluirla entre los destinatarios, aun de manera secundaria, se tradujo en la expresa voluntad de ponerla en conocimiento de su contenido y que, por tanto, su revelación por parte de aquella no entrañaría una afectación a la garantía de inviolabilidad de la correspondencia.

Su posición fue compartida por el juez Mauro A. Divito, quien sostuvo, en ese sentido: *...más allá de que el texto de los correos electrónicos ha sido obtenido mediante el ingreso –como ya se dijo, no justificado– a las casillas de los imputados, en los casos puntuales en los que aquellos fueron también enviados a la querellante, dicha circunstancia impide predicar que su incorporación al proceso ha importado una*

afectación a las garantías constitucionales de los restantes intervinientes. En efecto, las particulares características del correo electrónico, en tanto posibilitan el intercambio simultáneo entre más de dos personas, imponen ponderar cuidadosamente esta circunstancia al evaluar los alcances de las expectativas de privacidad que gozan de protección constitucional, pues estas –razonablemente– conducen a excluir a los terceros del círculo de quienes se hallan facultados para acceder al mensaje, mas no a aquel que se encuentra entre sus destinatarios.

En definitiva, el tribunal convalidó parcialmente la decisión de la jueza de instrucción, revocando la declaración de nulidad que se relacionaba exclusivamente con la incorporación de los correos electrónicos que tuvieron entre sus destinatarios a la querellante, incluida como "copiada".

Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VII. Causa N° 70.022/14, caratulada "G., L.". 23 de febrero de 2018

La defensa interpuso un remedio de apelación para poner en crisis la decisión de rechazar el planteo de nulidad que dedujera ante el juez de instrucción, el cual se encontraba destinado a cuestionar la validez de los documentos presentados por la querella al formular la denuncia –dado que habían sido obtenidos de la computadora laboral de G. sin contar para ello con la autorización judicial pertinente–, así como del peritaje que con posterioridad se practicara sobre la computadora aportada por el acusador privado.

Resulta menester destacar que la defensa aclaró, durante la audiencia oral, que la impugnación no pretendía abarcar a los correos electrónicos que el acusado había enviado a uno de los socios gerentes de la empresa querellante, desistiendo en ese punto, de su voluntad recursiva.

El tribunal concluyó que los agravios de la defensa no resultaban atendibles, pues de las constancias del legajo surgía con claridad que G. sabía que los socios gerentes de la empresa contaban con las claves de acceso a su computadora y a su correo electrónico laboral, para poder supervisar su labor y para suplirlo en caso de necesidad –considerando su posición jerárquica– y que en tales condiciones, ese acceso, *...se encuentra fuera del ámbito de privacidad protegido por la Constitución Nacional.*

Con relación al estudio pericial practicado sobre el disco rígido de la computadora aportada por la querella –su propietaria– y que era utilizado por el acusado, el tribunal no encontró elementos que permitiesen sostener que este hubiese sido manipulado o adulterado, destacando

que el procedimiento se había llevado a cabo con notificación de todas las partes interesadas, las cuales pudieron controlar su desarrollo, con el auxilio de los peritos que las partes propusieron con ese propósito.

En función de estas consideraciones, el tribunal convalidó la decisión del juez de grado, pues más allá del valor que eventualmente corresponda asignar a la prueba obtenida en esas condiciones y a partir del referido peritaje, no se observaban en este caso, vicios o defectos que autorizaran a aplicar la grave sanción que la parte reclamaba y cuya procedencia, por lo demás, debe siempre analizarse con criterio restrictivo (de acuerdo con lo dispuesto en el artículo 2° del CPPN).

Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala I, caratulada "C.J.A y otros s/nulidad". 25 de marzo de 2019

La controversia llevada al análisis de la Cámara versó sobre la validez de la incorporación como prueba de cargo de correos electrónicos provenientes de la casilla privada del empleado, obtenidos y presentados por la empleadora, querellante en la causa.

Los camaristas de la Sala I declararon la nulidad de estos elementos probatorios por considerar que habían sido obtenidos a partir de una vulneración a los artículos 18 y 19 de la Constitución Nacional; existiendo, una expectativa de privacidad en cabeza del empleado que suponía privados dichos correos.

Pues bien, los camaristas Pablo Guillermo Lucero y Hernán Martín López entendieron: *la intromisión de las comunicaciones en la forma de mensajes electrónicos, tanto en el correo interno, como aquellos que se envían y reciben en el particular, genera una afectación en el ámbito privado…* En tal sentido, manifestaron: *dentro de los derechos individuales de una persona –contemplado por la Constitución Nacional–, ya sea como derivación del derecho a la propiedad o como un derecho autónomo a la intimidad –contemplado en los Pactos Internacionales con jerarquía supra constitucional–, existe un deber del Estado de regular aquellos ámbitos privados donde sus titulares han exhibido un interés en que así se mantengan. Esa expectativa respecto a los ámbitos privados se vería claramente reflejada en que el correo electrónico posee características de protección de privacidad más acentuadas que la tradicional vía postal, ya que para su funcionamiento se requiere un prestador de servicio, el nombre de usuario y un código o contraseña de acceso, que impide la intrusión de terceros, accediendo a los datos infor-*

máticos ajenos sin la autorización o anuencia del titular de la casilla"; y, en consecuencia, "también en este caso debe mediar la autorización judicial para acceder a su conocimiento.

A su vez, expresaron que la prohibición que pesa sobre el empleador –en cuanto a la lectura del contenido de los correos electrónicos– encuentra sustento en la violación del derecho de privacidad del trabajador, y que, tampoco, se trata de un elemento configurativo del débito contractual, sino de una indiscutible e impenetrable dignidad y autodeterminación que como sujeto titulariza.

En un mismo orden de ideas, los camaristas coincidieron con lo sostenido por la defensa en cuanto a que se violó la expectativa de privacidad; puesto a que el empleado no tuvo conocimiento sobre tal circunstancia, como así tampoco sobre la modalidad de control que el empleador pretendía sobre sus tareas y que desencadenó con el acceso al correo personal del trabajador.

Finalmente, señalaron: *los correos electrónicos que fueran aportados como elementos probatorios por la querella para dar sustento a la imputación, fueron obtenidos a través de una intromisión en la privacidad, fundamentalmente porque nada se había establecido en relación a tal extremo como política de la empresa y que hubiese permitido a los empleados conocer, con la claridad que las normas citadas exigen, cuáles eran los límites a su intimidad, por lo que, más allá de que pudiera existir un cauce independiente de investigación, el cual será analizado al momento de resolver el recurso de apelación interpuesto contra el procesamiento en los autos principales, corresponde anular la incorporación de los correos en cuestión.*

Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala I. Causa N° 47.334/16, caratulada "CAO, José Antonio y otros/ nulidad". 25 de marzo de 2019

El doctor Gervasio Caviglione Fraga, letrado defensor de J. A. C., interpuso un recurso de apelación contra la resolución dictada por el juez de instrucción, por cuanto rechazó el pedido de nulidad oportunamente formulado por esa parte, con relación a la incorporación –y posterior valoración–, de los correos electrónicos que fueran aportados por la querella y que le habrían sido enviados por el acusado. La defensa sostuvo, entre otras cosas: *... la intromisión por parte de la querella en*

estas direcciones vulnera los derechos reconocidos en los art. 18 y 19 de la CN, siendo esta evidencia obtenida de manera ilegal.

El tribunal concluyó que correspondía hacer lugar a la pretensión de la defensa, al señalar: *...la intromisión de las comunicaciones en la forma de mensajes electrónicos, tanto en el correo interno, como aquellos que se envían y reciben en el particular, genera una afectación en el ámbito privado [...] por cuanto dentro de los derechos individuales de una persona –contemplado por la Constitución Nacional–, ya sea como derivación del derecho a la propiedad o como un derecho autónomo a la intimidad –contemplado en los Pactos Internacionales con jerarquía* supra *constitucional–, existe un deber del Estado de regular aquellos ámbitos privados donde sus titulares han exhibido un interés en que así se mantengan.*

En relación con las razonables expectativas de privacidad con que los usuarios de estos medios de comunicación podían contar, y con apoyo en los mecanismos que tienden a dotarlos de mayor seguridad, en comparación con aquellos que acompañan al sistema de correo postal tradicional *...ya que para su funcionamiento se requiere un prestador de servicio, el nombre de usuario y un código o contraseña de acceso, que impide la intrusión de terceros, accediendo a los datos informáticos ajenos sin la autorización o anuencia del titular de la casilla*, el tribunal sostuvo que para poder acceder a su contenido, debe contarse con la autorización judicial pertinente.

En función de estas consideraciones, el empleador... *tiene prohibido, en principio, leer e–mails enviados o recibidos por sus empleados. El contenido de tal prohibición no es otro que la violación del derecho de privacidad del trabajador, facultad que no comporta un elemento configurativo del débito contractual y que, por ello, hace a la indiscutible e impenetrable dignidad y autodeterminación que como sujeto titulariza.*

El tribunal afirmó, además, que frente al conflicto de intereses que el caso supone: *La averiguación de la verdad no puede erigirse como bastión del avasallamiento de derechos reconocidos por la Constitución Nacional, ni por parte de los particulares, ni del poder público. El derecho a la intimidad constituye uno de los derechos de la personalidad con mayor necesidad de custodia social, pues gravita sobre la libertad y el pensamiento.*

En este caso, por lo demás, el dependiente desconocía las posibilidades que el empleador tenía de invadir su intimidad, así como la modalidad de control que sobre las tareas que realizaba, aquel preten-

día ejercer *...fundamentalmente porque nada se había establecido en relación con tal extremo como política de la empresa y que hubiese permitido a los empleados conocer, con la claridad que las normas citadas exigen, cuáles eran los límites a su intimidad*. Y en ese sentido, el tribunal hizo hincapié en: *...los correos electrónicos en cuestión fueron enviados desde la casilla personal del imputado, que llevaba como dominio la inicial de su nombre seguida a su apellido*.

Los jueces concluyeron, entonces, que habiendo sido obtenida ilegítimamente la prueba relativa a los correos electrónicos aportados por la querella, correspondía declarar la nulidad de su incorporación al legajo.

XIII. b. 3. Fuero provincial

Suprema Corte de Justicia de Mendoza. Causa N° 99.077, caratulada "Dasmi, Noelia Celeste c/ provincia de Mendoza (Poder Judicial) s/ A.P.A.". 30 de diciembre de 2011

En el marco de un procedimiento administrativo, Noelia Celeste Dasmi promovió una acción procesal administrativa contra la provincia de Mendoza, persiguiendo la anulación de una resolución dictada por la Sala Administrativa de la Suprema Corte de Justicia, a través de la cual, se le impuso a la nombrada una sanción disciplinaria de diez (10) días de suspensión por infracción a los deberes y prohibiciones prescriptos en los artículos 13 inciso a), b), c) y f); 14 inciso f), j) y ll) del Decreto Ley 560/73; Acordada N° 17.868 y artículo 8 de la Ley 22.117.

Fundó sus agravios en que la decisión cuestionada se habría dictado en violación de la garantía del debido proceso, pues los correos electrónicos que servían de prueba de cargo se habrían obtenido ilegítimamente, tal como había considerado la Décimo Séptima Fiscalía de Instrucción de la Unidad Especial N° 6 de Delitos Especiales en el Expte. N° P-13.751/09, caratulado: *"F. c/ NN P/ Violación de secreto"*, que declaró la nulidad de esa prueba documental. Sostuvo, además, que tampoco surgía de las evidencias colectadas que hubiese sido ella quien enviara, efectivamente, los correos electrónicos que motivaran la aplicación de la sanción.

De las constancias del expediente se desprendía que otra funcionaria le habría solicitado a Dasmi información considerada confidencial y relacionada con los antecedentes policiales o criminales que pudieran

registrar varias personas, con fines extraños o ajenos a una causa penal en particular, y que, en este sentido, la nombrada le habría compartido, a través del mismo medio de comunicación lo solicitado.

La Sala de la Corte de Justicia de Mendoza adelantó, de ante mano dejando planteada la controversia mencionando: *...que si bien el correo corporativo constituye una herramienta de propiedad del empleador cuyo uso este tiene derecho a monitorear, al mismo tiempo es un medio de expresión personal del empleado, de comunicación. Por lo cual se discute sobre el alcance de la protección que tienen los mensajes del trabajador expresados por este medio, por imperio de la garantía de la inviolabilidad de la correspondencia epistolar del art. 18 de la Constitución Nacional. Y, por ende, hasta dónde pueden llegar las facultades del empleador, ya que la antes citada garantía actúa como una frontera en resguardo del derecho a la intimidad personal y dignidad del trabajador*.

Con cita de doctrina, señalaron los jueces: *Algunos, acertadamente desde nuestro punto de vista, realizan algunas distinciones que pueden ser útiles para la solución del presente caso, ya que la situación no será la misma si: (i) el uso del ordenador tiene lugar en el ámbito de trabajo compartiendo el recurso con otros trabajadores, o en el ámbito más privado de un ordenador individual asignado al trabajador. También, en cuanto al canal de comunicación, si: (ii) se usan cuentas de correo y conexiones propias de la empresa (o si se usa una cuenta web mail o una cuenta con un cliente de mail que graba los mensajes en el disco rígido, o las particulares; y (iii) si existen claves de acceso u otras situaciones que demuestren que el correo es personal y privado, o si: (iv) la política existente fue notificada al empleado y este la aceptó o, por el contrario, sabía que no existía confidencialidad alguna en la empresa sobre el uso de sus herramientas tecnológicas. También habrá que determinar (v) si la conexión a internet se desarrolló en horario de trabajo, o fuera del mismo y (vi) si esta tuvo lugar en el espacio físico de la oficina o fuera del mismo (pero con elementos del trabajo), cuestión que hoy día tiene importancia, por el desarrollo del teletrabajo (conf. PALAZZI, Pablo E., "Correo electrónico...", cit.). Como se colige fácilmente, el caso más complicado se presenta cuando existen claves de acceso u otras situaciones (como la asignación de computadoras a determinados usuarios) a partir de las cuales se pueda inferir que la cuenta de correo es personal y privada del trabajador, por cuanto tales circunstancias generan a favor del empleado lo que la jurisprudencia de los EE. UU.*

ha denominado como principio de "expectativa razonable de privacidad", doctrina que ha tenido un amplio predicamento local a partir del trabajo incipiente de MIRANDA DE HERMIDA, Beatriz, "El e–mail laboral en Argentina" (public. en DT 2001–B, p. 1892), quien postuló la formulación por parte de la empresa de políticas claras en el uso de esta herramienta advirtiendo al empleado que dicho uso debe ser realizado exclusivamente en función de su actividad laboral y haciéndole conocer el derecho de la compañía a controlar el correcto uso del e–mail, ya que de lo contrario se podría "crear una falsa expectativa de privacidad.

El tribunal sostuvo que la mayoría de los autores coinciden en que el derecho a la privacidad del trabajador cedería ante las facultades de control e inspección de su empleador sobre sus comunicaciones si, antes de ejercerlas y a través de reglamentos o de avisos expresos y claros, hubiese adelantado que contaba con ellas.

Tras examinar los planteos de la actora y confrontarlos con la prueba reunida, los jueces del Máximo Tribunal mendocino entendieron que, más allá de que se encontrase identificada la computadora desde la cual se habrían enviado los mensajes y su usuario, esto no resultaba prueba suficiente de que su emisor hubiese sido efectivamente aquel *...si no hay un mecanismo de autentificación o firma digital, para lo cual el servidor de correo debe estar configurado especialmente* y que esta circunstancia, sumada a la nulidad declarada en sede penal con respecto a esa prueba documental y, fundamentalmente, a que en el reglamento dispuesto por la Administración: *no se han fijado reglas claras sobre el modo, la oportunidad, ni la extensión de las facultades para poder examinar el contenido de las comunicaciones remitidas por los empleados del Poder Judicial en uso del correo electrónico institucional*, la pretensión de la accionante de que no debió valorarse *...como prueba directa la copia del e–mail remitido desde su dirección, para sustentar la imputación referida al contenido del correo electrónico*, resultaba atendible.

Sin perjuicio de lo anteriormente mencionado, el tribunal convalidó el acto administrativo cuestionado, excluyendo la prueba mencionada, el comportamiento merecedor de sanción, se encontraba suficientemente acreditado con otras evidencias. En esa dirección y en cuanto aquí interesa, afirmó: *el servicio de e–mail utilizado tanto para transmitir el mensaje original, como su respuesta es de titularidad del empleador, por lo cual se puede reglamentar su uso y vigilar el modo de cumplimiento de tales instrucciones, tal cual ha sido instrumentado por*

*la Acordada N° 17.868 del 25–3–2003, cuyo resolutivo II textualmente dispone: "recordar que los sistemas de computación y las computado*ras *del Poder Judicial de Mendoza están destinados exclusivamente para uso oficial, no pudiendo los usuarios dar a conocer sus contraseñas de acceso ni compartirlas con otros usuarios", razón por la cual el inciso b) del resolutivo VI del mismo reglamento determina que los usuarios del sistema de correo electrónico "serán absolutos responsables de todo mensaje que envíen utilizando los recursos del organismo"...*, aclarando que esa reglamentación quedaba obsoleta la época en que tuvieron lugar los hechos ventilados en el legajo y que su contenido se encontraba a disposición de todas las personas que integran el Poder Judicial e incluso del público general, en el sitio web oficial, en función de lo cual, podía tenerse por debidamente comprobado el uso irregular del servicio *...ya que –como mínimo, y desde el punto más favorable para la actora– la sumariada ha incumplido con su deber de no difundir su contraseña de acceso*, irregularidad que había *...perturbado gravemente la normal prestación del servicio.*

XIII. c. Jurisprudencia extranjera

XIII. c. 1. Tribunal Europeo De Derechos Humanos

Tribunal Europeo de Derechos Humanos. Gran Sala. Recurso N° 61496/08, caratulado "Barbulescu Contra Rumania" Sentencia Estrasburgo. 5 de septiembre de 2017

En este caso el Tribunal Europeo de Derechos Humanos (el Tribunal) analiza la petición de un ciudadano rumano que reclama que su despido se llevó a cabo en violación a su derecho consagrado en el artículo 8 de la Convención Europea de Derecho Humanos (la Convención). El caso se inició en los tribunales de Rumanía donde se validó el despido del peticionante que se llevó a delante a raíz del control de la correspondencia en el ámbito laboral, dicho control de las comunicaciones surgió por un supuesto uso de los elementos de la empresa para fines particulares, lo cual se encontraba prohibido por la empresa.

Barbulescu sostuvo que el despido por parte de su empleador se había basado en una violación de su derecho al respeto a su vida privada

y su correspondencia y que, al no revocar esa medida, los tribunales nacionales no habían cumplido con su obligación de proteger el derecho en cuestión. Se basó en el artículo 8 del Convenio, que dispone:

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

De los hechos descritos en la sentencia surge que efectivamente el empleador contaba con una política que prohibía cualquier tipo de comunicación con fines privados en la jornada laboral, la cual había sido firmada por el empleado. Los términos y condiciones incluidos en dicha política no establecían la posibilidad de control o monitoreo posterior por parte del empleador ni el alcance que dicho control tendría. Así, debía dilucidarse si la razonable expectativa de privacidad mantenía vigencia a pesar de que la prohibición señalada.

Por su parte, el gobierno rumano sostuvo que Barculescu *no podía demandar ninguna expectativa de "privacidad" con respecto a las comunicaciones que había intercambiado a través de una cuenta de mensajería instantánea creada para uso profesional.* Con referencia a la jurisprudencia de los tribunales franceses y chipriotas, afirmaron que los mensajes enviados por un empleado utilizando las facilidades técnicas puestas a su disposición por su empresa debían considerarse de naturaleza profesional a menos que el empleado los identificara explícitamente como privados. Señalaron que no era técnicamente posible utilizar el Messenger Yahoo para marcar los mensajes como privados; sin embargo, el demandante había tenido una oportunidad, durante la etapa inicial del procedimiento disciplinario, para indicar que sus comunicaciones habían sido privadas y sin perjuicio de esto, optó por mantener que estaban relacionadas con el trabajo.

El Gobierno se basó en otros tres argumentos para sostener que el artículo 8 del Convenio no era aplicable en el presente caso. En primer lugar, no había pruebas que sugirieran que la transcripción de las comunicaciones del solicitante había sido divulgada a sus compañeros de trabajo; el propio demandante había presentado la transcripción

completa de los mensajes en los procedimientos ante los tribunales nacionales, sin pedir que se impusiera ninguna restricción al acceso a los documentos en cuestión. En segundo lugar, las autoridades nacionales habían utilizado la transcripción de los mensajes como prueba porque el demandante lo había solicitado, y porque las autoridades judiciales ya habían comprobado que la monitorización de sus comunicaciones había sido legal. En tercer lugar, la nota informativa contenía suficiente información para que el demandante fuera consciente de que su empresa podría monitorizar sus comunicaciones".

El Tribunal sostuvo que su tarea en el presente caso era, por lo tanto, *aclarar la naturaleza y el alcance de las obligaciones positivas que el Estado demandado debía cumplir para proteger el derecho del demandante al respeto de su vida privada y correspondencia en el ámbito de su puesto de trabajo.*

Así consideró: *la proporcionalidad y las garantías procesales contra la arbitrariedad son esenciales. En este contexto, las autoridades nacionales deben tratar los siguientes factores como relevantes:*

(i) si el empleado ha sido notificado de la posibilidad de que el empresario pueda tomar medidas para monitorizar la correspondencia y otras comunicaciones, así como de la implementación de tales medidas. Si bien en la práctica los empleados pueden ser notificados de varias maneras dependiendo de las circunstancias de hecho particulares de cada caso, el Tribunal considera que para que las medidas se consideren compatibles con los requisitos del Artículo 8 del Convenio, la notificación normalmente debe ser clara sobre el tipo de seguimiento, dándose por adelantado;

(ii) el alcance de la supervisión por parte del empresario y el grado de intrusión en la privacidad del empleado. En este sentido, se debe hacer una distinción entre la monitorización del flujo de comunicaciones y la de su contenido. También se debe tener en cuenta si todas las comunicaciones o solo una parte de ellas han sido monitorizadas, al igual que si la monitorización fue limitada en el tiempo y el número de personas que tuvieron acceso a los resultados (consulte Köpke, citado anteriormente). Lo mismo se aplica a los límites espaciales de la monitorización;

(iii) si el empresario ha proporcionado razones legítimas para justificar la monitorización de las comunicaciones y el acceso a su contenido real (consulte los párrafos 38, 43 y 45 anteriores para obtener una descripción general del derecho internacional y europeo en esta área). Dado que la monitorización del contenido de las comunicaciones es, por

naturaleza, un método claramente más invasivo, requiere una mayor justificación;

(iv) si hubiera sido posible establecer un sistema de vigilancia basado en métodos y medidas menos invasivo que el acceso directo al contenido de las comunicaciones del empleado. A este respecto, debe haber una evaluación a la luz de las circunstancias particulares de cada caso de si el objetivo perseguido por el empresario podría haberse alcanzado sin haber accedido directamente al contenido completo de las comunicaciones del empleado;

(v) las consecuencias del control para el empleado sometido a él (ver, mutatis mutandis, el criterio similar aplicado en la evaluación de la proporcionalidad de una interferencia con el ejercicio de la libertad de expresión según lo protegido por el artículo 10 del Convenio en Axel). Springer AG c. Germany [GC], nº. 39954/08, § 95, 7 de febrero de 2012, con referencias adicionales); y el uso que hizo el empresario de los resultados de la operación de monitorización, en particular si los resultados se utilizaron para lograr el objetivo declarado de la medida (ver Köpke, citado anteriormente);

(vi) si el empleado había recibido las garantías adecuadas, especialmente cuando las operaciones de monitorización del empresario eran de carácter invasivo. Dichas garantías deben garantizar, en particular, que el empresario no pueda acceder al contenido real de las comunicaciones en cuestión, a menos que el empleado haya sido notificado antes de esa eventualidad.

Finalmente, el Tribunal sostuvo que las autoridades nacionales deben garantizar que un empleado cuyas comunicaciones hayan sido monitorizadas tenga acceso a los órganos judiciales con jurisdicción para determinar, al menos en esencia, si se observaron los criterios descritos anteriormente y si las medidas impugnadas eran legales.

En este caso en concreto, el Tribunal resolvió: *los tribunales nacionales –rumanos– no determinaron, en particular, si el demandante había recibido una notificación previa de su empresa sobre la posibilidad de que sus comunicaciones (...) pudieran ser monitorizadas; tampoco tuvieron en cuenta el hecho de que no había sido informado de la naturaleza o el alcance de la supervisión, o el grado de intrusión en su vida privada y correspondencia. Además, no pudieron determinar, en primer lugar, las razones específicas que justifican la introducción de las medidas de monitorización; en segundo lugar, si el empresario podría haber utilizado medidas que menos invasivas de la vida privada*

y la correspondencia del demandante; y, en tercer lugar, si se pudo haber accedido a las comunicaciones sin su conocimiento.

Teniendo en cuenta todas las consideraciones anteriores, y sin perjuicio del margen de apreciación del Estado demandado, el Tribunal considera que las autoridades nacionales no brindaron la protección adecuada del derecho del demandante al respeto de su vida privada y su correspondencia y, por consiguiente, no lograron un justo equilibrio entre los intereses implicados. Por lo tanto, ha habido una violación del artículo 8 del Convenio".

XIII. c. 2. España

Tribunal Supremo. Sala de lo Social, Resolución STS N° 594/2018. 08 de febrero de 2018

Si bien el caso traído a consideración, no se trata de un caso penal sino, más bien, se trata de uno en el que se analiza la procedencia del despido de un empleado por "transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo"; lo cierto es que se aplican en el caso los estándares fijados en el caso "Barbulescu" del TEDH contra Rumania y se aplican los entandares que allí se fijan para considerar si era válido que el empleador revise la correspondencia de un empleado, sin que se viole el derecho a la intimidad y la privacidad de las comunicaciones.

El hecho que motivó el despido se inició a raíz de que un tercer empleado de la compañía encontrara unos comprobantes de transferencias de fondos a favor del empleado despedido en la fotocopiadora pública de la empresa y las elevara a sus superiores. Esto motivó que se iniciara una investigación interna que incluiría la revisión de los correos del empleado que había recibido los pagos y posteriormente fue despedido. Por su parte, el empleado despedido negó haber recibido pago o regalo alguno por parte de los proveedores y demandó a su empleador por considerar que el despido no resultaba procedente.

Así, en las instancias inferiores se concluyó que el despido correspondía y la defensa técnica del empleado dedujo recurso de casación ante el Tribunal Supremo solicitando que debían ser declaradas nulas y no podían ser incluidas a consideración las pruebas ilícitamente obtenidas a través del control del correo electrónico del actor, no así las pruebas

encontradas por el empleado en la fotocopiadora pública de la oficina ya que se trató de un encuentro casual en un lugar común de edificio.

En primer lugar, el TS analizó su propia jurisprudencia reconociendo las facultades que tienen los empresarios de adoptar medidas que considere oportunas para la dirección y fiscalización del cumplimiento de las obligaciones y deberes laborales dentro de la empresa. Por su parte, también reconoció la plena vigencia del derecho a la intimidad en el marco de una relación laboral: *el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana... Así pues, lo que garantiza el art. 18.1 CE es el secreto sobre nuestra propia esfera de vida personal, excluyendo que sean los terceros, particulares o poderes públicos, los que delimiten los contornos de nuestra vida privada [STC 159/2009, de 29 de junio, FJ 3; o SSTC 185/2002, de 14 de octubre, FJ 3; y 93/2013, de 23 de abril, FJ 8] (FJ 5).*

Así, se observa en caso la puja de dos derechos de la misma jerarquía y en la que se debe decidir si la revisión de la correspondencia se encontraba justificada o por el contrario el empleador se excedió en sus facultades fiscalizadoras. El TS advierte que si bien el propio tribunal poseía una vasta jurisprudencia para fijar los criterios de oportunidad en la que el empleador podía revisar la correspondencia de un empleado, era oportuno traer a colación el reciente pronunciamiento del Tribunal Europeo de Derechos Humanos en el caso conocido como "Barbulescu" y realizar el "test" de validez que se fijaba en dicha resolución.

De allí, que analizaron el caso traído a estudio con las siguientes preguntas:

"i) ¿El empleado ha sido informado de la posibilidad de que el empleador tome medidas para supervisar su correspondencia y otras comunicaciones, así como la aplicación de tales medidas? Si bien en la práctica esta información puede ser comunicada efectivamente al personal de diversas maneras, según las especificidades fácticas de cada caso, el Tribunal considera que, para que las medidas puedan ser consideradas conforme a los requisitos del artículo 8 del Convenio, la advertencia debe ser, en principio, clara en cuanto a la naturaleza de la supervisión y antes del establecimiento de esta. ii) ¿Cuál fue el alcance de la supervisión realizada del empleador y el grado de intrusión en la

vida privada del empleado? A este respecto, debe hacerse una distinción entre el control del flujo de comunicaciones y el de su contenido. También se debería tener en cuenta si la supervisión de las comunicaciones se ha realizado sobre la totalidad o solo una parte de ellas y si ha sido o no limitado en el tiempo y el número de personas que han tenido acceso a sus resultados (véase, en este sentido, la sentencia Köpke, precitada). Lo mismo se aplica a los límites espaciales de la vigilancia. iii) ¿El empleador ha presentado argumentos legítimos para justificar la vigilancia de las comunicaciones y el acceso a su contenido? Dado que la vigilancia del contenido de las comunicaciones es por su naturaleza un método mucho más invasivo, requiere justificaciones más fundamentadas. iv) ¿Habría sido posible establecer un sistema de vigilancia basado en medios y medidas menos intrusivos que el acceso directo al contenido de comunicaciones del empleado? A este respecto, es necesario evaluar, en función de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario puede alcanzarse sin que este tenga pleno y directo acceso al contenido de las comunicaciones del empleado. v) ¿Cuáles fueron las consecuencias de la supervisión para el empleado afectado... con las referencias citadas? ¿De qué modo utilizó el empresario los resultados de la medida de vigilancia, concretamente si los resultados se utilizaron para alcanzar el objetivo declarado de la medida...? vi) ¿Al empleado se le ofrecieron garantías adecuadas, particularmente cuando las medidas de supervisión del empleador tenían carácter intrusivo? En particular, estas garantías debían impedir que el empleador tuviera acceso al contenido de las comunicaciones en cuestión sin que el empleado hubiera sido previamente notificado de tal eventualidad".

Destacó el tribunal que *la lectura de los prolijos razonamientos utilizados por el TEDH en el asunto "Barbulescu", pone de manifiesto –entendemos– que el norte de su resolución estriba en la ponderación de los intereses en juego, al objeto de alcanzar un justo equilibrio entre el derecho del trabajador al respeto de su vida privada y de su correspondencia, y los intereses de la empresa empleadora (así, en los apartados 29, 30, 57, 99, 131 y 144). Y al efecto –resumimos– son decisivos factores a tener en cuenta: a) el grado de intromisión del empresario; b) la concurrencia de legítima razón empresarial justificativa de la monitorización; c) la inexistencia o existencia de medios menos intrusivos para la consecución del mismo objetivo; d) el destino dado por la empresa al resultado del control; e) la previsión de garantías para el trabajador.*

Finalmente, el TS entendió que en el caso en concreto la revisión de la correspondencia no había sido ilegítima, ya que había razones que justificaban esa intromisión resolviendo rechazar la demanda del empleado despedido entendiendo que su despido había sido justificado.

Tribunal Supremo. Sala de lo Penal. –Causa N° 3754/2018 N° de Resolución: 489/2018. 23 de octubre de 2018

El Dr. Jesús Urraza Abad en representación del imputado interpuso recurso de apelación ante la Cámara de Casación contra la resolución dictada el 1° de junio de 2017 por la Sección Primera de la Audiencia Provincial de Vizcaya en causa seguida contra el recurrente por un delito de administración desleal.

Trimarine Internacional Spains L.U (en adelante "Trimarine") era comercializadora de pescados y mariscos. El acusado, Maximiliano (quien carece de antecedentes penales), desde 2004 desempeñó los cargos de apoderado y secretario del consejo de administración de Trimarine, y a partir de mayo de 2007 se desempeñó además como gerente en virtud de un contrato de alta dirección, cargo que cesó a partir de junio de 2011 en razón de su despido, el cual hubiera sido declarado procedente por la jurisdicción social. Este, desde 2004 y 2011 ha realizado una serie de operaciones comerciales propias del giro comercial de Trimarine. Así como también participó en sociedades vinculadas a la misma empresa.

El auto que el imputado apeló fue el que lo condenó *como autor de un delito de apropiación indebida con una pena de cinco años de prisión, con inhabilitación especial para el derecho a sufragio pasivo y once meses de multa con una cuota diaria de 100 euros y responsabilidad civil a favor de Trimarine Spain.* El acusado a través de su intervención activa ejecutó operaciones en perjuicio patrimonial para la empresa Trimarine y en correlativo beneficio personal para él. Los motivos por los cuales el recurrente preparó el recurso de casación fueron la infracción al precepto constitucional al amparo del art. 852 (derecho a un proceso con todas las garantías), al precepto constitucional al amparo del art. 852 por vulneración del derecho fundamental a la intimidad, al secreto de las comunicaciones y a la protección de datos personales (previstos en el art. 18.1, 18.2 y 18.4), subsidiariamente la infracción de ley al amparo del art. 849.2 por indebida ignorancia del contenido literosuficiente de determinados documentos obrantes en

autos. Asimismo, infracción del precepto constitución del art. 852, vulneración del derecho a la presunción de inocencia y por infracción de precepto constitucional al amparo del art. 852 vulneración del derecho fundamental a la legalidad y derecho de libertad (arts. 25,1 y 17.1), apropiación indebida (art. 250.1 1-5 CP) e infracción la ley de amparo del art. 849.1 aplicación indebida de los arts. 109 y 110 CP.

Este propugnó la nulidad del examen efectuado de su computadora personal y en consecuencia la inutilizabilidad de todas las pruebas que se derivan de este escrutinio, en el que se pudo acceder a miles de correos electrónicos pertenecientes a él, lo cual podrían ser pruebas efectuadas por la prohibición consagrada en el art. 11.1 y, por tanto, sin aptitud para fundar la condena.

En torno a ello, los jueces expresaron que la cuestión se decidirá primeramente en si se puede hablar de violación de un derecho fundamental predicable de esa actuación de la mercantil (a) si la respuesta fuera afirmativa habría, pues en ese caso que ventilar a continuación *in casu* si esto arrastraría la inutilizabilidad de la prueba (b), finalmente, y en un tercer escalón es preciso indagar sobre el alcance de tal consecuencia (c) si es que esta se afirma.

Teniendo en cuenta lo anteriormente planteado, los jueces han expresado que la doctrina no siempre ha sido homogénea, ni es lineal. En este sentido, se han detectado algunas discrepancias y muchos matices diferentes, a veces, manifestación de una evolución interpretativa, hasta en el seno de un mismo órgano se ha podido apreciar divergencias y cambios. *…Que hay derechos fundamentales en juego, nadie puede dudarlo: como se ha dicho gráficamente con frase feliz y por ello, muy repetida, los trabajadores no dejan ni su intimidad ni el resto de los derechos en la oficina o empresa.*

Adujeron:*… es una obviedad por nadie discutida que la relación laboral impone modulaciones, en esos derechos, aunque nunca absolutas, como se ha preocupado de resaltar la jurisprudencia (vid arts. 18 y 20.3 del Estatuto de los trabajadores; de redacción un tanto obsoleta y no acompasada con las nuevas –o ya no tan nuevas realidades tecnológicas). Esas limitaciones admisibles en el seno de la relación empresario–trabajador no serían sin más extrapolables a otros ámbitos (vid. voto particular de la STC 26/2018, de 3 de marzo). …hemos declarado –afirma nuestro Tribunal Constitucional– que la intimidad protegida por el art. 18.1 CE no se reduce a la que se desarrolla en un ámbito doméstico o privado; existen también otros ámbitos, en particular el*

relacionado con el trabajo o la profesión, en que se generan relaciones interpersonales, vínculos o actuaciones que pueden constituir manifestación de la vida privada (STC 12/2012, de 30 de enero, FJ 5). Por ello expresamente hemos afirmado que el derecho a la intimidad es aplicable al ámbito de las relaciones laborales (SSTC 98/2000, de 10 de abril FFJJ 6 a 9; 186/2000, de 10 de julio, FJ 5). (vid igualmente STS – Sala 4ª– 119/2018, de 8 de febrero).

En el mismo orden de ideas, los jueces mencionaron una sentencia del orden social de la STS (Sala Cuarta) de 2007 en la cual el Tribunal Supremo razona que de acuerdo con las exigencias de buena fe *se debe establecer previamente las reglas de uso de esos medios con la aplicación de prohibiciones absolutas o parciales e informar a los trabajadores de que existirá control y de los medios que han de aplicarse en orden a comprobar la correlación de los usos así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio, cuando este, sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo*. En este sentido, agregaron que hay un relevante signo diferenciador entre el acceso por el empresario y el acceso por agentes públicos, en el cual en el primero en virtud de sus facultades de supervisión del trabajo que se presta por una relación laboral, en el segundo en virtud de potestades públicas. Entonces, la clave está en si el trabajador ha consentido anticipadamente reconociendo esa capacidad de supervisión al empresario y, por tanto, cuenta con ello, está advertido, es decir, es una limitación conocida y contractualmente asumida.

Asimismo, el Juez resaltó también la relevante jurisprudencia constituida con Barbulescu, en la cual se habla de la insoslayable necesidad de ponderar los bienes en conflicto, de una parte, el interés del empresario en evitar o descubrir conductas desleales o ilícitas del trabajador. Prevalecerá solo si se atiene a ciertos estándares que han venido a conocerse como el test del mentado precedente anteriormente mencionado. En el cual se enuncian criterios de ponderación relacionados con la *necesidad y utilidad de la medida, inexistencia de vías menos lesivas, sospechas fundadas, etc…* que en particular no admite acceso no consentido al dispositivo de almacenamiento masivo de datos si el trabajador no ha sido advertido de esa posibilidad.

Partiendo de las premisas mencionadas anteriormente, los jueces mencionaron que esa es la clave que les permite resolver este asunto y terminan concluyendo: *En las circunstancias en que se llevó a cabo hay*

que afirmar que el ordenamiento ni consiente, ni consentía en la fecha de los hechos, tal acción intrusiva por ser lesiva de derechos fundamentales. Sin perjuicio de lo anterior, también destacaron que lo que vicia la prueba es el acceso no legítimo. En este sentido, la valoración de la legitimidad de la actuación inicial (acceso a la computadora que usaba el querellado) no puede hacerse más que mediante un juicio *ex ante*. A esos efectos es indiferente que solo se hayan buscado elementos que tuvieran relación con la actividad mercantil de la empresa o que se haya eludido cuidadosamente adentrarse en cualquier archivo o comunicación en la que se percibiese el más mínimo aroma de vinculación con la intimidad o la privacidad. Esto, que solo es posible dilucidar en un juicio *ex post,* no cambia ni puede cambiar la valoración que se hace *ex ante.*

Respecto a los mails examinados, mencionaron que ninguno de los presupuestos legitimadores aparece en los hechos. Los jueces insistieron que, en el caso presente, a la vista de la jurisprudencia existente y predominante en el momento de la actuación empresarial cuya licitud fiscalizamos ahora, se podía y debía haber extremado la cautela: *...no existiendo advertencia de que el ordenador había de ser usado exclusivamente para los fines de la empresa y no constando al empleado que la empresa se reservaba la potestad de su examen, por mucho que se utilizasen métodos informáticos especialmente poco invasivos y selectivos, constituía un cierto atrevimiento (una indiligencia), no recabar antes el consentimiento del titular o, en su defecto, la autoridad judicial. ... Algo de osadía se aprecia en la iniciativa adoptada por la empresa. La prueba no es rescatable; no puede utilizarse.*

Finalmente, la Sala entendió: *no se encuentran en condiciones en casación, al margen, por tanto, de toda inmediación, ni de dilucidar esas cuestiones, ni, una vez discriminado el material probatorio inservible de aquel que puede fundar una sentencia, ponderar si puede considerarse destruida la presunción de inocencia.* Ello obliga a reenviar la causa al Tribunal *a quo* para un nuevo enjuiciamiento que, partiendo de esa premisa ahora afirmada –el examen de la computadora vulneró derechos fundamentales– determine qué pruebas no están afectadas por esa realidad y si estas pueden apoyar o no un pronunciamiento de culpabilidad. *El defecto señalado no lleva a la absolución, sino a la reposición de las actuaciones al momento en que se produjo para su subsanación y continuación y nueva terminación de la causa con arreglo a derecho.*

Por último, agregó: *...la tarea de la Sala de Casación queda culminada con la primera sentencia y el reenvío de la causa al órgano de*

origen para reponerla al momento indicado y culminarle con arreglo a derecho. La causa finalizó estimando parcialmente el recurso de casación interpuesto por el recurrente, contra la sentencia dictada por el juez de instancia anterior en causa seguida contra el recurrente por un delito de administración desleal. Anularon la sentencia retrotrayendo las actuaciones al momento indicado para que sean tramitadas y concluidas con arreglo a derecho.

XIII. c. 3. Estados Unidos

Corte *Suprema de Los Estados Unidos de América. Causa N° 08/1332, caratulada "Ciudad De Ontario, California, Y Otros, Solicitantes C. Jeff Quon Y Otros", 560 U.S. 746 17 de junio de 201030*

El demandante, la ciudad de Ontario, adquirió localizadores alfanuméricos –*pagers*– capaces de enviar y recibir mensajes de texto los cuales serían entregados al Departamento de Policía de la Ciudad.

Al momento de adquirir los *pagers,* el Ayuntamiento anunció una "Política de uso de ordenadores, internet y correo electrónico" (Política de ordenadores) que se aplicaba a todos los empleados; asimismo, cada *pager* podía ser utilizado hasta determinado número de caracteres y, todos aquellos mensajes que superaran dicho límite deberían ser abonados de forma adicional.

Entre otras disposiciones, la política de uso especificaba que el Ayuntamiento "se reserva el derecho de supervisar y registrar toda la actividad de la red, incluido el uso del correo electrónico y de internet, con o sin previo aviso. Los usuarios no deben tener ninguna expectativa de privacidad o confidencialidad al utilizar estos recursos".

Así las cosas, el Ayuntamiento entregó los *pagers* al demandado Quon y a otros agentes del departamento de policía de Ontario, todos los cuales firmaron la política de uso.

Luego de varios meses de hacer uso de estos dispositivos, el jefe del Departamento de Policía detectó que tanto Quon como otros policías se excedían de forma regular en los límites de caracteres que tenían los

[30] Ver en https://caselaw.findlaw.com/us–supreme–court/08–1332.html

pagers. A raíz de esto, intentó determinar si este exceso era debido a mensajes enviados a raíz de su trabajo o bien eran mensajes relacionados con cuestiones personales, a fin de evaluar si debían ser afrontados por el Departamento y aumentar –en todo caso– el límite.

Así las cosas, después de que la empresa prestataria del servicio facilitara las transcripciones de los mensajes de texto de Quon y de otro empleado –de los meses agosto y septiembre de 2002–, se descubrió que muchos de los mensajes de aquel no estaban relacionados con el trabajo y que, algunos, eran sexualmente explícitos.

A partir de esta información, el jefe del Departamento de Policía remitió el caso a la división de asuntos internos del Departamento. Allí, el funcionario encargado de la investigación interna tomó como parámetro el horario de trabajo de Quon a fin de eliminar de la investigación todos aquellos mensajes enviados fuera de este, pero solo unos pocos podían ser excluidos. A raíz de ello, Quon fue sancionado por infringir las normas del Departamento.

Él y los demás demandados –cada uno de los cuales había intercambiado mensajes de texto con Quon durante los meses de agosto y septiembre– interpusieron una demanda, alegando –entre otras cosas– que se habían violado sus derechos de la Cuarta Enmienda y la Ley Federal de Comunicaciones Almacenadas (en adelante SCA) al obtener y revisar la transcripción de los mensajes del *pager* de Quon y que la empresa prestataria del servicio había violado la SCA al entregar dicha transcripción.

Por su parte, el Superior del Tribunal de Distrito revocó la decisión y, en este sentido, si bien coincidió en que Quon tenía una expectativa razonable de privacidad en sus mensajes de texto, este concluye que el registro no era razonable, aunque se realizara con una justificación legítima y relacionada con el trabajo; el dictamen señalaba una serie de medios menos intrusivos que podrían haber sido utilizados en la auditoría. Asimismo, el tribunal concluyó que la empresa prestataria había violado la SCA al entregar la transcripción.

Pues bien, llevado el planteo a la Corte Suprema de los Estados Unidos, sus integrantes rechazaron lo planteado por Quon. Según el voto del juez Kennedy –al cual adhirieron los otros miembros– se señaló: *este caso se refiere a la afirmación por parte de un empleador del gobierno (...) a leer los mensajes de texto enviados y recibidos en un localizador que el empleador poseía y entregó a un empleado. El empleado sostiene que la privacidad de los mensajes está protegida por la*

prohibición de registros e incautaciones irrazonables que se encuentra en la Cuarta Enmienda de la Constitución de los Estados Unidos, que es aplicable a los Estados por la Cláusula del Debido Proceso de la Decimocuarta Enmienda. Mapp v. Ohio, 367 U. S. 643 (1961). Aunque el caso afecta a cuestiones de gran importancia, el Tribunal concluye que puede resolverse mediante principios establecidos que determinan cuándo un registro es razonable.

Señaló el juez que, a primera vista, la política informática del Departamento no se aplicaría a los mensajes de texto enviados a través de *pagers,* dado que –si bien– comparten similitudes con un correo electrónico, ambos difieren en el hecho de que los mensajes de texto son enviados a través de estaciones base receptoras de frecuencias inalámbricas propiedad de la empresa que prestaba el servicio de *pagers* y, en el caso de los correos electrónicos, estos eran remitidos a través de los propios servidores propiedad de la Ciudad de Ontario.

El primer punto sobre el cual comienza a desarrollar su voto Kennedy es si Quon tenía una expectativa razonable de privacidad. Según las constancias de la causa, el Departamento de Policía estableció que los mensajes de los *pagers* no se consideraban privados. La política informática de la ciudad establecía: "los usuarios no deberían tener ninguna expectativa de privacidad o confidencialidad al utilizar" las computadoras de la ciudad. Aquí el punto radica en que, con posterioridad a firmar esa política, desde el Departamento de Policía se había aceptado la práctica de que Quon abonara el exceso en la tarifa que venía a raíz de los mensajes demás que enviaba, por ello, Quon sostenía podía esperar razonablemente que el contenido de sus mensajes siguiera siendo privado.

En relación con ello, el Juez se expidió señalando: *el Tribunal debe proceder con cuidado al considerar todo el concepto de expectativas de privacidad en las comunicaciones realizadas en equipos electrónicos propiedad de un empleador gubernamental.* El poder judicial corre el riesgo de equivocarse al elaborar demasiado las implicaciones de la Cuarta Enmienda de la tecnología emergente antes de que su papel en la sociedad haya quedado claro, e indicó: *La prudencia aconseja ser cauteloso antes de que los hechos del presente caso se utilicen para establecer premisas de gran alcance que definan la existencia, y el alcance, de las expectativas de privacidad de las que gozan los empleados cuando utilizan dispositivos de comunicación proporcionados por el empleador. Los rápidos cambios en la dinámica de la comunicación y la*

transmisión de información son evidentes no solo en la propia tecnología, sino en lo que la sociedad acepta como comportamiento adecuado.

Luego de otras consideraciones, el Tribunal concluyó que el registro estaba motivado por un propósito legítimo relacionado con el trabajo, y dado que su alcance no era excesivo, el registro era razonable y señaló que el demandado no podía tener una expectativa de privacidad amplia que implicara que su empleador no podría llegar a acceder a sus comunicaciones.

Corte *Suprema del Estado de Nueva Jersey, caratula "Marina Stengart V. Loving Care Agency, Inc., Steve Vella, Robert Creamer, Lorena Lockey, Robert Fusco, And Lca Holdings, Inc." 30 de marzo de 201031*

En el caso en cuestión la Suprema Corte resolvió que la política sobre el uso de los dispositivos de un empleador no amparaba –lo suficiente– su facultad de vigilar la cuenta de correo electrónico personal de un empleado cuando no notificaba expresamente de ello al empleado.

Al momento de resolver, los jueces señalaron que, en el lugar de trabajo moderno, por ejemplo, el uso personal y ocasional de internet es habitual; sin embargo, ese simple acto puede plantear cuestiones complejas sobre la vigilancia del lugar de trabajo por parte del empleador y la expectativa razonable de privacidad del empleado.

No obstante lo cual, el caso presentaba particularidades sobre la medida en que una empleada puede esperar privacidad y confidencialidad en los correos electrónicos personales con su abogado, a los que accedió en un dispositivo perteneciente a su empleador.

La demandante utilizó una *laptop* que le proporcionó la empresa para intercambiar correos electrónicos con su abogado a través de su cuenta de correo electrónico personal, protegida por contraseña y basada en la web. Con posterioridad a estas comunicaciones, presentó una demanda por discriminación laboral contra su empleador, Loving Care Agency, Inc. (Loving Care) y otros.

Al momento de aportar las pruebas al Tribunal en el marco de la demanda laboral, Loving Care contrató a un experto en informática forense para recuperar todos los archivos almacenados en la *laptop*,

[31] Consultado en https://caselaw.findlaw.com/nj–supreme–court/1522648.html

incluidos los correos electrónicos, que se habían guardado automáticamente en el disco duro, los cuales fueron revisados y utilizados como elemento de prueba.

El tribunal de primera instancia había sostenido que, a la luz de la política escrita de la empresa en materia de comunicaciones electrónicas, la demandante renunció al privilegio abogado-cliente al enviar correos electrónicos en una computadora de la empresa; fallo que fuera revertido por la Cámara de Apelaciones.

Los jueces de la Suprema Corte fallaron en este último sentido y sostuvieron que, dadas las circunstancias, Stengart podía esperar razonablemente que las comunicaciones por correo electrónico con su abogado a través de su cuenta personal siguieran siendo privadas, y que enviarlas y recibirlas a través de una *laptop* de la empresa no eliminaba el privilegio abogado-cliente que las protegía.

Cámara de Apelaciones del Estado de California. - N° C059133, caratulada "Gina M. Holmes V. Petrovich Development Company, Llc". 13 de enero del 2011

En el caso, se resolvió que los correos electrónicos enviados por la demandante, Holmes, a su abogado –en relación con una posible acción legal contra la empresa Petrovich, sus empleadores y los demandados– no constituyeron *una comunicación confidencial entre el cliente y el abogado;* ello, toda vez que la demandante utilizó una computadora de la empresa demandada para enviar los correos electrónicos a pesar de que (1) se le había informado de la política de la empresa de que sus dispositivos debían utilizarse únicamente para asuntos de la empresa y que los empleados tenían prohibido utilizarlos para enviar o recibir correo electrónico personal, (2) se le había advertido de que la empresa supervisaría sus computadoras para comprobar el cumplimiento de esta política de la empresa y, por tanto, podría *inspeccionar todos los archivos y mensajes en cualquier momento*, y (3) se le había advertido explícitamente de que los empleados que utilizaran las computadoras de la empresa para crear o mantener información o mensajes personales *no tienen derecho a la privacidad con respecto a esa información o mensaje.*

La Corte de Apelaciones aclaró *que una comunicación entre abogado y cliente no pierde su carácter privilegiado por la única razón de que se comunique por medios electrónicos o porque las personas que partici-*

pan en la entrega, facilitación o almacenamiento de la comunicación electrónica puedan tener acceso al contenido de la comunicación.

Sin embargo, en el caso particular, el Tribunal sentenció que no había tal privilegio en los emails enviados por la demandante a su abogado, ya que los correos electrónicos enviados a través de los dispositivos de la empresa en las circunstancias analizadas eran similares a consultar a su abogado en la sala de conferencias de su empleador, en voz alta, con la puerta abierta, de modo que cualquier persona razonable, esperaría que su discusión con las quejas sobre su empleador fuera escuchada por él. Al utilizar el dispositivo de la empresa para comunicarse con su abogado, sabiendo que las comunicaciones violaban la política del uso de los dispositivos de informática de la empresa y que podían ser descubiertas por su empleador debido a la supervisión del uso del correo electrónico por parte de la empresa, la demandante no se comunicó *de forma confidencial por medios que, en conocimiento del cliente, no revelan la información a otras personas que no sean las que están presentes para promover el interés del cliente en la consulta o aquellas a las que la revelación es razonablemente necesaria para la transmisión de la información o el cumplimiento del propósito para el que se consulta al abogado.*

El manual del empleado, que Holmes admitió haber leído y firmado, contenía disposiciones que explicaban claramente la política relativa al uso de los recursos tecnológicos de la empresa, como computadoras y cuentas de correo electrónico corporativo.

Aquel indicaba a los empleados, que los recursos tecnológicos de la empresa deben utilizarse únicamente para los asuntos de la empresa y que los empleados tienen prohibido enviar o recibir correos electrónicos personales. Además, el manual advertía: *los empleados que utilicen los recursos tecnológicos de la empresa para crear o mantener información o mensajes personales no tienen derecho a la privacidad con respecto a esa información o mensaje* e indicaba que la empresa podía *inspeccionar todos los archivos o mensajes en cualquier momento y por cualquier motivo a su discreción* y que supervisaría periódicamente sus recursos tecnológicos para comprobar el cumplimiento de la política de la empresa.

XIV. Entrevistas

A continuación se transcriben las entrevistas desarrolladas con los especialistas técnicos Pablo Romanos y Adrián Acosta.

XIV. a. Pablo Romanos

¿Cuál es su experiencia, en caso de tenerla, de la utilización de drones en las investigaciones judiciales?
Pablo Romanos: No he trabajado directamente, ya que lo que hice fue desarrollar la herramienta de investigación y los que los utilizaron fueron las fuerzas del Centro de Investigación Judicial. Se hicieron algunas pruebas por parte de la Policía de la Ciudad de Buenos Aires y el Ministerio Público Fiscal.

¿Cuál es el mecanismo desarrollado para la utilización de Crozono?
Se trata de una herramienta que básicamente se enfoca en la adquisición de evidencia remota, accediendo a distancia a información que puede estar almacenada o trasmitida desde una red en una conexión pública. Se trata de una herramienta de "remote forensic" básico, fue diseñada para ejecutarla desde un dron o un robot, que va a ejecutar la

herramienta de forma automática una serie de procesos que se dividen en tres partes.

La primera es la exploración, un método de "Discovery" de forma aérea en el que se hace un reconocimiento físico de la zona que se busca reconocer. Es un proceso de barrido similar al rastrillaje en el que se busca puntos de acceso a wifi.

Esta fase tiene una parte de reconocimiento, otra de procesamiento y genera reportes. Que culmina en los reportes de todos los puntos de acceso wifi de la zona. En este primer paso se levantan varios puntos de acceso, dependiendo del lugar. Por ejemplo, en la zona del Obelisco (N. de R. Corrientes y 9 de Julio y alrededores) hemos efectuado pruebas y se han detectado cerca de 300 puntos.

Vale aclarar que en este primer paso se trata de una técnica de investigación en redes abiertas (OSINT), no está "rompiendo" ninguna clave ni realizando ninguna técnica de "remote forensic".

¿Y se pueden realizar técnicas de *remote forensics*?

Una vez que se determina los puntos de acceso que se quieren investigar, se pasa a la segunda fase que denominada "Crozono auditor" que utiliza técnicas para poder romper contraseñas, capturando de forma abierta información de los canales de comunicación del punto de acceso tratando de *crackear* la contraseña. Este proceso no es rápido y a veces se demora, ya que lo que hace el dron es capturar el tráfico que hay entre los clientes que están conectados al punto de acceso, copiarla y a partir de esa información *crackear* la contraseña.

¿Sería una interceptación de datos en tiempo real?

Lo que hace es capturar el *handshake* que sería el cruce de manos entre el cliente y el SSID-wifi. Cuando se quiere conectar un dispositivo a una red de wifi hay un proceso que se llama "handshake" en el que hay un intercambio de datos básico, y es en ese proceso en el que se "negocia" la contraseña. Lo que hace el proceso es "capturar" esa negociación y trabajar con el concepto de *hash*, tratando de romper la contraseña sobre la base de colisiones de *hash*.

El proceso es el siguiente: alguien tiene un punto de acceso desde un celular. El dron lo que hace es cortar la conexión, *desautenticarla*, ya que en el momento en que se intenta conectar de nuevo, es decir, se vuelve a negociar la contraseña. El sistema puede capturar la información y puede averiguar la contraseña. Entonces, *desauntetica* a todos

los clientes, que luego buscan establecer nuevamente la conexión, y en el momento que se conectan el dron captura el *hanschake* y lo lleva al servidor a efectos de establecer la contraseña.

Después de *crackear* la contraseña, el dron accede al wifi, y se pone como un dispositivo más dentro de la red del sospechoso y empieza a enumerase como un equipo más y "ver" qué equipos hay alrededor, para poder realizar una serie de pruebas más complejas.

Una vez que se "rompe" la puerta de entrada al domicilio, se procede a ejecutar un procedimiento específico que depende del delito que se investiga. Hay uno para los casos de tenencia y distribución de imágenes de explotación sexual infantil, daño informático, fraude informático y a la propiedad intelectual. La herramienta hace el procedimiento de forma automática. Por ejemplo, en el caso de casos de explotación sexual infantil el programa indagará el sistema operativo del sospechoso, cuáles aplicaciones tiene abiertas, los servicios, a qué redes está conectado, y a partir de una base de datos de hashes, busca la colisión con los *hashes* de las imágenes que tiene el sospechoso en el disco.

Hay que entender que se trata de un "entorno vivo" que permite acceder a contraseñas y claves criptográficas que se perderían si se realiza un allanamiento, se desconectan los equipos y se los lleva a un laboratorio para analizar.

Hay cinco formas de acceder remotamente al equipo. El primero es el "troyano o *malware* judicial" y se da a partir de una conexión a internet de forma directa. Después existe la forma básica de hacer un *pentest* de forma manual; la forma de acceso a través de una antena, similar a lo que se hace con los drones. Luego se encuentra el agente encubierto, que físicamente puede acceder a un domicilio, colocar un *pendrive* en un dispositivo o instalar un *malware*, y finalmente lo que se hace con este mecanismo de drones.

XIV. b. Entrevista a Adrián Acosta

¿Qué conocimiento tiene de la utilización de *software judicial* a distancia en el marco de investigaciones judiciales?

La Argentina y el resto de los países de Latinoamérica y el Caribe están atrasados en diferentes áreas. Primero la parte jurídica en la que aparecen criterios más restrictivos respecto de la implementación de las técnicas de *remote forensics*. Es un proceso que también atravesó Europa,

que avanzó en adaptar su legislación, pero actualmente se encuentra en problemas para implementar este tipo de medidas por no contar con las herramientas forenses adecuadas.

Esto ocurre porque no es lo mismo una herramienta de inteligencia que una herramienta forense. Esta última tiene que *levantar el hash* que garantiza la integridad de la información y tiene que tener una validación. Es decir, no sirve cualquier *software*. Un *software* que levante una imagen exacta de un teléfono celular puede servir para inteligencia, pero no para validarlo como prueba en un proceso judicial.

Es un paralelismo con la interceptación de comunicaciones, que se utiliza en tareas de investigación para fundar una orden de allanamiento, o detenciones, pero como información.

Se necesitan tres aspectos para darles cause a las técnicas de *remote forensics:* en el ámbito legislativo con una norma que permita realizar este tipo de tareas, en el ámbito jurisdiccional con magistrados que dicten órdenes apropiadas para llevarlas a cabo y, finalmente, en el ámbito técnico, con herramientas que permitan aplicarlo.

Tenemos el ejemplo del *Software* "Antorcha" en Chile, que se utilizó para un caso particular en el que el abogado defensor del imputado solicitó el código fuente del *software* para saber cómo se utilizó. Algo similar a lo ocurrido en el caso "playpen".

¿Han existido planteos similares por la utilización del *software* directamente y no sobre la legalidad o ilegalidad de la medida?
En España, en años anteriores, ocurrió que los órganos de investigación contaban con la herramienta jurídica pero no con la técnica. Este es el gran desafío que tienen los países. Creo que además de la admisión legislativa de la medida, se debería desarrollar un registro de los *software* para utilizar para que no haya cuestionamientos sobre cuál se puede utilizar y cuál no.

¿Existen diferentes tipos de programas para realizar las medidas?
Hay hasta *software* "o click" que, con un dato de correo electrónico o número telefónico asociado la línea telefónica que se lo ataque y en pocos minutos se logra *levantar* la información.

Ahora bien, a partir de estas cuestiones cobra relevancia los cuestionamientos que puede haber sobre el derecho a la privacidad –para qué se buscan correos electrónicos si en la investigación se buscan imágenes de explotación sexual infantil, por ejemplo– sumado la nece-

sidad de una adecuada adquisición de la evidencia, ya que cuando hay un secuestro de dispositivos el procedimiento es diferente: se necesita aplicar un código *hash* para que se pueda comparar la información obtenida del dispositivo y alojada en este. Ya que cuando se secuestran dispositivos y se realizan pericias, se necesita poner un bloqueador de escritura y conectarlo al sistema para extraer la información que se precisa y, en caso de haber planteos de las partes, se cuenta con el dispositivo para poder cotejar. En cambio, al obtener la evidencia remotamente no se puede llevar adelante el mismo procedimiento ya que no se cuenta con el dispositivo. Si el usuario modifica en tiempo real la información, no se va a poder comparar el código *hash* que se aplica a la evidencia obtenida. Por ejemplo, si el usuario borra toda la información que se obtuvo mediante técnicas de *remote forensic*, ¿cómo se puede comprobar que se obtuvo de ese dispositivo en particular? Entonces, lo importante en este tipo de investigaciones termina siendo la necesidad de contar con el dispositivo físico.

XV. Bibliografía consultada

Aboso, G., "Acceso indebido a las comunicaciones electrónicas en el ámbito laboral (art. 153 del Código Penal)" –en Dupuy, D. y Kiefer, M. *Cibercrimen* –. Buenos Aires, Editorial Bdef, 2017.

Castex, F., *Responsabilidad penal de la persona jurídica y compliance*, Buenos Aires, Editorial Ad-Hoc, 2018.

Carrió, A., *Garantías Constitucionales en el Proceso Penal*, 6ta ed., Buenos Aires, Hammurabi, 2015.

Daray, R., y otros, *Código Procesal Penal Federal. Análisis doctrinal y jurisprudencial*, 2da. ed., Buenos Aires, Hammurabi, 2021.

Daskal, The un-territoriality of data, en *Yale Law Journal*., Vol. 125, 2015.

Dupuy, D., y otros, *Cibercrimen II*, Buenos Aires, Bdef, 2018.

Hairabedián, M., "El acceso a información y datos de teléfonos celulares", en Dupuy y Kiefer (Dir.) *Cibercrimen. Aspectos del derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet*, Buenos Aires, Bdef, 2017.

Kerr, O., Search and Seizures in a Digital World, en *Harvard Law Review*, Vol. 531, 2005.

Kerr, O., Ex ante regulations of computer search and seizure, en *Virginia Law Review*, Vol. 96, N.° 6, 2010.

Kerr, O., *Computer Crime Law*, 3ra. ed., West, Minnesota, 2013.

Kerr, O., Executing warrants for digital evidence: the case for use restrictions on nonresponsive data, en *Texas Tech Law Review*, Vol. 48, N.° 1, 2015.

Kerr, O., y Schneier, B., Encryption Workarounds, en *Georgetown Law Journal*, Vol. 106, Issue 4, 2018.

Kerr, O., Compelled Decryption and the Privilege against Self-Incrimination, en *Texas Law Review*, Vol. 97, Issue 4, 2019.

Ortiz Padrillo, J.C., *Problemas procesales de la ciberdelincuencia*, Madrid, Colex, 2013.

Palazzi, P., *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, Buenos Aires, Abeledo Perrot, 2016.

Polansky, J., *Garantías Constitucionales del procedimiento penal en el entorno digital*, Buenos Aires, Hammurabi, 2020.

Portillo, V., "Autoincriminación y nuevas tecnologías", en Riquert (dir) *Sistema penal e informática*, Buenos Aires, Hammurabi, 2019.

Salt, , M. *Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ad-Hoc, 2017.

Sánchez-Rodas Navarro, C. – "Información y Derecho: Restricciones en el uso del correo electrónico e internet por parte de los trabajadores por cuenta ajena", en Información, Libertad y Derechos Humanos. La enseñanza de la Ética y el Derecho de la Información, 2° Congreso Internacional de Ética y Derecho de la Información, disponible en https://eprints.ucm.es/id/eprint/6128/1/definitivo2.pdf. Valencia, 2005.

Sosa Escudero, W., *Big data*, 5ta ed., Buenos Aires, Siglo XXI Editores, 2019.

Sueiro, C. C., *Criminalidad Informática–La eficacia de la reforma al Código Penal en materia de delitos informáticos – Análisis de las leyes 26.388, 26.685 y 26.904*, Editorial Ad-Hoc, 2016.

Las autoras y los autores

Marcos Salt
Abogado (UBA). Doctor en Derecho (Universidad de Córdoba). Director de la Carrera de Especialización en Cibercrimen y Evidencia Digital Facultad de Derecho UBA. Profesor de Derecho Penal y Procesal Penal UBA.
msalt@derecho.uba.ar

Clementina Anselmi
Abogada (UBA).
anselmiclementina@gmail.com

Alejandra Daglio
Abogada (UBA) con orientación en Derecho Penal. Especialista en Cibercrimen y Evidencia Digital (UBA). Diplomada en Derecho Parlamentario (Universidad Austral). Consultora en reformas legales.
daglio389@gra.derecho.uba.ar

Esteban Diak
Abogado (UNLZ), con orientación en derecho penal y penal económico, diplomado en cibercrimen y evidencia digital, diplomado en inteligencia estratégica y maestrando en Ciberdefensa y Ciberseguridad
estebandiak@uca.edu.ar

Camila Engelberg
Abogada especialista en Derecho Penal (UBA). Diplomatura de extensión en "Modelos y prácticas de autogestión, lógicas de cuidado y justicia restaurativa en contexto de encierro" (Universidad Nacional de Mar del Plata). Jefa de despacho en la Defensoría Pública Oficial ante los Juzgados Federales de Primera Instancia en lo Criminal y Correccional Nro. 2 de Morón.
cengelberg@mpd.gov.ar

Martín Gershanik
Abogado (UBA) especialista en derecho penal, experto en políticas públicas en materia de justicia, consultor internacional en modernización y administración de justicia, evidencia digital y ciberdelito.
martin.gershanik@gmail.com

Ana Juárez
Profesora Adjunta Interina de la materia Parte especial del derecho penal de la cátedra del Prof. Fernando Córdoba (UBA). Especialista en derecho penal (UBA), maestranda en Derecho Penal (UBA y U. Sevilla). Profesora de posgrado de la materia Dogmática penal y ciberdelincuencia de la Carrera de Especialización en Cibercrimen y Evidencia Digital (UBA).
anajuarez@derecho.uba.ar

Ariel Liniado
Abogado (UBA). Profesor de Derecho penal (UBA y INSSP). Maestreando en Derecho penal por la Universidad de San Andrés. Ex becario de grado de la Université Catholiqué de Louvain y ex becario de grado UBACyT.
liniado@pvlabogados.com

Noelia Matalone
Abogada (UBA). Investigadora y docente en derecho penal e internacional penal (UBA-UNDAV-UTDT). Especialista en derecho penal y maestranda (UTDT).
nmatalone@derecho.uba.ar

Gabriel Páramos
Especialista en Derecho Penal (UBA). Docente en la asignatura Régimen del Proceso Penal. Facultad de Derecho (UBA). Cátedra del Profesor Fernando Córdoba.
gparamos@mpf.gov.ar

Mariana Piccirilli
Abogada (UCA), con orientación en derecho penal y penal económico. Maestrando en Ciberdefensa y Ciberseguridad. Diplomada en Prevencion de Lavado de Activos, Cibercrimen y Evidencia Digital y en Inteligencia Estrategica.
piccirillimaranam@gmail.com

Jonathan Polansky
Abogado, UBA; LL.M., Columbia University
jpolansky@derecho.uba.ar

Víctor Hugo Portillo
Abogado. Especialista en Derecho Penal (UBA). Doctorando en Derecho (UBA). Docente en Elementos de Derecho Penal y Procesal Penal Fac. De Derecho (UBA). Docente de Posgrado. Coordinador de la Carrera de Especialización en Cibercrimen y Evidencia Digital (UBA).
vportillo@derecho.uba.ar

Fernnado Quinteiro Vila
Abogado (UBA), con orientación en derecho penal especializado en ciberseguridad y seguridad de la información.
quinteiro085@est.derecho.uba.ar

Julián Martín Reale
Magíster en Derecho de la Ciberseguridad y Entorno Digital (Universidad de León, España - Becado por Fundación Carolina de España). Abogado especializado en derecho penal (UBA), cibercrimen y evidencia digital (UBA), protección de datos personales (Univ. Nebrija de Madrid) y seguridad de la información (UTN).
reale954@gra.derecho.uba.ar

Julieta Micaela Ríos
Estudiante de Derecho (UBA) con orientación en Derecho Penal. Colaboradora en Programa en Cibercrimen y Evidencia Digital (UBA).
rios508@est.derecho.uba.ar

Braian Matías Werner
Abogado (UBA) con orientación en Derecho Penal, con posgrado en Cibercrimen y Evidencia Digital (UBA). Consultor en ciberseguridad y privacidad.
drmatiaswerner@gmail.com

Se agradece a Mariana Kiefer y Catalina Neme por los aportes realizados en el inicio del presente proyecto de investigación.