Revista Electrónica de Estudios Penales y de la Seguridad
ISSN: 2531-1565

EL HACKEO MASIVO COMO HERRAMIENTA CONTRA EL CRIMEN ORGANIZADO. ANÁLISIS CONSTITUCIONAL Y LEGAL DE LOS CASOS ENCROCHAT, SKY ECC Y AN0M

MASSIVE HACKING AS A TOOL AGAINST ORGANIZED CRIME. CONSTITUTIONAL AND LEGAL ANALYSIS OF THE ENCROCHAT, SKY ECC AND AN0M CASES

Hernán Blanco
Secretario Letrado
Corte Suprema de Justicia de la Nación (Argentina)

Fecha de recepción: 1 de mayo de 2023.

Fecha de aceptación: 8 de noviembre de 2023.

RESUMEN

Las operaciones policiales concretadas entre 2020 y 2021, en las que se recurrió a herramientas tecnológicas avanzadas para permitir el monitoreo de las comunicaciones de los usuarios de los sistemas de mensajería encriptada EncroChat, Sky ECC y An0m, son casi unánimemente consideradas como las más importantes y exitosas de la historia contra el crimen organizado trasnacional. Sin embargo, la adopción de una estrategia centrada en la vigilancia masiva y simultánea de decenas de miles de personas y en el uso de programas informáticos espía ha puesto en crisis las concepciones establecidas en la tradición jurídica europea en cuestiones como la vigencia del principio de territorialidad en orden a la aplicación de la ley procesal; el alcance del derecho a la intimidad y la proporcionalidad de las injerencias estatales sobre el mismo; y el equilibrio entre el derecho de los acusados a controlar la prueba de cargo y el interés de las agencias de orden público en mantener la confidencialidad de las herramientas tecnológicas utilizadas para concretar la vigilancia. Hasta el momento, los tribunales nacionales europeos han optado mayoritariamente por sostener la legitimidad de las medidas adoptadas, aunque la palabra final está llamada a ser del Tribunal Europeo de Derechos Humanos, sin que esté claro si la actuación estatal en estos casos se ajusta, o no, a los parámetros establecidos en la jurisprudencia del referido tribunal sobre la materia.

ABSTRACT

The police operations that took place in 2020 and 2021, involving the use of advanced technological tools to eavesdrop on the communications of users of encrypted

messaging services EncroChat, Sky ECC and An0m, are almost unanimously considered as the most successful in history against transnational organized crime. However, the governmental use of spyware to carry on massive and simultaneous surveillance of thousands of people has challenged the assumed notions in European criminal law tradition regarding matters such as the territoriality principle; the limits of the right to privacy and the proportionality of the government's interference with it; and the balance between the defendant's right to confront incriminatory evidence and the government's interest in protecting the confidentiality of advanced surveillance tools. Even though, until now, European domestic courts have generally validated the surveillance measures adopted by police forces in these cases, the matter is most likely to be resolved by the European Court of Human Rights, since it is still not clear if the governments' behavior is in line with the standards set forth in the court's jurisprudence.

PALABRAS CLAVE

Govware – Transfronterizo – Proporcionalidad - Igualdad de armas.

KEYWORDS

Govware – Transborder – Proportionality – Equality of arms.

ÍNDICE

jurisprudencia de la Corte de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos. **5. CONFLICTO ENTRE EL DERECHO A CONTROLAR LA PRUEBA DE CARGO Y LA CONFIDENCIALIDAD DE LAS HERRAMIENTAS DIGITALES. IGUALDAD DE ARMAS.** 5.1. Planteos de las defensas contra la confidencialidad de las herramientas informáticas utilizadas en EncroChat. 5.2. Respuesta de los tribunales nacionales europeos a planteos sobre violación al derecho de defensa e igualdad de armas. 5.3. El derecho a controlar la prueba de cargo y la igualdad de armas en la jurisprudencia del Tribunal Europeo de Derechos Humanos. **6. BIBLIOGRAFÍA**.

SUMMARY

1. INTRODUCTION: NEW TECHNOLOGIES' INFLUENCE ON THE GOVERNMENT'S ABILITY TO INTERCEPT COMMUNICATIONS. 2 OVERVIEW OF POLICE OPERATIONS AGAINST ENCROCHAT, SKY ECC & AN0M. 2.1. French Gendarmerie's operation against EncroChat and its repercussions. 2.2. Belgium security forces' operation against Sky ECC and its repercussions. 2.3. FBI and Australian Federal Police's operation with An0m and its repercussions. 2.4. The controversies regarding EncroChat, Sky ECC and An0m police operations in European courts. An introduction. **3. TRASNATIONAL OPERATIONS AND THE TERRITORIALITY PRINCIPLE.** 3.1. The transnational enforcement of domestic procedure law in the EncroChat, Sky ECC and An0m cases. 3.2. Legitimacy of evidence obtained through transnational use of informatic tools. Applicable laws, academic positions and standards set forth in the jurisprudence of the European Court of Human Rights. 3.3. Motions against the use of evidence produced by transnational surveillance measures. Domestic court's responses. Result of the inquiry to the CJEU. **4. GOVERNMENTAL INTERFERENCE WITH THE RIGHT TO PRIVACY & SECRECY OF COMMUNICATIONS. PROPORTIONALITY AND PARTICULARITY PRINCIPLES.** 4.1. The right to privacy in European law. 4.2. The scope of the right to privacy according to European and American courts. 4.3. Preliminary analysis on the proportionality of the government's interference on the right to privacy. 4.4. The standards set forth by the European Court of Justice and the European Court of Human Rights. **5. CONFLICT BETWEEN THE ACCUSED'S RIGHT TO CONFRONT INCRIMINATORY EVIDENCE AND THE CONFIDENTIALITY OF DIGITAL TOOLS. EQUALITY OF ARMS.** 5.1. Defense's motions against the confidentiality of the informatic tools used in the EncroChat operation. 5.2. The European domestic court's response to objections regarding the rights to fair trial and equality of arms. 5.3. The right to confront incriminatory evidence and equality of arms according to the European Court of Human Rights. **6. BIBLIOGRAPHY**.

1. INTRODUCCIÓN: LAS NUEVAS TECNOLOGÍAS Y LA SUBSISTENCIA DE LA FACULTAD ESTATAL DE INTERCEPTAR DE LAS COMUNICACIONES.

Desde los albores de la lucha de los estados contra las distintas modalidades de criminalidad organizada, hace casi un siglo, la interceptación y monitoreo de las comunicaciones viene ocupando un lugar central, preponderante, en las

investigaciones conducidas por las agencias de orden público respecto de las bandas criminales de todo tipo, incluyendo también a las que se dedican a cometer actos terroristas. Los motivos por los que ello es así son evidentes: cuando el objeto de la pesquisa es el accionar de organizaciones regidas por rígidos códigos de silencio, fundamentales para la subsistencia de la agrupación y el éxito de su actividad ilícita, es difícil sobrestimar la utilidad de una herramienta de investigación que permite obtener evidencia *desde dentro*, generada (involuntariamente) por los propios protagonistas de la conducta ilegal, en lugar de intentar inferir qué está ocurriendo *desde fuera*.

Sin embargo, a partir del surgimiento de la Internet y su expansión global, comenzaron a aparecer nuevas tecnologías de la información y la comunicación (TICs) que pusieron en crisis la facultad estatal de monitorear las comunicaciones de los ciudadanos, no desde el punto de vista legal, sino en el plano técnico. Ello así desde que, por un lado, las comunicaciones a través de la Internet se concretan en forma *no intermediada* ("par a par"), es decir suprimiendo el punto focal en el que se llevaba a cabo la interceptación de las comunicaciones concretadas a través de la Red de Telefonía Pública Conmutada (RTCP); mientras que -por el otro- la confidencialidad de los "paquetes de datos" (incluyendo las comunicaciones) que transitan por la Internet se resguarda echando mano a una herramienta informática que oscurece su contenido, impidiendo que pueda ser interpretado por terceros no autorizados: la encriptación.

Debido a ello, desde 2010 distintas agencias de investigación, comenzando con el FBI, han comenzado a advertir sobre el riesgo de "quedarse a oscuras" ("going dark")[1], derivado de la creciente adopción -no sólo por parte de los criminales, sino del público en general- de métodos de comunicación desligados de la telefonía tradicional (como por ejemplo Skype o Facetime), que impiden o dificultan en gran medida el monitoreo por parte de las autoridades estatales. Esta situación se agravó considerablemente a partir de las revelaciones de el ex agente de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) estadounidense Edward Snowden sobre espionaje del gobierno de ese país a sus ciudadanos[2], que llevó a las principales compañías tecnológicas a implementar sistemas avanzados de encriptación "punto a punto" ("end-to-end") en los sistemas de mensajería más populares (Whatsapp, Messenger, Telegram, etc.). La principal consecuencia de ello es que hoy, las empresas proveedoras del servicio se ven imposibilitadas de detectar conductas o materiales

[1] El término fue utilizado públicamente por primera vez cuando la Consejera General del FBI, Valerie Caproni, compareció ante el Comité Judicial del Senado de los EE.UU. y usó la frase "quedar a oscuras" para referirse a la creciente brecha entre la facultad legal de las agencias gubernamentales para interceptor comunicaciones electrónicas y su capacidad práctica para hacerlas efectivas (ver: CAPRONI, Valerie: *Statement of the General Counsel of the Federal Bureau of Investigations before the House Judiciary Committee, Subcommitee on Crime, Terrorism, and Homeland Security*, Washington D.C., publicado el 17/2/2011).

[2] Al respecto, ver: GELLMAN, Barton / POITRAS, Laura, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", en The Washington Post, publicado el 7/6/2013; PELROTH, Nicole / LARSON, Jeff / SHANE, Scott, "NSA able to foil basic safeguards of privacy on web" en The New York Times, publicado el 5/9/2013; GELLMAN, Barton / SOLTANI, Ashkan, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", en The Washington Post, publicado el 30/10/2013; entre muchos otros.

ilícitos en las comunicaciones de los usuarios y prestar colaboración a las autoridades en relación con dichas conductas[3].

En tal contexto, y según señalan EUROPOL y EUROJUST, las agencias de orden público han reportado el uso de encriptación como herramienta "anti-forense" en la mayoría de sus casos[4]. Los sistemas de mensajería encriptada son utilizados en las comunicaciones entre criminales dedicados a un amplio rango de actividades delictivas. La mayoría de los casos se vinculan con el narcotráfico y otras modalidades de criminalidad organizada, pero también en investigaciones vinculadas a cibercrímenes, homicidios, blanqueo de capitales y distintos tipos de fraudes[5].

La respuesta inicial de las agencias de orden público y el poder político en muchos países consistió en reclamar la implementación de mecanismos para reestablecer la "interceptabilidad técnica" de estas nuevas formas de comunicación[6]. En igual sentido, los países miembros de la Unión Europea exhortaron a la implementación de soluciones para permitir el acceso de las autoridades a la evidencia digital sin prohibir o debilitar la encriptación en una reunión de ministros de justicia e interior en diciembre de 2016, llamamiento que fue reiterado por los jefes de gobierno en junio de 2017[7]. Sin embargo, pronto quedó demostrado que la introducción de estas "puertas traseras" ("backdoors") resulta imposible sin comprometer seriamente la seguridad de todo el ecosistema de comunicaciones por Internet, lo cual la torna inviable como solución al problema planteado[8].

En este escenario, comenzó a cobrar relevancia la posibilidad de recurrir a programas espías estatales ("govware"), como alternativa para poder acceder a la información en formato plaintext (incluyendo a las comunicaciones) sin necesidad de debilitar las herramientas de encriptación que constituyen el fundamento de los sistemas de seguridad de la Internet[9]. En esa dirección, distintas organizaciones

[3] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function on encryption* (joint report), European Commision, 2021, pág. 30.
[4] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 30.
[5] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 14.
[6] Así, por ejemplo, fiscales generales de los EE.UU., Francia, el Reino Unido y España publicaron una columna de opinión en el New York Times reclamando acceso estatal a los datos encriptados (ver: VANCE Jr., Cyrus R. / MOLINS, François / LEPPARD, Adrian / ZARAGOZA, Javier, "When phone encryption blocks justice", NY Times OpEd., publicada el 11/8/2015).
[7] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 30 (citas omitidas).
[8] En relación con esta cuestión, resulta de interés, sobre todo, el documento publicado por algunos de los principales expertos en ciberseguridad de los EE.UU., detallando los motivos por los que resulta inviable la implementación de "backdoors". Ver: ABELSON, Harold / ANDERSON, Ross / BELLOVIN, Steven M. / BENALOH, Josh / BLAZE, Matt / DIFFIE, Whitfield / GILMORE, John / GREEN, Matthew / LANDAU, Susan / NEUMANN, Peter G. / RIVEST, Ronald L. / SCHILLER, Jeffrey I. / SCHNEIER, Bruce / SPECTER, Michael / WEITZNER, Daniel J., *Keys under doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology Science and Artificial Intelligence Laboratory, publicado el 6/7/2017.
[9] Ver, por ejemplo: BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan, "Going bright: Wiretapping without weakening communications infrastructure", en IEEE Security & Privacy, vol. 11, N° 1, 2013, págs. 62/72; y "Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet", en Northwestern Journal of Technology and Intellectual Property, vol. 12, nro. 1, 2014, págs. 1/64; BOJARSKI, Kamil, "Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations", en The European Review of Organized Crime, vol. 2, N° 2, 2015, págs. 25/50; HENNESSEY, Susan, "The elephant in the room: Addressing child exploitation and going dark", en Hoover Institution,

vinculadas al cumplimiento de la ley, como la Asociación Internacional de Jefes de Policía (IACP, por sus siglas en inglés) o EUROPOL han destacado que el acceso a datos encriptados mediante el uso de técnicas de hackeo (con autorización legal) presentan ventajas significativas para los investigadores[10], toda vez que la recolección de la evidencia digital contenida en los equipos utilizados por los delincuentes resulta "esencial" para el éxito de las investigaciones criminales[11]. En los últimos quince años, han empezado a multiplicarse los casos de uso de govware, primero en los EE.UU. y luego en Europa, a punto tal que varios países (entre ellos, Francia, Países Bajos, el Reino Unido y Portugal, entre otros) han regulado expresamente el recurso a esa medida en su legislación procesal.

El siguiente paso en esta suerte de "carrera armamentística" tecnológica entre las agencias de orden público y los delincuentes fue el surgimiento de sistemas cerrados de mensajería encriptada, desarrollados (y en muchos casos comercializados) casi exclusivamente para el uso de las organizaciones criminales. Las compañías que desarrollaron estos sistemas, centrados el uso de "teléfonos inteligentes" (smartphones) modificados para minimizar el riesgo de intrusión mediante programas espías, prometían a sus clientes una protección casi impenetrable contra el monitoreo estatal, aspecto que convirtió a dichos equipos en una herramienta extraordinariamente útil para los grupos criminales cuya operatoria demanda un alto grado de coordinación *en tiempo real* entre los involucrados, tal como sucede -por ejemplo- con el narcotráfico[12].

Entre las primeras compañías en ofrecer este servicio estuvieron MPC (creada, de hecho, por una organización criminal dedicada al narcotráfico en Escocia)[13] y -sobre todo- la empresa canadiense Phantom Secure, que inició su actividad en 2008 y suministró equipos a bandas de narcotraficantes como el Cartel de Sinaloa, entre otros[14]. En 2018, existían en el mundo alrededor de 10.000 dispositivos con el sistema Phantom Secure, todos ellos Blackberries modificados suprimiendo la cámara, el micrófono y el GPS, programados para comunicarse únicamente con otros equipos de la misma red. Todos los mensajes intercambiados en la red Phantom Secure circulaban a través de servidores ubicados en Panamá y Hong Kong, ocultando su ubicación mediante servidores proxy[15]. La compañía garantizaba, asimismo, que los mensajes

---

Stanford University, Aegis Paper Series, N° 1701, 2017; y KERR, Orin S. / SCHNEIER, Bruce, "Encryption workarounds", en Georgetown Law Journal, vol. 106, N° 4, 2018, págs. 989/1019; entre otros.

[10] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices*, European Union, 2017, pág. 8.

[11] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 26.

[12] Ver: Departamento de Justicia de los EE.UU. (DOJ), Declaración jurada en apoyo de pedido de orden para interceptación de comunicaciones, Tribunal Federal del Distrito Sur de California, caso 21 MJ01948, pág. 5.

[13] Cfr. COX, Joseph: "How police secretly took over a global pone network for organized crime", en Motherboard. Tech by VICE, publicado el 2/7/2020.

[14] Cfr. ZHUANG, Yan / PELTIER, Elian / FEUER, Alan: "The criminals thought the devices were secure, but the seller was the FBI", en The New York Times, publicado el 8/6/2021, obtenido en: https://www.nytimes.com/2021/06/08/world/australia/operation-trojan-horse-An0m.html.

[15] Cfr. PARKIN, Simon: "'Every message was copied to the police': The inside story of the most daring surveillance sting in history", en The Guardian, publicado el 11/9/2021, obtenido en:

almacenados podían ser (y serían) borrados remotamente si sus equipos eran secuestrados por las agencias de orden público o comprometidos de algún modo. Como precaución adicional, los dispositivos no eran vendidos al público en general, sino que, a los efectos de obtenerlos y suscribirse al servicio, se requería la "recomendación" de un usuario existente, lo que también contribuyó a acotar la clientela de Phantom Secure a integrantes de organizaciones criminales. Ni la empresa ni sus distribuidores requerían o registraban los nombres reales de sus clientes, que interactuaban únicamente a través de alias[16].

Aunque las autoridades estadounidenses lograron desmantelar Phantom Secure y encarcelar a sus principales directivos, fracasaron en su intento de obtener una "puerta trasera" que les permitiese interceptar y monitorear las comunicaciones de las organizaciones criminales que utilizaban el sistema. Por añadidura, las herramientas informáticas en uso por entonces no parecían aptas para sortear la protección generada por esa clase de sistemas cerrados de mensajería encriptada. Y si bien entre 2020 y 2021, las agencias de orden público de Europa, Australia y EE.UU., consiguieron finalmente acceder al monitoreo de las comunicaciones de los usuarios de las empresas que ocuparon el vacío dejado por el mercado de las organizaciones criminales (EncroChat, Sky ECC y An0m), ello requirió el recurso a un método mucho más osado que los habitualmente empleados por las autoridades estatales, el cual tuvo un éxito resonante pero generó, a la vez, muchísimos interrogantes en torno a su legitimidad.

En los apartados siguientes, se reseñarán, en primer término, las operaciones que culminaron con la infiltración gubernamental de los sistemas de EncroChat, Sky ECC y An0m (§ 2); luego, los interrogantes que estas operaciones generaron, en los tribunales europeos, en cuanto a la aplicación extra-territorial de la ley procesal y la admisión de prueba (potencialmente ilegal), proveniente del extranjero (§ 3), en orden a la afectación al derecho a la intimidad consagrado en el art. 8 del Convenio Europeo de Derechos Humanos (CEDH) (§ 4) y -finalmente- al de igualdad de armas reconocido en el art. 6 del CEDH (§ 5).

2. RESEÑA DE LAS OPERACIONES CONTRA ENCROCHAT, SKY ECC Y AN0M.

2.1. La operación de la Gendarmería francesa contra EncroChat y sus repercusiones.

El primer gran impacto a nivel mundial, en relación con la interceptación de comunicaciones efectuadas a través de sistemas cerrados de mensajería encriptada, involucró a EncroChat, una firma legalmente incorporada en Europa que ofrecía software de encriptación y soluciones de hardware (equipos). A comienzos de 2020, EncroChat logró ocupar una posición dominante en el mercado de la criminalidad organizada en Europa[17] a partir de garantizar "perfecto anonimato" a quienes

https://www.theguardian.com/australia-news/2021/sep/11/inside-story-most-daring-surveillance-sting-in-history.

[16] Cfr. Procesamiento (indictment) en caso N° 18CR1404WQH, *US v. Vincent Ramos*, Tribunal Federal del Distrito Sur de California, junio de 2017, pág. 2.

[17] Cox, Joseph: "How police secretly took over a global phone network…", cit.

adquirieren los teléfonos (denominados "Carbon units") y suscribieran el servicio de mensajería encriptada de la empresa.

La aplicación era similar, en orden a su funcionamiento, a la creada una década antes por Phantom Secure, solo que con una protección contra el monitoreo estatal mucho más robusta. Conforme explican EUROPOL y EUROJUST, se basaba en el uso de teléfonos móviles "dedicados", es decir equipos Android con una única aplicación instalada: la de EncroChat. Todas las funciones vulnerables al hackeo -el GPS, el micrófono, los puertos USB- habían sido removidas, y los teléfonos contaban con un doble sistema operativo que ocultaba la presencia de la interfaz encriptada y eliminaba cualquier asociación entre la tarjeta SIM, el equipo y su usuario. Incorporaba, asimismo, contramedidas anti forenses adicionales para el caso de que los dispositivos fuesen comprometidos, como el borrado remoto de los datos almacenados, el de los mensajes desde el lado del receptor y la posibilidad de destruir toda la información almacenada en el equipo, tanto en forma manual (mediante la introducción de un código PIN) o automática, si se producía número determinado de intentos fallidos de introducir la contraseña de acceso[18]. EncroChat también siguió el modelo de negocios implementado por Phantom Secure al disponer que sus equipos no pudiesen ser adquiridos en negocios comunes, sino únicamente a través de una red internacional de revendedores, a un precio de 1.000 euros por unidad, con una suscripción con alcance mundial con un costo semestral de 1.500 euros, que incluía soporte técnico las 24 horas, todos los días del año[19].

Al momento de concretarse la operación contra la compañía, EncroChat contaba con aproximadamente 60.000 usuarios en todo el mundo[20]. Sin embargo, no existía ninguna sociedad legalmente constituida con ese nombre, ni tampoco se conocían sus responsables ni la ubicación de su sede social[21]. Las autoridades francesas advirtieron el uso ilícito del servicio en 2017, año en que comenzó a detectarse regularmente la presencia de teléfonos móviles de EncroChat en manos de integrantes de grupos criminales organizados, a cuyo contenido no les era posible acceder con las herramientas forenses existentes[22]. En tal contexto, los investigadores le solicitaron al Directorio General de Seguridad Interior (DGSI) francés que asistiese en una operación de vigilancia sobre la citada firma[23]. Luego, a instancias de la fiscalía especializada, se

[18] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., págs. 27/28 (citas omitidas).
[19] Ver: EUROPOL "Dismantling of an encryted network sends shockwaves through organized crime groups across Europe", publicado el 2/7/2020, obtenido en: https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.
[20] Cfr. GOODWIN, Bill "Encrochat: Appeal court finds 'digital phone tapping' admissible in criminal trials", en Computer Weekly, publicado 6/2/2021, obtenido en: https://www.computerweekly.com/news/252495964/EncroChat-Appeal-court-finds-digital-phone-tapping-admissible-in-criminal-trials.
[21] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence in EncroChat cases", en Eucrim, publicado el 19/5/2022, obtenido en: https://eucrim.eu/news/Alemania-federal-court-of-justice-confirms-use-of-evidence-in-encrochat-cases/§:~:text=After%20several%20Higher%20Regional%20Courts,first%20supreme%20court%20judgment%20in.
[22] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 27.
[23] GOODWIN, Bill: "French Supreme Court rejects EncroChat verdict after lawyers question secrecy over hacking operation", en Computer Weekly, publicado el 12/10/2022, obtenido en:

solicitó la asistencia de EUROJUST, organismo que facilitó la creación de un equipo conjunto de investigación entre Francia y los Países Bajos en abril de 2020, con la participación de EUROPOL[24]. La operación resultante se bautizó como "Operación Emma" en Francia y "26 Lamont", en los Países Bajos.

A fines de 2019, las autoridades francesas habían descubierto que EncroChat operaba desde servidores de la empresa OVH en la localidad de Roubaix (registrados a nombre de una persona de nombre Eric Miguel, titular de la empresa canadiense Virtue Imports), y obtuvo autorización para copiar y analizar la información contenida en los mismos[25]. A partir de ello, constataron que dichos servidores prestaban servicios a más de 66.000 tarjetas SIM de un proveedor de telecomunicaciones neerlandés, que eran utilizados en gran cantidad de países europeos[26]. Posteriormente, en abril de 2020 la unidad especializada en cibercrimen C3N de la gendarmería francesa -presuntamente con la asistencia de investigadores neerlandeses- logró introducir un "implante de software" (es decir, un programa espía) en el sistema[27].

Las primeras señales de intrusión fueron detectadas por los usuarios de EncroChat en mayo de 2020. Cuando la compañía confirmó la presencia de malware en su sistema y fracasó en sus intentos de erradicarlo, comunicó al ataque a los clientes y cortó el servicio SIM mientras buscaba una solución. Sin embargo, ya no podía confiar en que las propias actualizaciones a las que debía recurrir para hacerlo no estuviesen infectadas a su vez. La situación empeoró cuando a poco de reestablecer su servicio, la empresa telefónica KPN removió el "cortafuegos" que impedía a los servidores de la empresa comunicarse con los equipos. Acorralada, EncroChat decidió dejar de operar[28], y le envió un mensaje a los usuarios para que descartasen sus teléfonos.

Sin embargo, a esa altura ya era demasiado tarde. Para entonces, las autoridades francesas habían interceptado alrededor de 100 millones de mensajes intercambiados entre decenas de miles de usuarios, la mayoría basados en Europa[29]. La investigación conjunta reveló la existencia de más de un centenar de delitos y aportó información que dio lugar a la apertura de cientos de investigaciones en toda Europa, y múltiples arrestos en Francia, Inglaterra, Suecia, Noruega[30] y los Países Bajos. Solo en este último país, la información obtenida a partir de la interceptación de los mensajes de EncroChat permitió el arresto de más de 100 personas, el secuestro de 8 toneladas de cocaína,

https://www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy.

[24] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 27.

[25] Ver, al respecto, el fallo dictado *in re*: *R(C) v. Director of Public Prosecutions, National Crime Agency and 4 others*, Alto Tribunal Divisional de Justicia, Tribunales Reales de Justicia, caso N° CO/3275/2020, EWHC 2967, del 26/10/2020, § 5. Tambien GOODWIN, Bill: "French Supreme Court rejects EncroChat verdict…", cit.

[26] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence in EncroChat cases", cit..

[27] Cfr. GOODWIN, Bill: "French Supreme Court raises constitutional questions over EncroChat hacking secrecy", en Computer Weekly, publicado el 3/2/2022, obtenido en: https://www.computerweekly.com/news/252512850/French-Supreme-Court-raises-constitutional-questions-over-EncroChat-hacking-secrecy.

[28] Cfr. COX, Joseph: "How police secretly took over a global pone network for organized crime", cit.

[29] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 27.

[30] Ver: NOSSITER, Adam: "When police are hackers: Hundreds charged as encrypted network is broken", en *The New York Times*, publicado el 2/7/2020, obtenido en: https://www.nytimes.com/2020/07/02/world/europe/encrypted-network-arrests-europe.html).

1.200 kilogramos de metanfetamina y casi € 20 millones en efectivo, así como el desmantelamiento de más de 19 laboratorios de drogas sintéticas[31] y la prevención de delitos gravísimos.

El propio carácter "inexpugnable" atribuido por EncroChat al sistema de comunicaciones derivó en que la información obtenida mediante su infiltración fuese especialmente valiosa, toda vez que, sintiéndose seguros, los criminales que lo utilizaban no recurrían a eufemismos o palabras en código, sino que discutían sus negocios abiertamente y en todo detalle, revelando listas de precios, nombres de clientes y referencias expresas a las cantidades de drogas que comercializaban[32].

Si bien la mayoría de los detalles sobre el modo en que se concretó la infiltración del sistema EncroChat se mantienen en estricta reserva -en especial, las características del malware utilizado para concretarla[33]- se presume que el programa fue introducido por la Gendarmería francesa en lo servidores de la empresa en Roubaix, para que luego se distribuyera a los "Carbon units" mediante las actualizaciones automáticas de la aplicación, generando una "puerta trasera" o "implante" a través de la cual las autoridades podían extraer la información contenida en los dispositivos[34]. Esta metodología es conocida como un "ataque de cadena de suministro" ("supply chain attack"), siendo su principal característica que, debido a la naturaleza del mecanismo de distribución del programa espía, *debe forzosamente alcanzar a todos los usuarios del sistema atacado*. Ello significa que, en el caso de EncroChat, el hackeo masivo concretado por las autoridades francesas alcanzó a los 60.000 clientes de la firma.

Una vez instalado en los teléfonos celulares de la red EncroChat, el spyware estatal extrajo la información en dos etapas. Así, en la "Fase 1", el programa efectuó una búsqueda retrospectiva, recolectando y remitiendo a las autoridades francesas los datos relativos a los teléfonos (números IMEI[35] y nombres de usuarios), además de todos los que aún no habían sido borrados automáticamente (es decir, los almacenados en la semana previa). La "Fase 2", en cambio, fue *prospectiva*, capturando todos los datos generados de allí en adelante (específicamente, los mensajes generados por los usuarios. Estos mensajes no fueron captados mientras se encontraban en tránsito (ya que en ese momento estaban encriptados), sino al ser creados o recibidos en los dispositivos, es decir justo antes de encriptarse o justo después de haber sido desencriptados[36]. Esta última fase se extendió hasta el 13 de junio de 2020, fecha en la que la EncroChat les indicó a sus clientes que descartaran sus teléfonos móviles[37].

[31] Ver: EUROPOL: "Dismantling of an encryted network…", cit.
[32] Cfr. Cox, Joseph: "How police secretly took over a global pone network for organized crime", cit.
[33] Al respecto, ver *infra*, § 5.
[34] Cfr. Sommer, Peter: "Evidence from hacking: A few tiresome problems", en Forensic Science International: Digital Investigation, Vol. 40, 2022, pág. 1.
[35] Es un código pregrabado en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta. La empresa operadora puede usar el IMEI para verificar el estado del aparato mediante una base de datos denominada EIR ("Equipment Identity Register").
[36] Como se explica en el fallo *R(C) v. Director of Public Prosecutions*, cit., § 12.
[37] Ver: EUROPOL: "Dismantling of an encryted network…", cit.).

2.2. La operación de las fuerzas de seguridad de Bélgica contra Sky ECC y sus repercusiones.

Cuando el sistema EncroChat dejó de operar, las organizaciones criminales se volcaron a otra plataforma encriptada similar, llamada Sky ECC, calificada por la empresa prestadora del servicio (Sky Global) como la "más segura que podía comprarse"[38]. Según explicó el Departamento de Justicia de los EE.UU. en su acusación contra dicha compañía, ésta no comercializaba teléfonos sino una aplicación para comunicaciones encriptadas que podía descargarse en distintos smartphones (iPhone, Google Pixel, Blackberry y Nokia), la cual permitía intercambiar mensajes cifrados pero *sólo con otros usuarios de la misma red*, transmitidos a través de servidores ubicados en Canadá y Francia. La empresa ofrecía también a sus usuarios la posibilidad de eliminar remotamente los datos contenidos en los teléfonos en caso de que fuesen comprometidos de algún modo. En 2021 existían alrededor de 70.000 usuarios de Sky ECC[39], que pagaban una suscripción semestral de entre 800 y 2200 euros[40].

El dato que llamó la atención de las autoridades europeas fue que, de esos 70.000 clientes, alrededor de 25% de los usuarios activos se encontraban o bien en Bélgica (6.000 clientes) y los Países Bajos (con 11.000), con un alto porcentaje de estos concentrados en los alrededores del puerto de Amberes, un destino importante en el tráfico ilegal de drogas[41]. A partir del hallazgo de más de un centenar de teléfonos conteniendo la aplicación Sky ECC, y después de 2 años de preparación, los fiscales belgas autorizaron la realización de una operación de espionaje informático contra la citada red en 2020[42]. Como resultado de la misma, y mediante un método que no se dio a conocer, las fuerzas de seguridad belgas y neerlandesas lograron infiltrar la plataforma Sky ECC y leer los mensajes encriptados "en vivo"[43] por un período de tres semanas, recolectando información y actuando sólo cuando constataran la existencia de riesgos de vida. De ese modo, pudieron elaborar un cuadro inusualmente detallado de las redes criminales que actuaban en los puertos de Amberes y Rotterdam[44]. En total, se interceptaron alrededor de 100 millones de mensajes[45].

Agentes de la policía belga llevaron a cabo registros simultáneos en más de 200 domicilios, arrestando a 48 sospechosos. Al mismo tiempo, las fuerzas de seguridad

[38] Ver: GOODWIN, Bill: "Police cracks world's largest cryptophone network as criminals swap EncroChat for Sky ECC", en Computer Weekly, publicado el 10/3/2021, obtenido en: https://www.computerweekly.com/news/252497565/Police-crack-worlds-largest-cryptophone-network-as-criminals-swap-EncroChat-for-Sky-NCC.

[39] Ver: US Department of Justice (DOJ): "Sky Global executive and associate indicted for providing encrypted communication devices to help international drug traffickers avoid law enforcement", publicado el 12/3/2021.

[40] Ver: ROYER, Sofie / DEWITTE, Pierre: "Drawing the line between privacy by design and criminal liability", Kuleuven Law, publicado el 9/3/2021, obtenido en: https://www.law.kuleuven.be/citip/blog/drawing-the-line-between-privacy-by-design-and-criminal-liability/.

[41] Ver: GOODWIN, Bill: "Police cracks world's largest cryptophone network…", cit.

[42] Ver: GOODWIN, Bill: "Police cracks world's largest cryptophone network…", cit.

[43] Ver: GOODWIN, Bill: "Police cracks world's largest cryptophone network…", cit.

[44] Cfr. BOFFEY, Daniel: "Colombia's cartels target Europe with cocaine, corruption and torture", en The Guardian, publicado el 11/4/2021, obtenido en: https://www.theguardian.com/world/2021/apr/11/colombias-cartels-target-europe-with-cocaine-corruption-and-torture.

[45] Cfr. BOFFEY, Daniel: "Colombia's cartels target Europe…", cit.

neerlandesas registraron otros 75 domicilios y arrestaron a 30 personas[46]. Los detenidos en estos operativos incluyeron a agentes de las fuerzas de seguridad en activo, funcionarios de la fiscalía, del gobierno y de la autoridad tributaria, así como delincuentes responsables de numerosos hechos de violencia[47]. Se trató de la operación policial más grande de la historia de Bélgica, y -potencialmente- la más significativa contra las organizaciones de narcotráfico del oeste de Europa, dado que se secuestraron un total de 27 toneladas de cocaína en el puerto de Amberes, en buques de contenedores y casas seguras, con un costo estimado de 1400 millones de euros[48]. En este contexto, cobró especial trascendencia el descubrimiento, en las afueras de Amberes, de una estructura de 7 contenedores de los que 6 habían sido convertidos en celdas, y la última en una *cámara de torturas* con una silla de dentista especialmente adaptada y todo tipo de implementos[49].

El ataque contra Sky ECC se hizo público el 9 de marzo de 2021[50]. En un comunicado, Eurojust celebró los resultados de la colaboración entre las agencias de orden público de Belgica, Países Bajos y Francia, destacando que había permitido obtener información crucial sobre más de un centenar de operaciones criminales a gran escala y previniendo situaciones en las que se encontraba en riesgo la vida de personas[51]. Pocos días después -el 12 de marzo de 2021- un gran jurado en los EE.UU. dictó el procesamiento del CEO de Sky Global, Jean Francois Eap, y de uno de los principales distribuidores de Sky ECC, Thomas Herdman, acusándolos de participar en una asociación criminal dedicada a facilitar el tráfico internacional de narcóticos[52]. Asimismo, las autoridades estadounidenses tomaron el control de más de 100 dominios de internet propiedad de la compañía, haciendo cesar su actividad comercial[53].

[46] Ver: GOODWIN, Bill: "Police cracks world's largest cryptophone network…", cit.

[47] Cfr. BOFFEY, Daniel: "Colombia's cartels target Europe…", cit. En Francia, si bien en un comienzo no hubo detenciones, la policía Francesa identificó a unos 2.000 usuarios de Sky ECC, motivando la apertura de investigaciones judiciales por narcotráfico y delitos violentos (ver: The Guardian: "Police raids across Europe after encrypted phone network shut down", publicado el 10/3/2021, obtenido en: https://www.theguardian.com/technology/2021/mar/10/police-raids-across-europe-after-encrypted-phone-network-shut-down).

[48] Cfr. BOFFEY, Daniel: "Colombia's cartels target Europe…", cit.

[49] Ver: The Guardian: "Dutch arrests after discovery of 'torture chamber' in sea containers", publicado el 7/7/2020, obtenido en: https://www.theguardian.com/world/2020/jul/07/dutch-police-arrest-six-men-after-discovery-of-torture-chamber (énfasis añadido); y BOFFEY, Daniel: "Colombia's cartels target Europe…", cit.

[50] En un primer momento, Sky ECC publicó una declaración negando que el sistema hubiese sido infiltrado, atribuyendo la captura de los datos a una falsa aplicación de phishing denominada "Sky Ecc", instalada en teléfonos inseguros y comercializada a través de canales no autorizados (Ver: GOODWIN, Bill: "Police cracks world's largest cryptophone network…", cit.).

[51] Ver: EUROJUST: "New major interventions to block encrypted communications of criminal networks", publicado el 10/3/2021.

[52] Ver: US Department of Justice (DOJ): "Sky Global executive and associate indicted…", cit.

[53] Cfr. MARKS, Joseph: "Encrypted messaging apps present a dilemma for law enforcement", en The Washington Post, publicado el 18/11/2021, obtenido en: https://www.washingtonpost.com/politics/2021/11/18/encrypted-messaging-apps-present-dilemma-law-enforcement/.

2.3. La operación del FBI y la Policía Federal Australiana con el sistema An0m y sus repercusiones.

La caída de EncroChat y Sky ECC derivó en que cobrara preponderancia un *tercer sistema de comunicaciones* encriptadas, denominado An0m. Al igual que EncroChat, el sistema An0m estaba centrado en el uso de teléfonos celulares especialmente modificados, con todas las funciones susceptibles de ser explotadas para el espionaje suprimidas y equipados con una aplicación -a la que se accedía ingresando una clave numérica en la calculadora- que permitía la comunicación encriptada con otros usuarios de la misma red, en un circuito cerrado. Además de la posibilidad de eliminar remotamente la información contenida en los teléfonos en caso de que fuesen comprometidos (que las agencias de orden público habían comenzado a prevenir almacenando los equipos secuestrados en "bolsas Faraday"[54]), se podía también programar los equipos para que los datos se borraran automáticamente si el teléfono estaba fuera de línea por un lapso determinado de tiempo. También podía programarse la supresión de los mensajes después de ser leídos, y la creación de notas de voz con ésta última alterada para impedir la identificación del remitente[55]. La aplicación no podía adquirirse en tiendas online ni descargarse. Para acceder a la misma era menester comprar un teléfono An0m con la misma preinstalada, a un costo de 1.700 dólares por cada equipo, con una suscripción anual de 1.250 dólares[56].

Sin embargo, a diferencia de EncroChat y Sky ECC, An0m no era en absoluto una red segura de comunicaciones, sino el resultado de una operación conjunta sin precedentes, pergeñada por el FBI y la Policía Federal Australiana (PFA), responsables del desarrollo, fabricación y comercialización de los equipos. Como resultado de ello, cada uno de los más de 19 millones de mensajes enviados mediante la aplicación An0m desde su lanzamiento en 2018 había sido recolectado, y muchos de ellos leídos[57].

El origen de esta operación (bautizada como "Trojan Shield" por el FBI, y "Ironside" por la PFA), en cuyo marco se distribuyeron 12.000 celulares a integrantes de aproximadamente 300 organizaciones criminales en todo el mundo[58], se remonta a la investigación iniciada en EE.UU. contra Phantom Secure[59], en 2017. En dicha oportunidad, tras el arresto de los directivos de la firma, el FBI consiguió reclutar como "fuente humana confidencial" a uno de los distribuidores de los teléfonos de la mencionada firma, que estaba desarrollando la próxima generación de equipos (denominada An0m) y se la ofreció a la agencia junto con su red de distribuidores[60].

Como primer paso, se introdujo en el sistema de encriptación de An0m una "llave maestra" que les permitía a las agencias de orden público intervinientes descifrar todos los mensajes a medida que se transmitían. También por diseño, los mensajes enviados

[54] Contenedores de aluminio, que previenen la recepción de señales.
[55] Ver: PARKIN, Simon: "'Every message was copied to the police'…", cit.
[56] Ver: PARKIN, Simon: "'Every message was copied to the police'…", cit.
[57] Ver: PARKIN, Simon: "'Every message was copied to the police'…", cit.
[58] Cfr. BAKER, Stewart / KLEHM, Bryce: "Legal Tetris and the FBI's An0m program", en Lawfare, publicado el 22/7/2021, obtenido en: https://www.lawfareblog.com/legal-tetris-and-fbis-An0m-program.
[59] Ver *supra*, § 1.
[60] Ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., pág. 6 (notas omitidas). Según la propia declaración del DOJ, al desarrollador de An0m se le abonaron U$S 120.000 en concepto de honorarios y U$S 59.508 en concepto de gastos.

desde los equipos geolocalizados fuera de los EE.UU. estaban sujetos a un "reenvío con copia oculta" encriptado, recibido por un servidor automatizado ("iBot") localizado fuera de ese país, donde eran descifrados con la llave maestra[61]. Asimismo, se le asignaba a cada usuario un código de identificación alfanumérico (similar a un "PIN"). El FBI mantenía una lista actualizada de los códigos y de los correspondientes "nombres de usuario" de todos los clientes de An0m[62].

Para la distribución de los equipos, se adoptó el sistema "por invitación" implementado previamente por Phantom Secure, conforme el cual cada nuevo cliente debía ser recomendado por uno existente, lo que le otorgaba una apariencia de mayor seguridad al sistema. En este escenario, An0m se promocionó a través de una red de "influencers" integrada por figuras notorias del ambiente criminal[63]. Comenzando en el mes de octubre de 2018, se llevó a cabo la "prueba Beta" de An0m, en el marco de la cual la "fuente confidencial" del FBI entregó los primeros cincuenta teléfonos a tres ex distribuidores de Phantom Secure con abundantes conexiones con organizaciones criminales, sobre todo en Autralia. La PFA obtuvo autorización judicial para monitorear las comunicaciones concretadas a través del sistema, compartiendo con el FBI las más relevantes[64].

La red An0m creció orgánicamente y experimentó un crecimiento exponencial en 2019, tras la primera prueba en Australia, reclutándose distribuidores en España, Turquía, los Países Bajos, Finlandia, México y Tailanda, hasta llegar a 12.000 equipos en más de 90 naciones[65]. Especialmente relevante para esta expansión fueron las caídas de EncroChat (en julio de 2020) y de Sky ECC (en marzo de 2021)[66], que acarrearon que el número de usuarios activos de An0m *se triplicara*, de 3.000 a comienzos de 2021 a 9.000 en mayo del mismo año, tras la salida de servicio de Sky ECC[67].

En los 18 meses que duró la operación, el FBI y la PFA capturaron, tradujeron y analizaron cerca de 27 millones de mensajes[68]. De ese modo, lograron identificar a más de 300 organizaciones criminales que utilizaban An0m, incluyendo a la mafia italiana, bandas criminales de motociclistas en varios países, y numerosos grupos de narcotraficantes[69]. Tal como ocurrió con los dos sistemas reseñados precedentemente, la confianza de los usuarios en la seguridad de la red de comunicaciones era tal que no hablaban en código, sino que hacían referencia directa a los buques en los que se trasladaban las drogas y los puntos de descarga[70]. Dicha circunstancia permitió acumular una increíble cantidad de información, que derivó en unos 800 arrestos, el secuestro de

[61] Ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., pág. 7.
[62] Ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., pág. 7.
[63] Cfr. BAKER, Stewart / KLEHM, Bryce: "Legal Tetris and the FBI's An0m program", cit.
[64] Ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., págs. 7/8 (notas omitidas).
[65] Ver: PARKIN, Simon: "'Every message was copied to the police'…", cit.
[66] Cfr. WOLFF, Josephine: "One of the most unusual cybersecurity stories of the year is getting more complicated", en Slate, publicada el 3/12/2021, obtenida en: https://slate.com/technology/2021/12/fbi-fake-encrypted-messaging-platform-An0m-sky-global.html.
[67] Ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., pág. 11 (énfasis añadido).
[68] Cfr. ZHUANG, Yan / PELTIER, Elian / FEUER, Alan: "The criminals thought the devices were secure,...", cit.
[69] Ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., pág. 10.
[70] Cfr. ZHUANG, Yan / PELTIER, Elian / FEUER, Alan: "The criminals thought the devices were secure,...", cit.

más de 8 toneladas de cocaína, 22 de marihuana, 2 de metanfetaminas y anfetaminas, 6 de precursores químicos, 250 armas de fuego y más de 48 millones de dólares en distintas divisas, además del desmantelamiento de unos 50 laboratorios de drogas[71]. Por añadidura, previnieron 150 amenazas a la vida[72]. Solo en Suecia, la información obtenida contribuyó a impedir 10 asesinatos[73].

2.4. Controversias en torno a las operaciones contra EncroChat y Sky ECC y mediante An0m en los tribunales europeos. Introducción.

De la reseña efectuada en los apartados precedentes con respecto a los medios empleados para monitorear las comunicaciones efectuadas a través de las redes EncroChat, Sky ECC y An0m se desprenden una serie de características que inciden directamente sobre el análisis judicial que ya ha comenzado a llevarse a cabo en relación con aquellas operaciones en los tribunales europeos. En este orden de ideas, cabe destacar a las siguientes: a) el grado de sofisticación de las metodologías empleadas, que implicó un salto cualitativo exponencial en el ámbito de las operaciones contra el crimen organizado trasnacional, con pocos o nulos antecedentes en la historia[74]; b) el alcance masivo de la vigilancia desplegada por las agencias de orden público intervinientes, que se extendió a decenas de miles de usuarios en los primeros dos casos y algo menos de 10.000 en el último; c) el carácter trasnacional de la vigilancia, dado que -por la propia naturaleza de los métodos empleados- forzosamente alcanzó a usuarios no localizados dentro de la jurisdicción de las autoridades judiciales que autorizaron las medidas de vigilancia en Francia, Bélgica y Australia; d) el secreto existente respecto de distintas cuestiones atinentes a las operaciones policiales, como las características de los programas espías utilizados -en orden a EncroChat y Sky ECC- o la identidad del país en el que se almacenaron los datos recolectados mediante el sistema An0m; y e) los resultados obtenidos a partir de dichas operaciones, que -ya sea individualmente o en conjunto- las convierten en las más exitosas de la historia tanto en lo tocante a la cantidad de conductas ilícitas identificadas como al impacto sobre el crimen organizado trasnacional.

Las características apuntadas han ocasionado, como era de prever, en una profusa actividad recursiva de las defensas ante los tribunales europeos. Los primeros

[71] Cfr. BAKER, Stewart / KLEHM, Bryce: "Legal Tetris and the FBI's An0m program", cit.
[72] Cfr. ZHUANG, Yan / PELTIER, Elian / FEUER, Alan: "The criminals thought the devices were secure,...", cit.
[73] Ver: BBC News: "An0m: Hundreds arrested in massive global crime sting using messaging app", publicado el 8/6/2021, obtenido en: https://www.bbc.com/news/world-57394831.
[74] Un antecedente de hackeo masivo como los concretados respecto de EncroChat y Sky ECC se dio en los EE.UU. en el caso "Playpen", en el que el FBI asumió el control de una página web en la "Red oscura" dedicada al intercambio de imágenes de explotación sexual infantil e introdujo en la misma un programa espía que se introducía en las computadoras de los visitantes de la página cuando descargaban o subían contenidos ilegales (ver, al respecto: HENNESSEY, Susan, "The elephant in the room…", cit., págs. 12/14. La operación que tuvo como centro a An0m, en cambio, tiene como antecedente a la creación de la empresa de comunicaciones encriptadas Crypto AG, fundada en Suiza a fines de la Segunda Guerra Mundial, que operó durante más de 50 años, hasta que se descubrió que había sido operada todo ese tiempo por la CIA y el servicio secreto Alemán (ver, al respecto: MILLER, Greg: "The intelligence coup of the century", en The Washington Post, publicado el 11/2/2020, obtenido en: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

dos pronunciamientos en cobrar estado público (ambos en referencia a EncroChat) fueron dictados a fines de 2020 y principios de 2021 en Inglaterra[75]. En ellos, comenzaron a delinearse con claridad los principales focos de conflicto entre el uso de métodos novedosos de vigilancia informática y las doctrinas legales y constitucionales actualmente vigentes. A fines de 2021, se reportó la existencia de al menos una veintena de planteos ante los tribunales británicos. Mientras que, en Alemania, se encontraban en trámite más de 550 expedientes derivados de EncroChat, y se habían planteado objeciones ante los tribunales constitucionales de Francia, Bélgica y los Países Bajos[76].

En tal contexto, los principales cuestionamientos se centraron en los tres aspectos más problemáticos que presentan las operaciones reseñadas, que -como se adelantó[77]- serán analizados en los próximos tres apartados del presente trabajo: la legitimidad de la obtención extraterritorial de evidencia y su uso por terceros países, la proporcionalidad de la intrusión estatal sobre el derecho a la intimidad y privacidad de las personas afectadas y la posible afectación del derecho a la "igualdad de armas" derivada del secreto sobre los medios tecnológicos utilizados. Planteos que en algunos casos ya se han abierto paso hasta las esferas superiores de los sistemas judiciales nacionales y han dado lugar a la intervención del Tribunal Europeo de Derechos Humanos (TEDH), que en la actualidad tiene pendientes de resolución dos casos relacionados con EncroChat: las aplicaciones *A.L. v. Francia* (N° 44715/2020) y *E.J. v. Francia* (N° 47930/2021), en las que se cuestiona la posible vulneración de los arts. 6° (derecho a un proceso penal equitativo), 8° (derecho al respeto a la vida privada y la correspondencia) y 13° (derecho al recurso) del Convenio Europeo de los Derechos Humanos (CEDH)[78].

La jurisprudencia que emana de estos tribunales sobre los casos EncroChat, Sky ECC y An0m no sólo es extremadamente importante por los precedentes que puedan llegar a establecerse en orden al uso, por parte de las agencias de orden público, de métodos informáticos avanzados para la vigilancia de los ciudadanos[79], sino también por

[75] Se trata de los fallos *R(C) v. Director of Public Prosecutions* (citado *supra*, nota § 25) y *A, B, D & C v. Regina* (División Penal del Tribunal de Apelación de la Corona en Liverpool, Tribunales Reales de Justicia, casos Nros. 202100094 B1, 202100110 B1, 20200112 B1 y 20200113 B1, EWCA Crim 128, del 5/2/2021). Ambos fallos están vinculados al mismo caso, en el que un ciudadano de Liverpool (Inglaterra) fue arrestado por tráfico de cocaína y heroína y conspiración para cometer un homicidio, a partir de la evidencia obtenida por las autoridades británicas como resultado de la interceptación de las comunicaciones que había sostenido el imputado mediante el sistema EncroChat.

[76] Ver: Fuentitech.com: "Berlin court overturned ban on EncroChat evidence in criminal trials", publicado el 3/9/2021, obtenido en: https://fuentitech.com/berlin-court-overturned-ban-on-encrochat-evidence-in-criminal-trials/217620/.

[77] Ver *supra*, § 1.

[78] Cfr. ZARAGOZA TEJADA, Javier Ignacio: "Operaciones encubiertas digitales y convencionales. Un análisis desde la perspectiva de los derechos fundamentales y del derecho comparado", en AAVV, *La investigación penal en el entorno digital. Estudios sobre el impacto de las nuevas tecnologías digitales en el proceso penal*, Hammurabi, Buenos Aires, 2023, pág. 213.

[79] Con respecto a esto, cabe señalar que es difícil imaginar que luego de la infiltración sucesiva de dos de las principales redes de mensajería encriptada, y el descubrimiento de que otro había sido desarrollado desde un principio por el FBI, las organizaciones criminales vuelvan a confiar en esta clase de sistemas. Lo más probable parece ser, en consecuencia, que haga su aparición alguna metodología novedosa para impedir la vigilancia estatal, lo que a su vez requerirá de una nueva estrategia de las agencias de orden público para contrarrestarla. En cualquier caso, lo que es casi seguro es que deberá utilizarse algún recurso distinto al que se empleó en las operaciones de EncroChat, Sky ECC y An0m.

la propia naturaleza de la evidencia obtenida y su relevancia en las causas judiciales iniciadas a partir de la misma. En efecto, se aprecia que, en estos casos, la cuestión de la legitimidad de la interceptación de los mensajes o la eventual prohibición de su uso como prueba de cargo es determinante para el éxito o fracaso de las investigaciones contra los sospechosos identificados por intermedio de aquella. Ello así, desde que -en especial en lo tocante a EncroChat y Sky ECC, pero en parte también en An0m- la información obtenida por medio de estas operaciones constituye el elemento central de la imputación contra los integrantes de las organizaciones criminales. En este escenario, parece claro que, si la evidencia obtenida en estas operaciones es considerada admisible y válida, su contenido poco menos que garantiza la condena en un altísimo porcentaje de los casos, toda vez que -como ya se señaló- la libertad con la que los usuarios de estos sistemas discutían sus negocios ilícitos en los mensajes captados deja escaso margen para dudar de su culpabilidad. Mientras que, en sentido opuesto, la eventual exclusión de esta evidencia privaría de contenido a todos aquellos casos (que son la mayoría), en los que existía poco o ningún conocimiento sobre la actividad ilícita de los imputados con anterioridad a la interceptación de los mensajes, y la evidencia no era suficiente en aquellos supuestos en los que si se sospechaba la conducta ilegal.

3. CONFLICTO CON EL PRINCIPIO DE TERRITORIALIDAD. APLICACIÓN TRASNACIONAL.

3.1. La aplicación extra territorial de la ley procesal penal en los casos EncroChat, Sky ECC y An0m.

En un documento reciente[80], EUROPOL y EUROJUST destacaron que, a los fines de una cooperación legal exitosa entre las naciones en orden al intercambio de evidencia, resulta “crucial” que la prueba electrónica recolectada por un país pueda ser obtenida legalmente por otro. Señalan, en tal sentido, que si las autoridades de una determinada nación desean utilizar evidencia digital localizada en otra para su propia investigación, deben conseguirla a través de los canales legales, como ser una “Orden Europea de Investigación Europea” (OEI) o un pedido de asistencia legal recíproca.

La postura de estas organizaciones refleja la concepción tradicional sobre el denominado “principio de territorialidad” en materia de aplicación de la ley procesal, el cual encuentra su raíz en el concepto de soberanía, que en el ámbito del derecho internacional supone la independencia de las naciones respecto de cualquier otro actor y conlleva el derecho de ejercer, dentro de un espacio físico determinado, todas las funciones del Estado. En este escenario, el “principio de territorialidad” actúa como límite para impedir la intervención de cualquier poder jurisdiccional de un Estado en otro, el cual –pese a haber admitido ciertas restricciones o excepciones derivados de las necesidades modernas, en especial por los desafíos que representa la criminalidad organizada trasnacional— se mantiene prácticamente incólume *en lo que tiene que ver con los poderes procesales*. Así pues, la regla general sigue siendo que un órgano de persecución penal no puede ejercer actos coercitivos fuera del territorio del Estado que le otorgó su poder jurisdiccional. Por ende, conforme a las normas de derecho

[80] Ver: EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 15.

internacional vigentes, los poderes de las autoridades de persecución penal para realizar medidas de prueba y —en especial— para ejercer cualquier tipo de coerción en la obtención de una prueba están vinculados y limitados al territorio en el que se les ha otorgado poder jurisdiccional[81].

La aplicación de estos principios generales, que no resulta problemática en el mundo físico, se torna mucho más compleja en lo que se refiere a la evidencia electrónica, sobre todo cuando su obtención involucra la actuación en el ciberespacio, ámbito en el que la libertad en el intercambio de información digital les resta trascendencia a las fronteras geográficas. Hasta hace muy poco, sin embargo, dicha circunstancia no había contribuido a resquebrajar el (casi) monolítico consenso político internacional en torno a la aplicación estricta del principio de territorialidad, según el cual una vez establecida la ubicación de los datos se le reconoce jurisdicción sobre los mismos al Estado en cuyo territorio se encuentren[82].

La apuntada complejidad queda aún más de manifiesto en casos como los que son objeto del presente trabajo. Ello así, desde que el uso de herramientas de anonimato (como las que facilitan la navegación anónima en Internet y ocultan la verdadera identidad de su usuario) dificulta en gran medida dar aviso u obtener autorización de las naciones que puedan verse afectadas por una operación de hackeo (legal) *hasta después de haberse concretado* el mismo y revelado la ubicación del (los) objetivo(s)[83]. Esto es, precisamente, lo que ha ocurrido con respecto a las operaciones contra EncroChat y Sky ECC y la que involucró a la plataforma An0m, toda vez que las agencias de orden público intervinientes, aun sabiendo que las medidas de vigilancia iban necesariamente a traspasar las fronteras del país en que fueron autorizadas, *no tenían modo de saber a ciencia cierta en donde se encontraba cada uno de los usuarios afectados* por la interceptación de las comunicaciones.

Así, por ejemplo, en el caso del hackeo de EncroChat, si bien es sabido que la intrusión informática propiamente dicha (en los servidores de la empresa) tuvo lugar en territorio francés, amparada por la autorización de un magistrado de ese país, lo cierto es que la modalidad empleada para concretar la vigilancia sobre los usuarios (esto es: descargando el spyware estatal en los teléfonos de todos los usuarios mediante actualizaciones del sistema) implicó forzosamente que terminasen hackeando los dispositivos de personas *localizadas fuera de las fronteras de Francia* (y, por consiguiente, también fuera de la jurisdicción del juez que dispuso la medida).

De hecho, conforme surge de documentos legales publicados en ese país, sólo 380 de los 32.477 teléfonos intervenidos por las fuerzas de seguridad francesas estaban en territorio francés, siendo que casi el 98% de los aparatos se encontraban allende sus fronteras[84]. Por consiguiente -y como se planteó en un caso en el Reino Unido- la

[81] Cfr. SALT, Marcos, "Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina", en Revista de Derecho Penal y Procesal Penal, Buenos Aires, Abeledo-Perrot, vol. 2013-6, págs. 201/203 (citas omitidas).

[82] Cfr. BLANCO, Hernán, *Tecnología informática e investigación criminal*, La Ley, Buenos Aires, 2020, págs. 363/363.

[83] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 29 (citas omitidas, énfasis añadido).

[84] Cfr. COLLERAN, Kevin: "French legal challenge over EncroChat cryptophone hack could hit UK prosecutions", en Techlive, publicado el 8/5/2021. Tanto es así que en otros países casi se duplicó la

autorización librada por el juez en Francia derivó en la implantación de malware en teléfonos móviles localizados -por ejemplo- en Inglaterra, que interceptaron comunicaciones efectuadas (exclusivamente) entre personas localizadas en ese país[85].

En este escenario, parece claro que las autoridades de las naciones en las que se concibieron y concretaron las operaciones en estudio *optaron deliberadamente por no ceñirse al principio de territorialidad*. Esta decisión es especialmente clara en el caso EncroChat, en el que las agencias de orden público de Francia y los Países Bajos le comunicaron a las de varios otros países de Europa que iban a interceptar mensajes de sus ciudadanos *con independencia de si recibían, o no, autorización para ello* por parte del resto de las naciones del Continente[86]. Ello surge en forma expresa de un fallo dictado en Inglaterra, en el que se detalló que el equipo conjunto de investigación franco neerlandés a cargo de la denominada "Operación Emma" le comunicó a las autoridades inglesas que la interceptación iba a comenzar en marzo de 2020, que iba a tener alcance mundial e involucrar a ciudadanos ingleses y que se iba a avanzar con o sin autorización del Reino Unido. Se le indicó, sin embargo, a dichas autoridades, que si así lo deseaban podían obtener la evidencia resultante mediante una OEI[87].

La conformación del mencionado equipo de investigación había tenido lugar en 2018, a instancias de Francia, con la cooperación de EUROJUST, que fomentó a su vez la intervención de EUROPOL, agencia que prestó apoyo financiero, técnico y logístico para la actividad del equipo, además de coordinar el intercambio posterior de información con las naciones involucradas[88]. En dicho marco, EUROJUST organizó cinco reuniones de coordinación con autoridades de Francia y los Países Bajos para planificar la operación, en dos de las cuáles participaron también, en carácter de invitados, enviados de Suecia, el Reino Unido, Noruega y España[89]. La evidencia resultante del hackeo de EncroChat fue compartida inicialmente con las autoridades de los Países Bajos a través del propio equipo de investigación, y luego con los restantes países interesados, ya sea por medio de OEIs (como es el caso del Reino Unido[90] y Alemania[91], por ejemplo) o rogatorias[92]. Un

cantidad de teléfonos intervenidos en el país donde se libró la orden judicial original. Así, por ejemplo, en Suecia se hackearon más de 700 celulares (Cfr. Tech News Terminal: "Swedish Court Docket finds ambiguities in hacked EncroChat cryptophone proof", publicado el 11/5/2021, obtenido en: https://technewsterminal.com/swedish-court-docket-finds-ambiguities-in-hacked-encrochat-cryptophone-proof/.

[85] Ver fallo A*, B, D & C v. Regina*, cit. § 34.

[86] Cfr. CORFIELD, Gareth: "Encrochat hack evidence wasn't obtained illegaly, High Court of England and Wales rules – Trial judges will decide whether to admit it", en The Register, publicado el 13/11/2020, obtenido en: https://www.theregister.com/2020/11/13/encrochat_hack_judicial_review_judgment/ (énfasis añadido).

[87] Ver fallo *R(C) v. Director of Public Prosecutions*, cit., § 11.

[88] Ver: EUROPOL: "Dismantling of an encryted network…", cit..

[89] Cfr. GOODWIN, Bill: "How diplomatic immunity silenced the prosecutor who coordinated Sweden's EncroChat probe", en Computer Weekly, publicado el 10/2/2022, obtenido en: https://www.computerweekly.com/news/252513203/How-diplomatic-immunity-silenced-the-prosecutor-who-coordinated-Swedens-EncroChat-probe.

[90] Ver, al respecto, lo señalado en los fallos *R(C) v. Director of Public Prosecutions*, cit., § 2 y *A, B, D & C v. Regina*, cit. § 13.

[91] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence in EncroChat cases", cit.

[92] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 27.

proceso similar se habría utilizado -aunque la información al respecto es muy escasa- para obtener (y luego compartir) la evidencia digital en el caso Sky ECC.

En la operación referida al sistema An0m, en cambio, se recurrió a un proceso considerablemente más complejo. Como ya se ha señalado, la autorización inicial para implementar la vigilancia a través del mencionado sistema de mensajería encriptada se libró en Australia, lugar en que también se distribuyeron los primeros teléfonos. Sin embargo, dado que la normativa australiana no permitía compartir la evidencia resultante, el equipo de investigación debió recurrir a un tercer país (cuya identidad aún se desconoce, aunque estaría en Europa[93]), el cual aceptó albergar (con la correspondiente autorización judicial) un servidor en donde se almacenaron las copias de todos los mensajes intercambiados por los usuarios fuera de los EE.UU. mediante la plataforma An0m (inicialmente encriptados), y compartir la evidencia con el FBI -a través de pedidos de asistencia legal mutua- a cambio de las llaves criptográficas necesarias para poder desencriptar los mensajes, que habían sido retenidas por esta última agencia[94]. De este modo, sólo una vez que los intercambios se iniciaron, en octubre de 2019, este tercer país pudo leer también los mensajes interceptados almacenados en el servidor radicado en su territorio[95].

Si bien, por diseño, el FBI no podía, en principio, acceder a la información perteneciente a los teléfonos de los usuarios de An0m localizados en los EE.UU.[96], se acordó con la PFA que esta última agencia tuviese a su cargo el monitoreo de dichas personas, pudiendo dar a conocer la información a su par estadounidense cuando de la misma surgiese la posible existencia de una "amenaza a la vida"[97].

El resto de los países afectados (esto es, aquellos cuyos ciudadanos tenían consigo teléfonos de An0m cuyos mensajes fueron interceptados) fue informado con posterioridad, a medida que el análisis de la información obtenida como resultado de la operación por parte del FBI o la PFA demostraba ser relevante para sus autoridades. Así, por ejemplo, la policía federal alemana (BKA, por sus siglas en dicho idioma) fue notificada de la existencia de esta evidencia recién en enero de 2021. Luego, a partir de la presentación de un pedido de asistencia jurídica mutua al Departamento de Justicia de los EE.UU. en marzo de 2021, la citada agencia obtuvo acceso a una "plataforma de análisis" conteniendo los datos recolectados a través de la vigilancia del sistema An0m

[93] Ver: Cox, Joseph: "A European country helped the FBI intercept An0m messages, but it wants to remain hidden", en Motherboard: Tech by Vice, publicado el 3/6/2022, obtenido en: https://www.vice.com/en/article/qjbggq/An0m-third-country-europe-european-union-fbi.

[94] Ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., págs. 8/9.

[95] A fin de evitar que mediante una orden judicial en el extranjero se vigilara a ciudadanos estadounidenses, el FBI introdujo en el sistema una "geo cerca" (geo fence), de modo tal que los mensajes originados en los EE.UU. no se copiaran en el servidor localizado en el tercer país. En caso de que uno de los teléfonos pertenecientes al sistema An0m se trasladase a ese país, el FBI acordó con la PFA que esta última le haría saber si se detectaba alguna "amenaza inminente a la vida" en territorio norteamericano (ver: DOJ, Declaración jurada en apoyo de pedido de orden para interceptación…, cit., págs. 8/9).

[96] Según la información originalmente divulgada por el FBI, había solo 15 usuarios de An0m en ese país. Sin embargo, con posterioridad esa cifra fue puesta en duda cuando se hicieron públicos documentos consignando el envío a los EE.UU. de unos 100 teléfonos, aunque se desconoce si permanecieron allí o fueron reexportados (ver: Cox, Joseph: "FBI honeypot company An0m shipped over 100 phones to the United States", en Motherboard: Tech by Vice, publicado el 12/1/2022, obtenido en: https://www.vice.com/en/article/epxp8w/fbi-An0m-shipped-100-phones-united-states.

[97] Cfr. Cox, Joseph: "FBI honeypot company An0m shipped over 100 phones…", cit.

(otros datos fueron transmitidos mediante discos rígidos encriptados). Sin embargo, no se les comunicó a las autoridades alemanas la identidad del "tercer país" que autorizó la instalación del servidor con los datos[98].

3.2. Legitimidad de la evidencia obtenida a través del uso transfronterizo de herramientas informáticas. Normativa aplicable, posiciones doctrinarias y estándares en la jurisprudencia del Tribunal Europeo de Derechos Humanos.

En un comentario que resulta de aplicación a los casos objeto de este trabajo, EUROPOL y EUROJUST señalan que las técnicas empleadas por las agencias de orden público para contrarrestar la encriptación de evidencia relevante (como, por ejemplo, el uso de govware) deben estar amparadas en disposiciones específicas o generales de la normativa procesal nacional. Aspecto que resulta problemático cuando -como ocurre con los casos reseñados- se trata de operaciones trasnacionales en los que los sospechosos, las eventuales víctimas, los delitos cometidos y la infraestructura informática se encuentran en distintos países, por lo que resultan aplicables regímenes legales diferentes[99].

Sobre el punto, vale tener presente que el ataque informático concretado en orden a EncroChat se llevó a cabo en Francia al amparo de una serie de órdenes judiciales libradas conforme la normativa procesal de ese país, en el que la Ley 2016-731, del 3 de junio de 2016, incorporó en forma expresa en los arts. 706-102-1 al 706-102-7 el Código de Procedimiento Criminal (CPC) la facultad para utilizar software espía estatal (*govware*) como herramienta de investigación[100], previendo tanto su introducción física en el sistema o servidor objetivo como el acceso remoto[101]. De igual manera, la normativa procesal de los países bajos -que también intervino en la investigación primigenia sobre EncroChat- cuenta con disposiciones específicas regulando el uso estatal de spyware (arts. 126nba y 127ffa) a partir de la reforma introducida en el código procesal local por la Ley III de Crimen Informático (*Wet computercriminaliteit III*), que entró en vigor en marzo de 2019[102].

En cuanto a la operación referida a Sky ECC, aunque se conoce aún muy poco respecto a quién y en base a qué se autorizó el hackeo a los servidores (y cómo y en donde se concretó), cabe recordar que el país en que la orden judicial se habría librado

---

[98] Cfr. MONROY, Matthias: "German An0m investigations: The mysterious EU third state", en Security Architectures in the EU, publicado el 4/4/2022, obtenido en: https://digit.site36.net/2022/04/04/german-An0m-investigations-the-mysterious-eu-third-state/.

[99] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12.

[100] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 42 y Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 10. En línea con lo establecido en las normas mencionadas, los arts. 230-1 al 230-5 del CPC facultan a los jueces a autorizar, en caso de que se detecten la presencia de herramientas anti forenses que impidan acceder a la información buscada (como por ejemplo la encriptación), el empleo de recursos (técnicos) sometidos a secreto de defensa.

[101] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 73 (citas omitidas).

[102] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12. Sobre la normativa neerlandesa, ver también: ŠKORVÁNEK, Ivan / KOOPS, Bert-Jaap / CLAYTON NEWELL, Bryce / ROBERTS, Andrew: "My computer is my castle' New privacy frameworks to regulate police hacking", en Brigham Young University Law Review, Vol. 2019, N° 4, 2019, págs. 1018/1020.

-Bélgica- cuenta con una norma específica dentro de su código de procedimientos (art. 88 ter § 3) que en forma expresa habilita el acceso remoto a datos, incluso si están ubicados fuera de su territorio[103]. Por último, en lo tocante a la interceptación de las comunicaciones efectuadas a través de la plataforma An0m, la operación se inició bajo la legislación australiana, conforme lo establecido en la ley "TOLA" (Telecommunications and Other Legislation Amendment), vigente desde 2018, que faculta a las agencias de orden público a utilizar medios técnicos para interceptar mensajes en el marco de investigaciones criminales[104]. El secreto (que aun persiste) en torno a la identidad del "tercer país" (presumiblemente europeo) al que recurrió el FBI para obtener cobertura legal para el monitoreo de las comunicaciones de An0m impide, hasta el momento, conocer cuáles fueron las normas procesales que se aplicaron a tal efecto.

No puede pasarse por alto, no obstante, que la evidencia resultante de las tres operaciones mencionadas no sólo se utilizó en las naciones en las que se obtuvo la autorización judicial para la implementación de las medidas de vigilancia, sino que fue compartida con otros países en los que residían personas cuyos teléfonos también fueron monitoreados, dando lugar a numerosos procesos criminales basados en dicha evidencia. En orden a ello, EUROPOL y EUROJUST señalan que, habida cuenta que la admisibilidad de la prueba informática obtenida en los tribunales de terceros países ha de ser decidida conforme la normativa procesal de esas naciones, es preciso que el intercambio de evidencia se lleve a cabo respetando las distintas legislaciones nacionales[105].

En tal contexto, vale tener presente que la información producto de las operaciones EncroChat, Sky ECC y An0m fue recibida tanto por países que cuentan con normas que regulan específicamente el uso de spyware, como por otros en las que no se ha legislado aun sobre la cuestión. En el primer grupo se encuentra, por ejemplo, el Reino Unido, donde el hackeo estatal ha sido regulado en la "Investigatory Powers Act" (IPA) de 2016, que permite utilizar cualquier medio técnico a fin de concretar ya sea una interceptación de comunicaciones ("Targeted Interception") -regulada en el art 15(2) de la citada ley[106]- o una "interferencia de equipos" ("Targeted Equipment Interference" o TEI), normada en el art. 99 §§ (1)(a) al (8) de la IPA. La primera diferencia entre ambas medidas de vigilancia es que conforme se desprende de lo dispuesto en el art. 99(6) de la ley, la TEI solo puede emplearse para obtener comunicaciones u otros datos que estén almacenados en un sistema de telecomunicaciones antes o después de ser transmitidos[107]; mientras que la TI se usa para capturar las comunicaciones mientras se encuentran "en tránsito". La segunda es que la "interceptación de comunicaciones" se encuentra sometida a la limitación prevista en el art. 56(1) de la misma ley, que dispone que la prueba resultante no puede ser válidamente incorporada al

[103] Ver: EUROJUST: "Cybercrime Judicial Monitor", Eurojust Limited, N°. 2, noviembre 2016, págs. 38/39 (notas omitidas). En tal caso, la información solo puede ser copiada y el juez a cargo de la investigación, a través del ministerio público fiscal, debe informar en forma inmediata al Ministro de Justicia, a cargo de notificar al Estado extranjero involucrado (en caso de que pueda ser identificado).

[104] Cfr. PARKIN, Simon: "'Every message was copied to the police…", cit. En más detalle, sobre TOLA, ver: EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 32.

[105] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 15.

[106] En el que se autoriza la interceptación, por cualquier medio, de una comunicación postal o telecomunicación y sus "datos secundarios".

[107] Art. 99(8) de la IPA.

proceso (a fin de resguardar el secreto sobre los métodos utilizados), restricción que no aplica a las TEI.

Otras naciones de Europa que han recibido evidencia proveniente de EncroChat también cuentan con disposiciones en su legislación nacional que autorizan el uso de "medios técnicos" (informáticos) para capturar las comunicaciones u obtener datos digitales, como por ejemplo Suecia[108] y Suiza[109]. Asimismo, han incorporado normas sobre la materia los legisladores de Dinamarca[110], España[111], Polonia y Rumania[112]. Sin perjuicio de lo expuesto, la ausencia de regulación expresa no supone necesariamente una prohibición del uso de técnicas de hackeo como medida de investigación. De hecho, un reporte del Parlamento Europeo determinó que la mayor parte de los países del continente recurrían a las referidas técnicas, ya sea con sustento en normas procesales específicas o amparándose en las "zonas grises" de su legislación[113].

Es así que, por ejemplo, en Alemania, se recurre al uso de spyware estatal para interceptar comunicaciones, ya sea con apoyo en lo establecido en el art. § 20k(1) de la ley orgánica de la policía federal alemana (*Bundeskriminalamtgesetz* – BKAG)[114] o de conformidad con las disposiciones de los arts. §§ 100a, 100b y 100e del Código de Procedimientos en lo Penal (*Strafprozessordnung* – StPO) de ese país, que regulan la interceptación de telecomunicaciones y el registro online[115]. De igual manera, en Italia, los tribunales han ratificado en varios precedentes la legitimidad del uso de programas espías por parte de las agencias de orden público, amparadas en la aplicación analógica de las normas procesales vigentes[116]. En este escenario, parece claro que, si la ausencia de normas que regulen expresamente el uso de spyware no supone un obstáculo para que las autoridades de esos países recurran a dichas técnicas para obtener evidencia digital, tampoco debiera serlo para admitir la prueba recolectada de esa manera por otros estados.

La cuestión más problemática no es, entonces, la relativa a la posible inadmisibilidad de la evidencia recolectada en las operaciones EncroChat, Sky ECC y An0m por considerar que no podría haber sido obtenida conforme las normas de los países que la recibieron; sino si es legítima la incorporación, en los tribunales de estos

---

[108] Ver: EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 10.
[109] Ver: EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12.
[110] Ver: EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 10.
[111] Para un análisis más detallado de la normativa vigente en España, ver: BLANCO, Hernán: "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre", en InDret, Vol. 1/2021, 2021, págs. 431/501.
[112] Ver: EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 10.
[113] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., págs. 10 y 42 (citas omitidas).
[114] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 42.
[115] Cfr. ŠKORVÁNEK, Ivan / KOOPS, Bert-Jaap / CLAYTON NEWELL, Bryce / ROBERTS, Andrew: "My computer is my castle'…", cit., págs. 1013/1014.
[116] Sobre el tratamiento de este tema en la jurisprudencia italiana, ver: DE ZAN, Tomasso, "E-evidence and cross border data requests in Italia", en AA.VV., *EUnited against crime: Improving criminal justice in European Union cyberspace*, Instituti Affari Internazionali, 2016, Roma, págs. 42/59; y ŠKORVÁNEK, Ivan / KOOPS, Bert-Jaap / CLAYTON NEWELL, Bryce / ROBERTS, Andrew: "My computer is my castle'…", cit., págs. 1016/1018.

últimos estados, de prueba informática referida a sus ciudadanos que ha sido obtenida por las agencias de orden público de otra nación a través de una *medida restrictiva del derecho a la privacidad que se proyectó más allá de los límites establecidos a su jurisdicción* (de acuerdo al principio de territorialidad).

Al respecto, algunos autores señalan que, ante la ausencia de iniciativas internacionales efectivas para permitir las investigaciones transfronterizas en la internet, prohibir iniciativas nacionales para el acceso transfronterizo no constituye una alternativa realista[117]. En ese orden de ideas, BOJARSKI apunta que, en atención al carácter global del fenómeno del ciberdelito (aspecto que, aunque el autor no lo mencione, también podría aplicarse a la actuación de organizaciones criminales como las alcanzadas por las operaciones de EncroChat, Sky ECC y An0m), resulta casi imposible remediarlo sin autorizar a las agencias de investigación a perseguir a los responsables más allá de las fronteras de un determinado Estado[118].

En esa dirección, se han efectuado una serie de planteos en procura de conciliar las iniciativas nacionales que legitiman la adopción de medidas de obtención de prueba transfronterizas con el principio de proporcionalidad[119]. En tal contexto, un enfoque doctrinario apunta a relativizar la aplicabilidad del principio de territorialidad enfocándose en el carácter "virtual" del acceso de un Estado a los datos ubicados en otro, a cuyo efecto distinguen entre el tipo de ejercicio de la jurisdicción al que refería el principio de no intervención -el envío *físico* de agentes de las fuerzas de seguridad al territorio de otro Estado para arrestar a un sospechoso o llevar adelante una investigación penal- de la investigación informática, que no involucra el ingreso de agentes a otro país[120]. En la misma línea, BRIEHL y EHLSCHEID explican que en la medida en que el acceso a los datos por las autoridades investigadoras no vaya más allá del que podría tener el Estado afectado, la intensidad de la intrusión es tan baja (debido a la ausencia de presencia física de los funcionarios que la llevan a cabo dentro del territorio extranjero) que la búsqueda no puede ser considerada como una infracción a la soberanía de ese Estado[121].

---

[117] Cfr. DE HERT, Paul / BOULET, Gertjan, "Cloud computing and trans-border law enforcement access to private sector data. Challenges to sovereignty, privacy and data protection", en AA.VV., *Big data and privacy. Making ends meet*, Future of Privacy Forum & Stanford Center for Internet & Society, 2013, págs. 23/24.

[118] Cfr. BOJARSKI, Kamil, "Dealer, hacker, lawyer, spy…", cit., pág. 40 (citas omitidas).

[119] Aunque la mayoría de ellas han sido desarrolladas teniendo en miras no a medidas de vigilancia como las adoptadas en los casos en estudio, sino a los problemas planteados por el fenómeno de la "pérdida de (conocimiento de la) locación" —entendido como la imposibilidad de identificar la locación de los datos almacenados en servidores remotos ("computación en nube") a los efectos del ejercicio de las facultades de las autoridades judiciales y policiales; y el surgimiento de países que actúan como "refugios de evidencia digital", obstaculizando cualquier medida de cooperación judicial internacional para la obtención de prueba sobre ciberdelitos cometidos fuera de sus fronteras (al respecto, ver: BLANCO, Hernán, *Tecnología informática e investigación criminal*, cit., págs. 364/368).

[120] Cfr. KERR, Orin S. / MURPHY, Sean D., "Government hacking to light the dark web. What risks to international relations and international law?", en Stanford Law Review Online, vol. 70, 2017, pág. 66 (citas omitidas - énfasis añadido). En igual sentido, en la doctrina alemana, se pronuncia SCHAUMBURG (citado por SEITZ, Nicolai: "Transborder search: A new perspective in law enforcement?", en Yale Journal of Law and Technology, vol. 7, N° 1, 2005, págs. 23/50., págs. 33/34).

[121] Cfr. SEITZ, Nicolai, "Transborder search...", cit., pág. 41 (citas omitidas).

Otros autores entienden que incluso en registros transfronterizos realizados a sabiendas (o con la sospecha) de la ubicación extraterritorial de los datos, se podría acceder y recopilar los datos a efectos de ganar tiempo mientras se requiere el permiso del Estado afectado para utilizarlos en un proceso criminal concreto[122], postura que guarda algún tipo de similitud con la adoptada por las autoridades francesas en el caso EncroChat, en que dieron aviso a las autoridades de otros países sobre la medida que iba a adoptarse (aunque, por cierto, aclarando que iban a proceder con o sin permiso) y las invitaron a compartir los resultados de la misma).

Otro sector de la doctrina sostiene que debe admitirse una excepción "de buena fe" a la regla de la invalidez de las medidas transfronterizas, que se verificaría en el supuesto en que la autoridad encargada de la persecución asume erróneamente que los datos están ubicados en su territorio, o la ubicación de los mismos *no está clara o no puede ser identificada con certeza*. El argumento a favor de esta excepción es que, de lo contrario, el Estado actuante tendría que renunciar significativamente a sus atribuciones en su propio territorio soberano[123]. De este modo se fundó el precedente dictado por la Cámara Federal de Apelaciones del 8° Circuito de los EE.UU. *in re*: *US v. Horton*[124], en el que se convalidó la orden judicial que autorizó la introducción de un programa espía en una página web de intercambio de imágenes de explotación sexual infantil, mediante el cual se hackearon las computadoras de miles de usuarios (en su mayoría localizados fuera de la jurisdicción del juez que libró la mencionada autorización)[125], en el caso "Playpen"[126].

En orden a la cuestión sobre la admisibilidad de la evidencia obtenida en el extranjero mediante una medida que podría no ser viable en la legislación nacional o adoptada en violación al principio de territorialidad, cabe señalar que el Tribunal Europeo de Derechos Humanos (TEDH) ha establecido que el análisis sobre la admisibilidad de la prueba le corresponde, en principio, a los tribunales nacionales, conforme la legislación local[127]. Según la interpretación del tribunal continental de derechos humanos, el CEDH no establece reglas generales en orden a la admisibilidad de la evidencia, sino que deja dicho aspecto librado, en principio, al arbitrio de los legisladores nacionales[128]. Esta interpretación se funda en el principio de

[122] Cfr. SEITZ, Nicolai, "Transborder search...", cit., pág. 41 (citas omitidas).

[123] Cfr. SEITZ, Nicolai, "Transborder search...", cit., págs. 40/ 41 (citas omitidas – énfasis añadido). En esta última postura parecen haberse enrolado las autoridades de varios países consultados en el marco de un relevamiento publicado en 2016 por EUROJUST entre los expertos de la Red Judicial de Cibercrimen de Europa (European Judicial Cybercrime Network) junto con otros en Suiza, Noruega y los EE.UU. Ello así, desde que de los 20 países que respondieron que el acceso remoto es posible conforme su legislación, 16 señalaron que ello es o puede ser permitido *aún en los casos en que se desconoce la ubicación de los datos* que se pretende obtener. Algunos consignaron que ante la ausencia de indicios respecto de la localización de la información se presume que el sistema se encuentra dentro del territorio, aunque otros indicaron que dicha postura aún no ha sido objeto de ratificación jurisprudencial (ver: Eurojust, "Cybercrime Judicial Monitor", cit., págs. 38 y 39).

[124] No 16-3976 (2017).

[125] Ello, con aplicación de la "excepción de buena fe" reconocida en el precedente *United States v. León* de la Suprema Corte de los EE.UU. (468 U.S. 897; 1984).

[126] Sobre el caso, ver *infra*, § 4.3.

[127] Cfr. TEDH, Guía sobre el artículo 6…, cit., pág. 42, § 217, con cita de las SSTEDH *in re*: *Schenk v. Suiza*, §§ 45/46, *Moreira Ferreira v. Portugal* (no. 2) [pleno], § 83 y *Heglas v. República Checa*, § 84.

[128] Cfr. SSTEDH *in re*: *Brualla Gómez de la Torre v. España*, § 31 y *García Ruiz v. España* [pleno], § 28.

"reconocimiento mutuo", que a su vez se funda en la premisa de que todos los países miembros de la comunidad europea respetan los derechos fundamentales y cuentan con salvaguardas suficientes para protegerlos en su normativa procesal[129].

En este escenario, el rol del TEDH no es determinar si ciertas clases de evidencia (como, por ejemplo, en el caso, la proveniente de un hackeo masivo) son admisibles o no, sino que reside únicamente en evaluar *si el proceso en su conjunto* puede ser considerado "justo"[130]. A tal efecto, el tribunal procura balancear el interés individual con el interés público en la cooperación internacional efectiva en investigaciones criminales, en las que etapas cruciales del proceso deben ser revisadas desde el punto de vista del derecho de defensa. En estos supuestos, el TEDH lleva a cabo una evaluación integral a la luz de los requisitos del art. 6 CEDH, tomando a la cooperación transfronteriza como una extensión del procedimiento criminal del estado requirente[131]. Aun así, el tribunal europeo ha concluido en algunos casos que incluso la circunstancia de que los tribunales nacionales fundaran una condena exclusivamente en transcripciones de comunicaciones ilegalmente obtenidas no supone una violación al art. 6 CEDH[132]. Los únicos supuestos en los que el tribunal continental puede controvertir la interpretación de los tribunales nacionales sobre la cuestión son cuando se verifica una inobservancia "flagrante" de la ley nacional o la misma es aplicada arbitrariamente[133].

Por otra parte, en lo tocante a la posible interferencia ilegal en la soberanía de otro estado derivada de la interceptación de telecomunicaciones, el TEDH señaló en el caso *Weber and Saravia v. Alemania*[134]*,* que la exigencia de que las medidas de coacción encuentren sustento en la ley incluye también a las normas internacionales aplicables en el país involucrado[135]. En tal contexto, en sustento de alegaciones sobre la posible infracción del Derecho internacional por parte de un estado, resultante de la violación a la soberanía territorial de un estado extranjero, el TEDH requiere evidencia en la forma de "inferencias concordantes" en punto a que las autoridades del estado acusado han actuado en forma extra territorial de un modo inconsistente con la soberanía de su par extranjero y, por consiguiente, contraria al Derecho internacional[136].

Surge, pues, el interrogante de si la conducta desplegada por Francia (en el caso EncroChat), Bélgica (respecto de Sky ECC) y EE.UU. y Australia (con relación a An0m) responde a estos parámetros. En orden a ello, cabe tener presente, en primer lugar, que no existe ningún instrumento internacional que legitime el uso transfronterizo de *govware*, y que ninguno de los países antes mencionados requirió autorización de los

[129] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework for digital evidence rules in criminal investigations", en Computer Law & Security Review", Vol 49, 2023, pág. 21.
[130] Cfr. TEDH, *Guía sobre el artículo 6…*, cit., págs. 42/43, § 218 (énfasis añadido).
[131] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., pág. 20 (citas omitidas).
[132] Cfr. SSTEDH *in re*: *Khan v. Reino Unido*, § 34; *P.G. y J.H. v. Reino Unido*, § 76 y *Beraru v. Rumania*, §§ 72/73.
[133] Cfr. SSTEDH *in re*: *Kruslin v Francia*, § 29; *Société Colas Est y otros v. Francia*, § 43 y (*mutatis mutandis*) *Lavents v. Letonia*, del 28/11/2002, § 114; *Leyla Şahin v. Turquía* [pleno], § 88 y *Weber y Saravia v. Alemania*, § 90.
[134] § 86.
[135] Con cita, *mutatis mutandis*, de las SSTEDH *in re*: *Groppera Radio AG and Others v. Suiza*, § 68; *Autronic AG v. Suiza*, § 56; *Stocké v. Alemania*, § 54; y *Öcalan v. Turquía* [pleno], § 90.
[136] Cfr. STEDH *in re*: *Weber and Saravia v. Alemania*, § 87.

demás estados afectados antes de ejecutar las medidas de vigilancia que afectaron a dispositivos ubicados en territorio extranjero, en manos de ciudadanos extranjeros. Si bien es cierto que Francia alertó a algunos países europeos de que iba a llevar a cabo la operación, también lo es que dicha advertencia no constituyó un pedido de autorización, toda vez que las autoridades francesas dejaron en claro que la operación iba a seguir adelante con independencia de si las demás naciones la aprobaban o no. Ahora bien: la actitud posterior de los países afectados, en cuanto aceptaron la evidencia resultante -distribuida a través de EUROJUST- sin plantear objeciones al modo en que fue obtenida, lleva a preguntarse si ello no equivale a un consentimiento '*ex post*' o aprobación tácita de lo actuado. Tanto más cuando esta actitud se reiteró, inmediatamente después, en los casos Sky ECC y An0m.

Por otro lado, conforme la jurisprudencia del TEDH, la interceptación de telecomunicaciones por una agencia extranjera no genera responsabilidad para el estado que recibe los resultados de aquella *ni siquiera cuando dicha interceptación ha sido concretada a pedido* de este último. Esta regla general solo podría verse exceptuada, en opinión del tribunal continental, en caso de verificarse ciertos supuestos que *no aplican a los casos objeto del presente trabajo*, a saber: que la agencia extranjera haya estado "a disposición" del estado receptor de la evidencia y actuado en ejercicio de la autoridad de aquél; si el estado receptor asistió a la agencia extranjera en la concreción de la medida de un modo que pudiese considerarse ilícito de haber tenido lugar en territorio del primero; si el estado receptor tuvo control o poder de decisión sobre la actuación de la agencia extranjera[137]. No obstante ello, el TEDH si advirtió que la protección ofrecida por el CEDH se tornaría nula si los estados parte pudiesen eludirla encomendando la interceptación de comunicaciones a países no signatarios[138]. Sin embargo, este supuesto no se habría verificado ni en los casos EncroChat y Sky ECC (en los que la evidencia se repartió entre países europeos) ni tampoco en An0m, en el que la iniciativa de la medida partió de los EE.UU. y Australia, que sólo después de iniciada la operación compartieron la evidencia resultante con las naciones europeas.

En lo tocante a la confiabilidad de la evidencia intercambiada a través de las fronteras, las limitaciones en el análisis del TEDH (que solo evalúa el cumplimiento de los requisitos formales para la cooperación internacional, pero ha establecido principios para el análisis de la evidencia generada en el extranjero) adquieren particular relevancia en lo tocante a la prueba digital, que es fácil de copiar e intercambiar, y puede ser utilizada en cientos de casos en múltiples jurisdicciones, como de hecho ocurre en los casos en estudio. Como contrapartida, las dificultades de las defensas para cuestionar la legalidad y confiabilidad de la evidencia se acrecientan, toda vez que el proceso de obtención y análisis interjurisdiccional de la prueba se mantiene opaco, en la medida en que las circunstancias exactas en las que la misma fue recogida y procesada puede ser desconocida incluso para los fiscales que la reciben y deben utilizarla, ya sea debido a la existencia de acuerdos de confidencialidad o por la no investigación de aquellas circunstancias. El resultado es la falta de un remedio efectivo para que las

[137] Cfr. SSTEDH *in re*: *Al-Skeini y otros v. Reino Unido* [pleno], §§ 130/139 y *Jaloud v. Países Bajos* [pleno], §§ 139 y 151; citados en *Big Brother Watch y otros v. Reino Unido* [pleno] § 495 (énfasis añadido).
[138] Cfr. STEDH *in re*: *Big Brother Watch y otros v. Reino Unido* [pleno] § 497.

defensas puedan revisar y cuestionar la evidencia proveniente del extranjero, así como de un marco jurídico que permita el control judicial[139].

La jurisprudencia del TEDH sobre estas cuestiones es relativamente escasa. En el caso *A.M v. Italia*[140], en el que no se le permitió a la defensa participar en el interrogatorio de testigos extranjeros, el tribunal consideró violentado el art. 6(3) del CEDH debido a que la sentencia se había fundado en forma decisiva en los dichos de esos testigos. En *Echeverri Rodriguez v. Países Bajos*[141], el TEDH estableció que el uso de evidencia extranjera en procedimientos locales podía generar la responsabilidad del Estado, pero enfatizó a la vez que el análisis principal sobre la prueba debía realizarse durante el juicio y no en la investigación previa. En opinión de STOYKOVA, esta última exigencia puede resultar problemática en atención a la ya señalada ausencia de información confiable sobre el modo en que pudo haberse obtenido la evidencia en el país de origen y de la regla que impide a un país revisar las medidas adoptadas en otro[142].

3.3. Planteos en contra de la utilización de la prueba obtenida mediante medidas de vigilancia trasnacionales. Respuesta de los tribunales nacionales. Resultado de la consulta al TJUE.

Como era esperable en atención a las características de las medidas de vigilancia adoptadas con relación a los usuarios de EncroChat, Sky ECC y An0m y su alcance trasnacional, se han producido numerosos planteos cuestionando su legitimidad ante los tribunales de los países en los que residen las personas involucradas en las investigaciones. Así, en Francia el máximo tribunal penal la (*Cour de Cassation*, CdC) rechazó parcialmente, en un fallo reciente[143], un recurso interpuesto por los defensores de varios imputados cuestionando -entre otras cosas- la violación al principio de territorialidad y alegando que la medida de vigilancia dispuesta respecto del sistema EncroChat debió haberse limitado a los teléfonos en uso en territorio francés[144]. Ello, a pesar de que -como ya se señaló[145]- dicha limitación era imposible de implementar en la práctica.

También en lo tocante a este último hackeo, en los Países Bajos los abogados defensores han controvertido la posición oficial del Ministerio Público Fiscal en punto a que el gobierno de ese país no tuvo participación alguna en la introducción del "implante técnico" en los servidores de EncroChat. Se apoyan, a tal efecto, en la información -revelada en expedientes criminales en el Reino Unido y otras naciones- sobre la existencia de una estrecha cooperación entre las agencias de orden público

[139] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., pág. 20 (citas omitidas).
[140] Cfr. STEDH *in re*: *A.M. v. Italia*, §§ 26/27.
[141] Cfr. STEDH *in re*: *Echeverri Rodríguez v. Países Bajos*.
[142] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., págs. 20/21 (citas omitidas).
[143] Ver: GOODWIN, Bill: "French Supreme Court raises constitutional questions over EncroChat hacking secrecy", en Computer Weekly, publicado el 3/2/2022, obtenido en: https://www.computerweekly.com/news/252512850/French-Supreme-Court-raises-constitutional-questions-over-EncroChat-hacking-secrecy.
[144] Cfr. GOODWIN, Bill: "French Supreme Court raises constitutional questions…", cit.
[145] Ver *supra*, § 2.1.

neerlandesas y francesas en la operación. En sentido opuesto, los acusadores públicos señalaron que no correspondía a los tribunales neerlandeses evaluar la legalidad de la operación desarrollada en Francia para capturar los mensajes de EncroChat posteriormente compartidos con las autoridades de otros países[146]. La discusión en Suecia se dio en términos casi idénticos[147].

En Inglaterra, se objetó el libramiento de una orden de "TEI"[148] para requerir evidencia sobre ciudadanos británicos que *ya había sido capturada* por la Gendarmería francesa sin que mediara un pedido previo de cooperación internacional entre ambos países[149], lo que para los defensores supuso autorizar a un poder extranjero -Francia- a hackear los teléfonos de los 9.000 usuarios británicos de EncroChat[150].

En Alemania se criticó el uso, en causas tramitadas en ese país, de evidencia obtenida mediante una medida concretada en Francia, que no hubiese podido implementarse conforme la ley alemana y que afectó severamente el derecho a la privacidad de ciudadanos alemanes[151]. Este argumento fue esgrimido, asimismo, en uno de los pocos casos vinculados a EncroChat que se ha dado a conocer hasta ahora en España, en el que los letrados de dos personas acusadas por narcotráfico solicitaron que todas las pruebas provenientes del hackeo a dicha plataforma se apartaran del caso, puesto que -en su opinión- las intervenciones telefónicas habían sido prospectivas e indiscriminadas. Señalaron, al respecto, que, aunque aquellas se ajustaran al derecho francés, no eran legales conforme la normativa española[152].

Una objeción muy similar se presentó, en relación con la operación concretada mediante el sistema An0m, contra la decisión del FBI de "triangular" la recolección de evidencia a través de un tercer país para eludir los obstáculos que le presentaba la legislación de los EE.UU., argumentándose que esta maniobra podría constituir una violación al "espíritu" de las normas, si no a su texto[153]. A su vez, atendiendo a dicha triangulación y al desconocimiento sobre cuál es ese tercer país, algunos defensores en Alemania han solicitado que no se admita la evidencia proveniente de An0m, apuntando que no es posible verificar dónde y con qué base legal fue obtenida[154]. Según informó el

---

[146] Cfr. GOODWIN, Bill: "Dutch prosecutor ordered to give evidence on EncroChat hack", en Computer Weekly, publicado el 13//2021, obtenido en: https://www.computerweekly.com/news/252503908/Dutch-prosecutor-ordered-to-give-evidence-on-EncroChat-hack.

[147] Ver: Tech News Terminal: "Swedish Court Docket finds ambiguities…", cit.

[148] Ver *supra*, § 3.2.

[149] Cfr. GOODWIN, Bill "Encrochat: Appeal court finds 'digital phone tapping' admissible…", cit. (énfasis añadido).

[150] Cfr. SYMONDS, Tom: "Encrochat: Secret network messages can be used in court, judges rule", en BBC News, publicado el 5/2/2021, obtenido en: https://www.bbc.com/news/uk-55953247.

[151] Argumentos casi idénticos fueron planteados en Suiza (ver: Nord News: "Criticism of the EncroChat evidence is growing", publicado el 23/3/2021, obtenido en: https://nord.news/2021/03/23/criticism-of-the-enchrochat-evidence-is-growing/) y en Suecia (Ver: Tech News Terminal: "Swedish Court Docket finds ambiguities…", cit.).

[152] Cfr. DORTA, Irene: "La Audiencia Nacional avala a un juez francés que intervino el 'chat de los narcos'", en La Razón (España), publicado el 8/12/2021, obtenido en: https://www.larazon.es/espana/20211207/54rcryfuzzeczbjuf3zpv5tine.html.

[153] Ver: PARKIN, Simon: "'Every message was copied to the police'…", cit.

[154] Ver: KLAUBERT, David: "Crypto service of the FBI: An0m chats can be used in court according to the Frankfurt District Court", en Teller Report, publicado el 25/1/2022, obtenido en:

propio FBI, la confidencialidad respecto de la identidad de esa otra nación se implementó a pedido de la misma, que solicitó que su participación se mantenga en secreto. De allí que, conforme los términos del acuerdo de cooperación entre ambos países, el FBI no puede "ni ahora ni en el futuro" revelar ese dato[155]. Lo que se señala, respecto de esta circunstancia -que, en la práctica, les impide a los defensores de las personas acusadas en base a la evidencia obtenida desde la plataforma An0m conocer qué normas se aplicaron para legitimar la medida y, en su caso, cuestionar su legitimidad con base a ellas- es que genera el interrogante de porqué, si lo actuado fue perfectamente legal, este tercer país insiste en mantenerse en el anonimato[156].

En el Reino Unido los tribunales se expidieron sobre planteos de las defensas objetando el uso de la evidencia proveniente del hackeo a EncroChat en el precedente *A, B, D & C v. Regina*. En el fallo citado, un tribunal de alzada de la ciudad de Liverpool[157] concluyó que la National Crime Agency (NCA) británica no les solicitó a las autoridades francesas que ejecutaran el hackeo a EncroChat, ni tampoco tenía competencia para hacerlo. Explicó, en tal sentido, que Francia ya había decidido avanzar con la operación e implantar el malware en todos los teléfonos de la compañía, estuviesen donde estuviesen. Por ende, no era necesaria una solicitud del Reino Unido, que tampoco tuvo lugar[158]. Entendió, por consiguiente, que el objeto de la OEI librada por ese país fue obtener la evidencia recolectada por las fuerzas de seguridad francesas como resultado de una medida de vigilancia que, se sabía, iba a llevarse a cabo en cualquier caso[159].

Por añadidura, el tribunal esgrimió un segundo argumento, bastante más problemático, para rechazar la afirmación de las defensas en punto a que las autoridades británicas habían convalidado, en la práctica, una intrusión informática (prohibida en la legislación del Reino Unido) perpetrada por una agencia policial extranjera. Ello así, toda vez que los sentenciantes afirmaron que dicha prohibición no era aplicable al caso, debido que la interceptación de los teléfonos *no se había concretado merced a una conducta desarrollada en el Reino Unido*[160]. Esta afirmación, no obstante, choca con el hecho evidente de que, al haberse descargado en los teléfonos de todos los usuarios, *la intrusión tuvo lugar en forma simultánea en todos los países en los que dichos equipos se encontraban* cuando el malware ingresó a su sistema, incluyendo naturalmente al Reino Unido[161]. No obsta a lo expuesto la circunstancia de que la infiltración original (o "infección", como la denominaron los investigadores) haya tenido lugar en Francia, desde que la propia mecánica del hackeo (en cuanto se trató de

https://www.tellerreport.com/life/2022-01-25-crypto-service-of-the-fbi--anom-chats-can-be-used-in-court-according-to-the-frankfurt-district-court.SJmtuhpTK.html.

[155] Cfr. Cox, Joseph: "A European country helped the FBI intercept An0m messages, but it wants to remain hidden", cit.

[156] Cfr. Cox, Joseph: "A European country helped the FBI intercept An0m messages, but it wants to remain hidden", cit.

[157] División Penal del Tribunal de Apelación de la Corona en Liverpool.

[158] *A, B, D & C v. Regina*, cit. § 30.

[159] *A, B, D & C v. Regina*, cit. § 31.

[160] *A, B, D & C v. Regina*, cit. § 32.

[161] Prueba de que la intrusión informática alcanzó a los teléfonos propiamente dichos es que los mensajes fueron capturados en formato "plaintext" (es decir, sin encriptar), lo que -como reconocieron los propios sentenciantes en el fallo citado- solo pudo ocurrir si fueron obtenidos mientras se encontraban almacenados en los propios dispositivos antes de encriptarse o tras haber sido desencriptados, ya que si hubiesen sido interceptados "en tránsito" hubiesen estado cifrados.

un "ataque de cadena de suministro"[162]) requirió de *una segunda infección* en cada uno de los dispositivos conectados a la red.

En un pronunciamiento ulterior[163], vinculado con el anterior, el Alto Tribunal Divisional[164], afirmó, que no le correspondía expedirse sobre la legalidad de la intrusión informática concretada en Francia, toda vez que la cuestión sobre la legalidad de la orden judicial que autorizó el hackeo a EncroChat era de competencia exclusiva de los tribunales franceses, de conformidad con la regla general conforme la cual las actuaciones cumplidas en otro país europeo para la obtención de evidencia deben ser tomadas como válidas a los efectos de una OEI[165].

En Alemania, sendos fallos del Alto Tribunal Regional de Bremen y del Alto Tribunal Regional de Hamburgo dictados en 2020 convalidaron, inicialmente, el uso como prueba de cargo, en ese país, de la evidencia proveniente de EncroChat[166]. No obstante ello, con posterioridad el Tribunal del Distrito de Berlín suspendió, en una resolución dictada en julio de 2021, un juicio oral sustentado en la evidencia obtenida en el hackeo del referido sistema, en el entendimiento de que -aunque legal en Francia- la medida violentaba la ley alemana[167]. En sustento de su decisión, el mencionado tribunal señaló que, conforme las normas vigentes en la Unión Europea, los estados miembros están obligados a notificar a sus pares antes de interceptar las telecomunicaciones de ciudadanos de otro país en territorio extranjero, lo cual -según la información disponible en ese momento- no parecía haber ocurrido en el caso[168].

Este último fallo, sin embargo, fue apelado por los acusadores y revocado por la alzada. La decisión de dejar sin efecto la resolución del juez de grado se fundó, en primer lugar, en el entendimiento de que los tribunales de Alemania no están facultados para cuestionar la legitimidad de un procedimiento efectuado conforme las normas de otro país, en la medida en que la evidencia no haya sido obtenida en cumplimento de un pedido de asistencia legal mutua iniciado en Alemania[169]. Ello, ya que de lo contrario se estaría debilitando la "confianza mutua" entre los países miembros de la UE. Asimismo, los sentenciantes explicaron que si bien la medida concretada en Francia no parecía cumplir con los requisitos establecidos en la normativa procesal alemana, ello no implicaba necesariamente la prohibición del uso de la evidencia resultante, destacando

[162] Ver, al respecto, lo señalado *supra*, § 2.1).
[163] *R(C) v. Director of Public Prosecutions*, cit.
[164] Alto Tribunal Divisional de Justicia.
[165] *R(C) v. Director of Public Prosecutions*, § 50.
[166] Cfr. WAHL, Thomas: "Dismantled encryption networks: German courts confirmed use of evidence from EncroChat surveillance", en Eucrim, publicado el 20/3/2021, obtenido en: https://eucrim.eu/news/dismantled-encryption-networks-german-courts-confirmed-use-of-evidence-from-encrochat-surveillance/.
[167] Ver: Fuentitech.com: "Berlin court overturned ban on EncroChat evidence in criminal trials", cit.
[168] GOODWIN, Bill: "Berlin court finds EncroChat intercept evidence cannot be used in criminal trials", publicado en Computer Weekly, obtenido en: https://www.computerweekly.com/news/252503524/Berlin-court-finds-EncroChat-intercept-evidence-cannot-be-used-in-criminal-trials.
[169] En dicho orden de ideas, el tribunal consideró acreditado también que las autoridades alemanas no habían estado involucradas en la decisión de sus pares francesas de concretar la operación. En esa dirección, concluyeron que la evidencia no había sido compartida con Alemania con motivo de un pedido de asistencia legal mutua, sino enviada voluntariamente por las autoridades francesas sin que mediara consulta previa.

que la prueba podía ser considerada como un "hallazgo casual", lo que permitía su utilización para enjuiciar a los usuarios alemanes de EncroChat[170]. En igual sentido, entendieron que tampoco la circunstancia de que se hubiese omitido la notificación a Alemania imponía dicha prohibición, dado que la actuación posterior de las autoridades alemanas dejaba en claro que no se hubiesen opuesto a la investigación[171].

En esta misma dirección, el Tribunal Federal de Justicia de Alemania (*Bundesgerichtshof* o BGH) convalidó también el uso de la evidencia proveniente de EncroChat con base en el principio de "libertad probatoria" establecido en el art. 261 del StPO, el cual, en opinión del tribunal, permitía compensar las diferencias entre la legislación alemana y la francesa en orden a la legitimidad de la medida de vigilancia adoptada. En ese orden de ideas, el BGH explicó que no correspondía confrontar lo actuado en Francia con la normativa alemana aplicable, y que la revisión del cumplimiento con la legislación extranjera no constituía un prerrequisito para el uso de la evidencia en los procesos penales desarrollados en ese país. Por último, el tribunal coincidió en concluir que de la posible violación del deber de notificar a Alemania sobre la interceptación iniciada en Francia no podía derivar en la prohibición del uso de la prueba resultante, por considerar dudoso que dicho deber haya sido establecido en resguardo de los individuos y siendo que, a todo evento, en la ponderación de intereses predominaba el del Estado en perseguir penalmente a los acusados[172].

Los tribunales alemanes también convalidaron el uso de la prueba proveniente de la operación encubierta que involucró a la plataforma An0m, señalando -con remisión a los fallos dictados en relación con EncroChat- que la exclusión de la evidencia solo podía darse en casos excepcionales, cuando se demostrase una violación de principios o derechos fundamentales[173]. Al respecto, el Alto Tribunal Regional de Franckfurt concluyó que el "tercer estado" europeo (no identificado) que intervino a instancias del FBI "probablemente" actuó en línea con la normativa europea; que no se apreciaba que la implementación de un falso sistema de mensajería secreta violentase el CEDH y que las autoridades alemanas no habían tenido intervención en la adquisición de los datos intercambiados a través de An0m[174]. El Alto Tribunal Regional de Darmstadt, empero, adoptó una postura más crítica, en cuanto estableció que la evidencia producida en esta última operación era solo "provisionalmente" admisible, encomendándole al acusador estatal averiguar la identidad del "tercer país" y en qué términos se libró la orden judicial que autorizó la recolección de la prueba[175].

En España, los planteos de la defensa contra el uso de la prueba proveniente de EncroChat en un caso de narcotráfico fueron rechazados por el magistrado interviniente en noviembre de 2021, en una decisión posteriormente convalidada por la Sala Penal de la Audiencia Nacional. En sustento de su decisión, el juez de primera instancia destacó que la cooperación recíproca y la confianza entre los estados de la Unión Europea le impedían cuestionar lo decidido por su par de Francia. Puntualizó, asimismo, que la intervención de EUROPOL y EUROJUST en el caso garantizaba la regularidad de lo

[170] Ver: Fuentitech.com: "Berlin court overturned ban on EncroChat evidence…", cit.
[171] Ver: Fuentitech.com: "Berlin court overturned ban on EncroChat evidence…", cit.
[172] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence…", cit..
[173] Ver: KLAUBERT, David: "Crypto service of the FBI…", cit.
[174] Cfr. MONROY, Matthias: "German An0m investigations: The mysterious EU third state", cit.
[175] Cfr. MONROY, Matthias: "German An0m investigations: The mysterious EU third state", cit.

actuado[176]. En su apelación, las defensas sostuvieron que, aunque la legislación francesa permitiese la interceptación de datos, ello no suponía que la misma, en cualquier extensión, duración y medida, fuese legal e insusceptible de nulidad por vulnerar el derecho al secreto de las comunicaciones y a la intimidad. Sin embargo, la Sala en lo Penal de la Audiencia Nacional rechazó ese argumento, recordando que la confianza existente entre los Estados pertenecientes a una misma comunidad jurídica (en este caso, España y Francia) determina que lo actuado fuera de las fronteras del primer país tenga visos de regularidad y licitud dentro de las mismas[177].

En sentido opuesto, desde la doctrina española ZARAGOZA TEJADA ha señalado que a su modo de ver, resulta dudoso que los criterios de "no indagación" y "hallazgo ocasional" sean suficientes para concluir que la prueba obtenida mediante el hackeo de la red EncroChat pueda ser utilizada en un proceso penal en territorio español, destacando, en tal sentido, que la jurisprudencia de la Sala Segunda del TS ha venido señalando que el principio de no indagación no puede constituir una auténtica "patente de corso" que pueda aplicarse sin fisuras a cualquier prueba entregada en virtud de un mecanismo de cooperación con un Estado extranjero, sino que deben observarse unos parámetros mínimos esenciales del proceso penal, que deben ser respetados en orden a la utilización de dicho material probatorio[178]. En esa misma dirección, Ibáñez López-Pozas destacó que a nivel europeo, la Gran Sala del Tribunal de Justicia de la Unión Europea (TJUE) manifestó, en un fallo del 21/12/2011 (asuntos acumulados C-411/2010, 239531/2011 y 493/2010) que "…*El derecho de la Unión se opone a la aplicación de una presunción irrefutable según la cual el Estado miembro designado como responsable* [...] *respeta los derechos fundamentales de la Unión Europea*"[179].

Lo cierto es, sin embargo, que en respuesta a los interrogantes planteados por el Tribunal Regional (*Landgericht*) en lo Civil y Penal de Berlín (Alemania)[180], la Abogada General Tamara Capeta del TJUE presentó, con fecha 26 de octubre de 2023, sus

[176] Cfr. DORTA, Irene: "La Audiencia Nacional avala a un juez francés…", cit.

[177] Auto 3/2022 del 5 de enero de 2022 (La Ley 1755/2022), de la Sección 4° de la Sala en lo Penal de la Audiencia Nacional. Ver, al respecto: GABILONDO, Pablo: "El WhatsApp secreto que usaban los narcos se vuelve en su contra ante la justicia", en El Confidencial, publicado el 26/1/2022, obtenido en: https://www.elconfidencial.com/espana/2022-01-26/encrochat-whatsapp-narcos-audiencia-nacional_3363806/.

[178] Cfr. ZARAGOZA TEJADA, Javier Ignacio: "Operaciones encubiertas digitales y convencionales. Un análisis desde la perspectiva de los derechos fundamentales y del derecho comparado", en AAVV, *La investigación penal en el entorno digital. Estudios sobre el impacto de las nuevas tecnologías digitales en el proceso penal*, Hammurabi, Buenos Aires, 2023, pág. 214 (con cita de las SSTS 456/2013 y 816/2021).

[179] Cfr. IBÁÑEZ LÓPEZ-POZAS, Fernando L.: "De las masivas interceptaciones de datos a las masivas vulneraciones de derechos fundamentales: la respuesta del Tribunal de Justicia de la Unión Europea", en Diario La Ley, N° 10033, Sección Tribuna, Wolters Kluwer, 21/3/2022 (citado de documento electrónico), pág. 11.

[180] En el marco del asunto C-670/22, *Stantsanwaltschaft Berlin v. M.N.*, del TJUE. Allí, el tribunal regional alemán planteó una serie de interrogantes referidos a la autoridad competente para librar una orden europea de investigación (OEI), la posibilidad de utilizar dicho instrumento para obtener evidencia ya recolectada por el país requerido, la admisibilidad de dicha evidencia cuando su integridad no puede ser verificada independientemente por el país requirente y la medida que derivó en su obtención no hubiese sido admisible en este último; como así también si podría derivarse una prohibición de la utilización de las pruebas a partir de los principios de efectividad y equivalencia del Derecho de la Unión Europea.

conclusiones ante el tribunal[181], proponiendo que responda a las consultas del *Landgericht* de Berlín señalando que: (a) el Derecho de la Unión Europea no exige que la OEI para el traslado de pruebas existentes que se hayan obtenido mediante intervención de telecomunicaciones sea emitida por un tribunal cuando en el Derecho nacional del país requirente, un fiscal puede ordenar el traslado en un caso interno similar; (b) la evaluación de la necesidad y proporcionalidad de una OEI dirigida al traslado de pruebas existentes corresponde a la autoridad de emisión, con la posibilidad de que el tribunal competente controle tal evaluación (tomando en consideración que el acceso a los datos de comunicación constituye una injerencia grave sobre la vida privada, que solo puede justificarse por un interés público importante en la investigación y persecución de delitos); (c) al decidir si puede, o no, emitir una OEI para el traslado de pruebas ya existentes, la autoridad de emisión no puede examinar la legalidad de la obtención de pruebas subyacente en el Estado de ejecución, siendo irrelevante, en orden a ello, si las medidas se ejecutaron en el territorio del Estado de emisión o en interés del mismo; (d) la notificación que debe llevar a cabo el Estado que -unilateralmente- intervenga telecomunicaciones en el territorio de otro puede dirigirse a cualquier autoridad que considere pertinente; y (e) el Derecho de la Unión Europea no regula la admisibilidad de las pruebas recabadas mediante una OEI, sino que dicho aspecto se rige por el Derecho nacional, el cual debe respetar los derechos de defensa consagrados en los arts. 47 y 48 del CEDH.

4. LA INJERENCIA SOBRE EL DERECHO A LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES. LOS PRINCIPIOS DE PROPORCIONALIDAD Y ESPECIFICIDAD

4.1. El derecho a la privacidad en el contexto jurídico europeo.

En atención al carácter masivo de las operaciones de hackeo estatal dirigidas contra EncroChat y Sky ECC (con más de 60.000 usuarios afectados en cada caso) y el alcance de la operación encubierta desarrollada en An0m (casi 10.000 usuarios), era de esperar que -como finalmente ha ocurrido- un alto porcentaje de los planteos invalidantes ensayados por las defensas se centraran en denunciar una injerencia indebida en el derecho a la intimidad y privacidad de las personas afectadas.

Este derecho se encuentra amparado en el art. 12 de la Declaración Universal de los Derechos Humanos y en el art. 17 (incisos 1° y 2°) del Pacto Internacional de Derechos Civiles y Políticos. Más específicamente, en el plano europeo, ha sido consagrado en el art. 7 de la Carta de Derechos Fundamentales de la Unión Europea y en el art. 8.1 del CEDH[182], En particular, el art. 8.2 de este último convenio establece que cualquier injerencia de la autoridad pública en el ejercicio del derecho de mención solo es legítima cuando la misma "*…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*

[181] Obtenido en: https://curia.europa.eu/juris/document/document.jsf;jsessionid=EEF3F45D476085A9ADBA8A86C66FF78D?text=&docid=279144&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=100225.

[182] En los que se consagra el derecho al respeto a la vida privada y familiar, el domicilio y las comunicaciones.

económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

Sin duda alguna, el recurso a técnicas sofisticadas de vigilancia como las empleadas en los casos EncroChat, Sky ECC y An0m conlleva una restricción de mayor importancia sobre el derecho a la intimidad de las personas que las medidas tradicionalmente empleadas, en la medida en que permitió acceder a la totalidad de la información que los usuarios almacenaban en sus teléfonos móviles, que en el contexto de la vida en las sociedades modernas comprende una enorme cantidad y variedad de datos de carácter personal y sensible[183]. Y ello, incluso en dispositivos que -como los que aquí se analizan- se utilizaban únicamente para el intercambio de mensajes encriptados.

Sin embargo, también es cierto que el empleo de esta clase de técnicas deviene imprescindible para sostener la facultad estatal de monitorear las comunicaciones de los ciudadanos (en los casos establecidos en las leyes y con la autorización de la autoridad competente) frente al surgimiento de nuevas herramientas tecnológicas con capacidad anti forense, como -por ejemplo- los sistemas de mensajería encriptada reforzada como EncroChat y Sky ECC. En relación con ello, organismos representantes de las agencias de orden público, como la IACP o EUROPOL, destacan el incremento en la efectividad de las investigaciones que supone el uso de técnicas de hackeo, sin las cuales en muchos casos puede resultar imposible investigar conductas ilícitas y perseguir eficazmente a los criminales que las cometen[184].

En este escenario, el Parlamento Europeo señaló que en la medida en que las prácticas de hackeo estatal sean necesarias para superar el problema de "quedar a oscuras" ("going dark") y proporcionales para cumplir con su objetivo, los ordenamientos procesales nacionales pueden legítimamente restringir el derecho a la privacidad mediante la sanción de disposiciones legales que regulen el uso de dichas técnicas incorporando límites y requisitos apropiados[185]. En ese orden de ideas, se enfatiza que la normativa local debe garantizar que el uso de técnicas de hackeo *no sea indiscriminado o masivo*[186], exigencia que, *a priori*, podría parecer incongruente con el modo en que se produjo la interceptación de las comunicaciones en los casos de EncroChat, Sky ECC y An0m.

En línea con la postura del Parlamento Europeo, la mayoría de los ordenamientos procesales en los países en los que impactaron las operaciones antes mencionadas contienen disposiciones que limitan el alcance del recurso a técnicas sofisticadas de vigilancia estatal. Así, por ejemplo, en Francia, el empleo de estas medidas está restringido a la investigación de "delitos graves" especialmente enumerados en los arts.

---

[183] Como lo destacó, en forma acertada, la Suprema Corte de Justicia de los EE.UU. al fallar en el precedente *Riley v. California* (134 S. Ct. 2473, del 2014).

[184] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 21 (énfasis eliminado). Con cita de International Association of Chiefs of Police (IACP): "Data, privacy and public safety: A law enforcement perspective on the challenges of gathering electronic evidence", IACP, 2015 Summit Report.

[185] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 22.

[186] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 69 (énfasis añadido).

706-73 y 706-73-1 del CPC francés, que incluye a ilícitos propios de la criminalidad organizada, terrorismo y cibercrimen[187]. Lo mismo ocurre en el Reino Unido, en el que el art. 106(1)(a) de la IPA dispone que, a los efectos de autorizar el uso estatal de spyware, la TEI sólo puede emitirse a efectos de prevenir o detectar un "delito serio".

En el derecho procesal alemán, el art. §100a(3) del StPO demanda que la autorización de una medida de este tipo este precedida por una sospecha razonable sobre la posible comisión de un delito y que el empleo de técnicas de hackeo se dirija únicamente contra el sospechoso u otras personas que puedan estar comunicándose con aquél. En igual sentido, en los Países Bajos, la normativa procesal establece que el recurso a técnicas de hackeo legal está restringida a los equipos utilizados por las personas sospechosas de haber cometido un delito[188]. Por último, en España, el uso estatal de spyware para la investigación criminal está regulado en las nuevas disposiciones introducidas en el Título VIII de la Ley de Enjuiciamiento Criminal (LEC) a través de la Ley Orgánica 13/2015, del 5 de octubre[189]. En tal contexto, el legislador español ha restringido el uso de dicha herramienta a la investigación de una serie de delitos considerados "graves" o de investigación compleja[190], además de disponer que el juez autorizante debe efectuar un estricto juicio de proporcionalidad antes de librar la orden respectiva[191].

Resulta evidente que los legisladores nacionales tuvieron como referencia, al sancionar las disposiciones referenciadas en los párrafos precedentes, a los métodos de hackeo legal que venían empleándose desde comienzos del presente siglo, usualmente centrados en la intrusión de equipos (teléfonos móviles u ordenadores) de personas específicas, mediante "vectores de ataque" (por lo general correos electrónicos o mensajes de texto) específicamente elaborados para generar una acción que permitiese el ingreso del spyware estatal (conforme la modalidad conocida como "spear phishing"). Sin embargo, y como se aprecia fácilmente, los hackeos concretados en contra de EncroChat y Sky ECC excedieron largamente la modalidad antes mencionada, la que -por otra parte- resulta inaplicable contra sistemas cerrados como los implementados por dichas compañías, especialmente diseñados para prevenir una intrusión de ese tipo.

Lógicamente, el carácter novedoso de la metodología empleada por las agencias de orden público en los casos de mención genera dudas en orden a si el accionar estatal

---

[187] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 73.

[188] Cfr. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Legal frameworks*…, cit., pág. 50 (énfasis eliminado).

[189] Ver, al respecto: BLANCO, Hernán: "El hackeo con orden judicial en la legislación procesal española…", cit., págs. 431/501.

[190] Enumerados en el art. 588 septies (a)(1) de la LEC. En tal contexto, la decisión de legitimar el uso de spyware (también) para perseguir "[d]*elitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación*" ha generado las mayores críticas por parte de la doctrina española. Así, por ejemplo, BUENO DE LA MATA considera que la misma deja "una puerta peligrosamente abierta", que en su opinión se debería eliminar para evitar que el uso de esta herramienta de manera analógica quede librada a la discrecionalidad del juzgador (ver: BUENO DE LA MATA, Federico: "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el Fortalecimiento de las Garantías Procesales y la Regulación de las Medidas de Investigación Tecnológica", en Diario La Ley, N° 8627, Sección Doctrina, 19/10/2015)

[191] Cfr. Art. 588 bis(c) de la LEC.

se encontraba, o no, amparado por la normativa procesal invocada para autorizar las medidas o para justificar el uso de la evidencia resultante en causas penales. Esta circunstancia fue aprovechada por las defensas de los imputados para realizar planteos dirigidos a invalidar el recurso a la información obtenida como prueba de cargo contra sus asistidos.

4.2. La discusión sobre el derecho a la privacidad ante los tribunales europeos y estadounidenses.

En Francia, las primeras medidas investigativas autorizadas por la justicia concernían al accionar de uno de los representantes de EncroChat, identificado como Eric Miguel, el cual había alquilado los servidores que utilizaba dicha firma a través de una compañía registrada en Vancouver (Canadá) llamada Virtue Imports. Estos servidores estaban alojados en el data center de una empresa francesa de "software como servicio" llamada OVH, en Roubaix[192] en el que posteriormente la Gendarmería francesa consiguió introducir el "implante técnico" con el que concretó el hackeo. Según se dio a conocer en uno de los fallos dictados en el Reino Unido, en total se libraron cinco órdenes judiciales los días 30 de enero, 12 de febrero, 4 de marzo, 20 de marzo y 31 de marzo de 2020[193], a través de las cuáles se autorizaron las distintas fases del hackeo a la red EncroChat.

De conformidad con la legislación francesa, la provisión del servicio de EncroChat, por sí sólo, podía ser considerada como un delito pasible de ser investigado, con independencia de la actividad criminal que eventualmente desarrollaran los clientes de la firma a través de los teléfonos móviles encriptados provistos por aquella. Ello, desde que el art. 30 de la Ley 2004-575 sobre "Economía Digital" califica como un delito la provisión, transferencia desde otro país miembro de la Comunidad Europea o importación de tecnología de encriptación sin previa autorización del poder ejecutivo francés, conducta castigada con hasta un año de prisión y multa de € 15.000[194].

Sin embargo, la medida de vigilancia implementada por la Gendarmería francesa no se limitó a las comunicaciones de Eric Miguel o a la legalidad de la introducción de los dispositivos EncroChat en Francia, sino que alcanzó, por intermedio de los servidores de la empresa, a la totalidad de los usuarios del sistema. A partir de ello, los defensores en Francia calificaron a la interceptación de los teléfonos de EnroChat como "masiva e indiscriminada", excediendo largamente al objeto de la investigación que motivó la autorización judicial inicial dictada por el magistrado en Lille[195]. Alegaron, al respecto, que se produjo una "captura masiva" de datos sin relación alguna con la supuesta actividad criminal de Miguel o con cualquier otra actividad delictiva[196]. Ello, por cuanto -a su modo de ver- no existió conocimiento o sospecha concreta de esa clase de actividad *con anterioridad* a que se autorizara la introducción del spyware estatal.

[192] Cfr. COLLERAN, Kevin: "French legal challenge over EncroChat…", cit.
[193] Ver fallo: *R(C) v. Director of Public Prosecutions*, cit., § 23.
[194] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12 (citas omitidas).
[195] Cfr. GOODWIN, Bill: "French Supreme Court raises constitutional questions…", cit.
[196] Cfr. COLLERAN, Kevin: "French legal challenge over EncroChat…", cit.

En sentido opuesto, las autoridades francesas afirmaron que *la tenencia de un teléfono de EncroChat, por sí sola, podía ser considerada como un indicio de actividad criminal*, debido a su alto precio[197]. En esa dirección, pusieron de resalto la preferencia que venían demostrando hacia el uso de dichos equipos los integrantes de las organizaciones criminales en Europa desde antes de que se iniciase la investigación, y aun admitiendo que una porción de los usuarios de la red podía no estar involucrada en conductas delictivas, estimaron que esa porción no excedía del 10% de los usuarios franceses[198].

A pesar de estos planteos, la legalidad de la actuación estatal en el caso EncroChat fue ratificada mediante una resolución dictada el 8 de abril de 2022 por el Consejo Constitucional (*Conseil Constitutionnel*) Francés[199], un cuerpo colegiado -creado por la Constitución de la V República del 4 de octubre de 1958- que si bien no actúa como tribunal jerárquicamente superior al Consejo de Estado ni al Tribunal de Casación, ostenta entre sus competencias el control de constitucionalidad de las leyes[200]. Aunque cabe aclarar que, en su resolución, el consejo no hizo referencia específica a las objeciones centradas en la indebida restricción del derecho a la intimidad.

Sin perjuicio de lo expuesto, vale señalar que en el primer fallo publicado de un tribunal europeo sobre alguno de los casos reseñados[201] se analizaron (bien que oblicuamente), planteos vinculados a la proporcionalidad de la medida de investigación dispuesta en Francia, aunque la cuestión central del fallo giró en torno a un tema distinto[202]. En efecto, en dicho caso, la defensa argumentó que, para ser válida, la EIO que amparó la obtención de la evidencia proveniente de EncroChat por las autoridades británicas debió tener por objeto un delito y una serie de sucesos previos y específicos, lo que no ocurrió en el caso, en el que -a juicio del recurrente- la orden no se libró para propiciar una investigación sino para hacerse con evidencia recolectada en Francia[203]. En esa dirección, destacó que al momento de emitirse la misma, en los tribunales de Liverpool no existía ninguna prueba que vinculase a su asistido con ningún delito[204], y que, mediante la mencionada orden, las autoridades británicas habían llevado a cabo una "operación de pesca"[205].

La moción de la defensa fue rechazada. En sustento de su decisión, el tribunal señaló que la normativa que regula la emisión de las EIO no prohíbe que sea emitida en

---

[197] Cfr. SYMONDS, Tom: "Encrochat: Secret network messages can be used in court, judges rule", cit. (énfasis añadido).

[198] Ver: Motherboard: "EncroChat lawyers say clients haven't had fair trials", publicado el 18/2/2022, obtenido en: https://nationalcybersecuritynews.today/encrochat-lawyers-say-clients-havent-had-fair-trials-emailsecurity-phishing-ransomware/.

[199] Conseil Constitutionnel, Décision n° 2022-987 QPC.

[200] Ver, al respecto: https://www.conseil-constitutionnel.fr/es/presentacion-general.

[201] *R(C) v. Director of Public Prosecutions*, cit.

[202] Puntualmente, si el hackeo concretado por las autoridades francesas había tenido por objeto a datos que formaban parte de una "comunicación" o a datos "almacenados", dado que -conforme la normativa vigente en el Reino Unido sobre la materia, en el primer supuesto la información obtenida no hubiese podido ser utilizada en causas criminales, pero si la que es producto del segundo supuesto (al respecto, ver la reseña sobre la normativa británica aplicable efectuada *supra*, § 3.2.

[203] *R(C) v. Director of Public Prosecutions*, cit., § 30.

[204] *R(C) v. Director of Public Prosecutions*, cit., § 31.

[205] *R(C) v. Director of Public Prosecutions*, cit., § 58.

el supuesto de que exista una sospecha razonable sobre la comisión de un delito, pero se desconozcan, al momento de dictarse la orden, las circunstancias particulares de la conducta objeto de la misma y el concreto encuadramiento jurídico que corresponde asignarles[206]. Explicó que las EIO tienen por objeto tanto la investigación de delitos que ya se cometieron como de los que se sospecha que pudieron haberse cometido (o no), y/o cuando no se ha identificado o pueda identificarse a un sospechoso, siendo precisamente ese el propósito de la investigación: establecer si se cometió o se está cometiendo un delito y quién o quiénes lo estarían cometiendo[207]. Este último habría sido, en opinión del tribunal, el supuesto verificado con respecto a la orden librada para obtener la evidencia proveniente de la operación contra EncroChat.

Por añadidura, el tribunal refirió que el pedido inicial de información emitido por las autoridades británicas a tal efecto contenía, de hecho, una lista de 16 personas presuntamente ligadas a la criminalidad organizada y sospechadas de participar en la distribución de teléfonos EncroChat en el Reino Unido. Aclaró, sin embargo, que de la lectura del documento se desprendía que el objeto de la solicitud británica era asistir en la investigación sobre los delitos que podrían estar cometiéndose con la ayuda de los equipos encriptados, y no contra las personas involucradas en su distribución. Con relación a ello, compartió la opinión de las autoridades francesas en punto a que la tenencia de teléfonos EncroChat otorgaba un razonable sustento a la sospecha sobre la posible comisión de ilícitos, por entender que los mencionados equipos eran "desarrollados y específicamente comercializados para servir a la comunidad criminal, facilitando la actividad delictiva", conforme la experiencia recogida por las agencias de orden público[208]. Pero fue todavía más lejos, afirmando que existía un "consenso interno e internacional" en punto a que los teléfonos EncroChat eran utilizados "exclusivamente" por criminales, dado que ofrecían un medio seguro para que las organizaciones criminales se comuniquen en relación con su accionar delictivo[209].

Las dudas sobre si la investigación iniciada en Francia (y que dio sustento a la autorización judicial para llevar a cabo la interceptación de las comunicaciones) tenía por objeto a los operadores del sistema EncroChat o a sus usuarios también generó polémicas en los Países Bajos. Allí, en respuesta a planteos cuestionando la legalidad de la referida interceptación (y la admisibilidad de la información resultante), el Ministerio Público Fiscal argumentó que la medida de vigilancia había estado dirigida "principalmente" contra los operadores de la red. En sentido opuesto, los abogados defensores señalaron que del contenido de los documentos publicados por los tribunales británicos podía inferirse que *el objetivo de la operación de hackeo habían sido los usuarios*. Sin embargo, en julio de 2021 un tribunal en la ciudad de Den Bosch resolvió que lo consignado en dichos documentos no era en principio incompatible con el argumento de la fiscalía en punto a que la investigación se había dirigido *contra los operadores* de EncroChat[210].

[206] *R(C) v. Director of Public Prosecutions*, cit., § 33.
[207] *R(C) v. Director of Public Prosecutions*, cit., §§ 53/56.
[208] *R(C) v. Director of Public Prosecutions*, cit., § 16.
[209] *R(C) v. Director of Public Prosecutions*, cit., § 3.
[210] Cfr. GOODWIN, Bill: "Dutch prosecutor ordered to give evidence on EncroChat hack", en Computer Weekly, publicado el 13/7/2021, obtenido en:

En Alemania, se produjo una fecunda discusión jurisprudencial sobre la legitimidad del uso contra ciudadanos de ese país de la evidencia obtenida a partir del hackeo de la Gendarmería francesa a EncroChat y su transferencia a las autoridades alemanas. Las primeras decisiones sobre la cuestión fueron dictadas por los tribunales regionales de alzada de Bremen y Hamburgo en el marco de audiencias sobre detención preventiva de personas cuya actividad criminal había quedado al descubierto como resultado de la interceptación de los mensajes enviados a través de EncroChat. Ambos tribunales confirmaron (en diciembre de 2020 y enero de 2021, respectivamente) la validez de la evidencia obtenida en Francia para dar sustento a las medidas cautelares contra los sospechosos[211].

En sentido opuesto se expidió un magistrado del Distrito de Berlín, que consideró que el monitoreo de 30.000 usuarios de EncroChat era incompatible con una interpretación estricta del principio de proporcionalidad, y -por consiguiente- ilegal[212]. En esa dirección -y en línea con los argumentos esgrimidos por la defensa en el caso decidido ante los tribunales británicos, el juez destacó que en el momento en que se libró la EIO mediante la cual las autoridades alemanas obtuvieron la evidencia recolectada en Francia, no existía ninguna sospecha contra los usuarios de los equipos de EncroChat, que pudiese haber justificado la vigilancia de sus comunicaciones. Explicó que, aunque los criminales suelen preferir los canales de comunicación difíciles de monitorear, el mero uso de un teléfono móvil encriptado -incluso uno con un alto nivel de seguridad- no constituía en sí mismo un motivo para sospechar la comisión de un delito[213]. Afirmó, a su vez, que el descubrimiento posterior de conducta criminal a través del monitoreo de las comunicaciones no justificaba retroactivamente la interceptación. En efecto, entendió que ni siquiera las enormes cantidades de drogas secuestradas ni el "espectacular hallazgo" de una cámara de torturas en los Países Bajos podían utilizarse '*ex post*' para compensar la ausencia de elementos que abonaran, '*ex ante*' la presunción de que la red era predominantemente usada por criminales[214].

Sin embargo, el pronunciamiento del magistrado berlinés fue posteriormente revocado por el Tribunal de Apelaciones de Berlín[215]. En contra de lo afirmado por el juez de primera instancia, la alzada consideró que el modo en que se comercializaban los teléfonos EncroChat, su alto costo, el secuestro previo de esta clase de equipos en

https://www.computerweekly.com/news/252503908/Dutch-prosecutor-ordered-to-give-evidence-on-EncroChat-hack (énfasis añadido).

[211] Cfr. WAHL, Thomas: "Dismantled encryption networks…", cit.

[212] GOODWIN, Bill: "Berlin court finds EncroChat intercept evidence cannot be used in criminal trials", en Computer Weekly, publicado el 3/7/2021, obtenido en: https://www.computerweekly.com/news/252503524/Berlin-court-finds-EncroChat-intercept-evidence-cannot-be-used-in-criminal-trials.

[213] GOODWIN, Bill: "Berlin court finds EncroChat intercept evidence cannot be used in criminal trials", cit..

[214] GOODWIN, Bill: "Berlin court finds EncroChat intercept evidence cannot be used in criminal trials", cit. Con relación a ello, el juez destacó que el sistema EncroChat también podía resultar atractivo o útil para periodistas, activistas políticos que temieran la persecución estatal o empleados de compañías que manejasen material confidencial, sin que pudiese afirmarse válidamente que el elevado precio de los equipos sólo podía pagarse con el producto de la actividad criminal. Consideró que no existía evidencia concreta de que los 60.000 usuarios de EncroChat formaran parte de una "red criminal".

[215] Ver: Fuentitech.com: "Berlin court overturned ban on EncroChat evidence in criminal trials", cit. Esta decisión del BGH motivó, a su vez, la consulta del Tribunal Regional de Berlín al TJUE reseñada *supra*, § 3.3.

siete investigaciones previas en Francia (incluyendo a cinco vinculadas al narcotráfico), los elementos "anti forenses" de los dispositivos promocionados en la página de la firma y la ausencia de una sede social "oficial" o de empleados registrados, constituían elementos de juicio que daban sustento a la sospecha razonable de actividad criminal y justificaban la interceptación ordenada por el magistrado francés[216]. El tribunal destacó, asimismo, que al momento de decidir sobre la admisibilidad de la evidencia, era menester tener presente -además de los significativos riesgos para la salud pública- la amenaza que representa una estructura criminal promovida y financiada mediante el tráfico ilícito de drogas. Aseveró, por añadidura, que no usar la evidencia recolectada en Francia *violentaría "el sentido de justicia de los ciudadanos alemanes"*[217].

Sin perjuicio de lo expuesto, lo cierto es que la cuestión sobre la legitimidad del empleo, en procesos criminales sustanciados en Alemania, de los mensajes obtenidos a partir del hackeo de EncroChat (como así también, presumiblemente, los de Sky ECC y An0m) parece haber quedado zanjada como resultado de la decisión adoptada en marzo de 2021 por el Tribunal Federal de Justicia de Alemania (BGH)[218], que se expidió sobre la materia al revisar una condena a cinco años de prisión por narcotráfico dictada por el Tribunal de Alzada de Hamburgo, en cuyo marco la defensa había objetado la admisibilidad de la principal prueba de cargo en contra de su asistido, conformada por los mensajes que había intercambiado mediante la red EncroChat[219].

En lo tocante a los agravios vinculados al derecho a la intimidad y el secreto de las telecomunicaciones (amparado en el art. 10 de la Constitución de Alemania), el BGH entendió que debía darse preeminencia, en el análisis, al principio de proporcionalidad. A tal efecto, tomó en consideración lo establecido en la normativa procesal alemana en cuanto habilita el uso de datos personales "para otros fines" si la medida a través de la cual fueron recolectados podría haber sido dispuesta bajo las condiciones aplicables a las medidas de investigación más intrusivas (puntualmente, el registro online o la vigilancia acústica del domicilio), es decir en relación con delitos graves como el narcotráfico[220].

A partir de ello, el tribunal alemán concluyó que no se habían conculcado los derechos humanos, ni la ley Europea ni los requisitos fundamentales del debido proceso, que podrían derivar en una prohibición de uso de la evidencia. Al respecto, el BGH entendió que, de conformidad con la información disponible para las autoridades francesas al momento del primer acceso a los datos, la investigación no se había orientado a la vigilancia masiva de miles de usuarios sin sospecha previa, sino que se

---

[216] Ver: Fuentitech.com: "Berlin court overturned ban on EncroChat evidence…", cit.

[217] Ver: Fuentitech.com: "Berlin court overturned ban on EncroChat evidence…", cit. (énfasis añadido).

[218] BGH, decisión 5 StR 457/21, del 2/3/2021. Una reseña más detallada de este fallo puede encontrarse en: SALT, Marcos G.: "'Hacking legal' como medio de investigación en el proceso penal: Breves reflexiones sobre los desafíos jurídicos derivados de su aplicación trasnacional", en AAVV, *La investigación penal en el entorno digital. Estudios sobre el impacto de las nuevas tecnologías digitales en el proceso penal*, Hammurabi, Buenos Aires, 2023, págs. 282/285.

[219] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence in EncroChat cases", en Eucrim, publicado el 19/5/2022, obtenido en: https://eucrim.eu/news/Alemania-federal-court-of-justice-confirms-use-of-evidence-in-encrochat-cases/§:~:text=After%20several%20Higher%20Regional%20Courts,first%20supreme%20court%20judgment%20in.

[220] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence…", cit..

centró en una red diseñada desde un principio para facilitar la actividad criminal, y que operaba en secreto[221].

En este escenario, la hipótesis de las autoridades francesas encontró sustento, en opinión del BGH, en hallazgos iniciales que evidenciaban un uso criminal casi exclusivo de los teléfonos EncroChat, a partir de los cuáles podía sospecharse fundadamente el vínculo de los usuarios con la criminalidad organizada por el solo hecho de haber adquirido uno de estos equipos, que no estaban disponibles en los canales de distribución normales y tenían un costo considerable[222]. Destacó que conforme los primeros resultados del análisis de la evidencia de EncroChat, el 63,7% de los teléfonos móviles de la firma activos en Francia estaban siendo usados para fines criminales, siendo que los restantes equipos (36,3%) estaban o bien parcialmente inactivos, o no habían sido evaluados aun, lo que llevó a las autoridades de ese país a aseverar que la clientela de EncroChat era casi exclusivamente criminal[223].

En España, la controversia sobre la proporcionalidad de la medida ordenada en Francia se suscitó en el marco de una investigación (originalmente por blanqueo de capitales), que se profundizó a partir de la recepción, en la Fiscalía Antidroga española, de información obtenida mediante el hackeo de EncroChat (proveniente de la policía sueca) que daba cuenta de la intervención de los sospechosos en operaciones de narcotráfico. En dicho marco, la defensa de los imputados adujo que con la intervención de EncroChat se habían vulnerado derechos fundamentales, por lo que pidieron que se apartara por completo esta prueba. Este planteo fue rechazado por el juez interviniente, que entendió que la medida no había sido desproporcionada ni indiscriminada (como alegaban las defensas), toda vez que tuvo lugar en el marco de una causa judicial en trámite desde 2017, en la que se constató que el uso del sistema era delictivo. Esto último quedó demostrado, según el juez, por el hecho de que fue la propia empresa responsable del servicio la que conminó a los usuarios a deshacerse de sus terminales[224]. El fallo (dictado en noviembre de 2021) fue confirmado en enero de 2022 por la Sala en lo Penal de la Audiencia Nacional, que hizo propios los fundamentos del magistrado de primera instancia[225].

En lo tocante al caso Sky ECC, si bien todavía no se han publicado fallos, la discusión parece discurrir en términos similares a los de EncroChat. Así, por ejemplo, y en relación con la existencia de una sospecha razonable previa que justificase la interceptación de los mensajes de los usuarios del sistema, un fiscal en Francia afirmó que también en lo tocante a esta red, el uso parecía estar casi exclusivamente restringido a criminales de gran escala[226]. En sentido opuesto, los titulares de la compañía Sky Global (responsables del sistema Sky ECC) argumentaron -en el marco de una demanda legal contra el gobierno de EE.UU. en la que reclamó la devolución de los

[221] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence…", cit..
[222] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence…", cit..
[223] Cfr. WAHL, Thomas: "Federal Court of Justice confirms use of evidence…", cit.
[224] Cfr. DORTA, Irene: "La Audiencia Nacional avala a un juez francés…", cit.
[225] Cfr. GABILONDO, Pablo: "El WhatsApp secreto que usaban los narcos…", cit.
[226] Ver: The Guardian: "Police raids across Europe after encrypted phone network shut down", publicado el 10/3/2021, obtenido en: https://www.theguardian.com/technology/2021/mar/10/police-raids-across-europe-after-encrypted-phone-network-shut-down.

más de 100 dominios de Internet decomisados por las autoridades de ese país[227]- que la circunstancia de que sólo 6.000 de los casi 120.000 usuarios del sistema hayan migrado a An0m permitía inferir que el componente delictivo dentro de la red era comparativamente pequeño. En esa dirección, en la moción presentada por la empresa se afirmó que "*…el hecho de que una tecnología pueda ser utilizada con fines ilegítimos no implica que la propia tecnología haya sido diseñada con ese fin*"[228].

De ese modo, Sky Global buscó distanciarse de otros servicios similares como EncroChat o Phantom Secure. Aseveró, en tal sentido, que ni su CEO (Jean-Francois Eap, procesado en EE.UU., acusado de proveerle equipos encriptados a narcotraficantes en forma deliberada) ni sus directivos tenían conocimiento del uso ilícito que se les daba a los teléfonos móviles encriptados comercializados por la empresa, ni tampoco hicieron nada para facilitar la actividad criminal dentro de la plataforma Sky ECC. En orden a ello, argumentó que cualquier instancia de "borrado remoto" del contenido de los dispositivos debió haber sido facilitada por integrantes de su red de distribución tercerizada, en la que los distribuidores contrataban a sus propios agentes o revendedores[229].

De igual manera, la discusión en relación con Sky ECC también reprodujo la que se dio en torno a EncroChat, en punto a cuál fue el objetivo de la operación gubernamental. Al respecto, los investigadores belgas (que cumplieron un rol fundamental en la concreción de la misma) señalaron que su propósito principal fue impedir que el sistema Sky ECC siguiese funcionando, desmantelar su infraestructura y decomisar las ganancias ilícitas de los revendedores de la empresa[230]. Sin perjuicio de lo cual, se aprecia que, aunque ese propósito se cumplió, la interceptación propiamente dicha se dirigió, en realidad, a las comunicaciones *de los usuarios del sistema*, antes que a las de los operadores del mismo. Por otro lado, en la ya mencionada moción contra el gobierno estadounidense, Sky Global denunció que la verdadera finalidad del ataque contra el sistema Sky ECC no había sido la de poner fin a la actividad delictiva concretada por intermedio del mismo, sino empujar a los usuarios a volcarse al sistema An0m, secretamente manejado por el FBI[231].

Con respecto a An0m, un tribunal en Alemania consideró admisible la evidencia recolectada por el FBI a partir de la interceptación de los mensajes intercambiados a través de la plataforma An0m (diseñada, operada y comercializada por dicha agencia y la Policía Federal Australiana) y compartida con las autoridades europeas por medio de EUROPOL. En Finlandia, en cambio, un tribunal resolvió en noviembre de 2021 que la mencionada evidencia no podía ser utilizada contra dos ciudadanos finlandeses acusados de blanqueo de capitales, en relación con la transferencia (finalmente no concreta) de € 10.000 a un narcotraficante español. En línea con la postura de las defensas, el tribunal de distrito entendió que la información proveniente de An0m había sido obtenida ilegalmente, toda vez que -conforme la ley finlandesa- la recolección de pruebas a través de medidas restrictivas de derechos de carácter secreto sólo es legítima con respecto a delitos con un máximo de pena superior a los tres años de prisión,

[227] Cfr. WOLFF, Josephine: "One of the most unusual cybersecurity stories…". cit.
[228] Cfr. MARKS, Joseph: "Encrypted messaging apps…", cit.
[229] Cfr. WOLFF, Josephine: "One of the most unusual cybersecurity stories…". cit.
[230] Ver: GOODWIN, Bill: "Police cracks world's largest cryptophone network…", cit.
[231] Cfr. MARKS, Joseph: "Encrypted messaging apps…", cit.

requisito que no se cumple en lo tocante al blanqueo de capitales, que tiene prevista una pena máxima de dos años de prisión en Finlandia[232].

4.3. Análisis preliminar sobre la proporcionalidad de la injerencia sobre el derecho a la intimidad.

A mi modo de ver, para arribar a una conclusión, aunque sea preliminar, acerca de si la actuación de las autoridades estatales en los distintos casos reseñados configuró, o no, una restricción legítima al derecho a la intimidad de los ciudadanos afectados por las medidas de vigilancia implementadas por las agencias de orden público, se deben analizar las distintas hipótesis que parecen coexistir (al menos) en lo tocante a las operaciones contra EncroChat y Sky ECC. Al respecto, cabe señalar que aunque se desconoce si el objetivo principal de la actuación estatal en la operación referida a Sky ECC estuvo dirigida contra el accionar de los responsables de los mencionados sistemas de mensajería encriptada o el de los usuarios (cuyas comunicaciones fueron, en última instancia, las alcanzadas por la interceptación), si se sabe, en relación con EncroChat, que la solicitud inicial de la fiscalía francesa (del 29/1/2020), indicaba que el objetivo de la medida de vigilancia original era "identificar a los usuarios", "revelar sus actividades delictivas" y "detenerlos". Recién a partir del mes de abril de ese mismo año se comenzó a investigar en forma directa la actividad delictiva cometida por los usuarios[233].

En lo que respecta al primer objetivo (esto es: a la investigación dirigida prioritariamente contra los sistemas EncroChat o Sky ECC), cabe recordar que según señalaron EUROJUST y EUROPOL[234], las actuaciones iniciadas en Francia con relación al primer sistema se referían a la presunta infracción a lo establecido en el art. 30.III de la Ley 2004-575 sobre "Confianza en la economía digital", en cuanto demanda autorización previa del Primer Ministro para la provisión, transferencia desde un Estado Miembro de la Comunidad Europea o importación de métodos de criptografía no destinados "*…exclusivamente a aportar funciones de autenticación o control de integridad*" (sancionada con pena de un año de prisión y multa en el art. 35.I.1 de la misma ley).

Más allá de las dudas sobre si la investigación de un delito castigado con penas de dos años de prisión, imputado a una entidad concreta, puede llegar a justificar la aprehensión de un material incriminatorio tan importante, que afecta a más de 60.000 personas, muchas de las cuáles no eran objeto de investigación hasta ese momento[235], el fundamento de la medida dispuesta en Francia resulta problemática ya desde el punto de vista legal, toda vez que los arts. 706-102-1 y 706-102-2 del CPC francés (que regulan el uso de govware) sólo autorizan el recurso a una medida de esta clase con relación a los delitos enumerados en los arts. 706-73 y 706-73-1 del mismo código, enumeración en la que *no está incluida la infracción prevista en el art. 35.I.1 de la ya mencionada Ley 2004-575*. Y si bien los artículos mencionados aluden a varias formas de actuación bajo

[232] Cfr. COX, Joseph: "Court throws out messages obtained by FBI honeypot phone company An0m", en Motherboard. Tech by VICE, publicado el 30/11/2021, obtenido en: https://www.vice.com/en/article/pkppqk/court-throws-out-messages-from-An0m-Finlandia-España.
[233] Cfr. IBÁÑEZ LÓPEZ-POZAS, Fernando L.: "De las masivas interceptaciones de datos…", cit., pág. 13.
[234] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12 (citas omitidas).
[235] Cfr. ZARAGOZA TEJADA, Javier Ignacio: "Operaciones encubiertas digitales y convencionales…", cit., pág. 216.

la modalidad de organización criminal, que justifican el uso de programas espías estatales, ninguna de ellas lo es en orden a la introducción o distribución ilícita de tecnología de encriptación.

En este escenario, un supuesto hipotético en el que podría sostenerse la legitimidad de la interceptación dispuesta radica en que, al momento de dictarse las autorizaciones judiciales que ampararon la infiltración del sistema EncroChat, el objeto de la investigación hubiese sido la distribución no autorizada de dispositivos encriptados *a los efectos de facilitar otras conductas ilegales*, probablemente vinculadas a la criminalidad organizada. Ello guardaría coherencia con la correlación temporal, ya apuntada, entre los reiterados secuestros, por parte de las fuerzas de seguridad francesas, de teléfonos encriptados de dicha empresa en manos de personas sospechadas de pertenecer a organizaciones criminales y el inicio de la pesquisa sobre EncroChat.

Sin embargo, incluso en la hipótesis planteada en el párrafo precedente, surge el interrogante sobre si resulta proporcional disponer, en el marco de una investigación *contra los responsables de una compañía* que distribuye teléfonos encriptados a sabiendas de que facilita el crimen organizado, *disponer la vigilancia de las comunicaciones de todos los clientes* de la mencionada empresa. Al respecto, podría ser relevante que -de conformidad con lo establecido en el art. 132-79 del Código Penal francés-, el uso de encriptación para facilitar la comisión de un delito es considerado un agravante la conducta ilícita en cuestión, y justifica el recurso a medios técnicos para obtener la evidencia en formato plaintext a partir de lo dispuesto en los arts. 230-2 y 706-102-1 del CPC[236], aunque no está para nada claro que dicha circunstancia, por si sola, resulte apta para justificar semejante ampliación del objetivo inicial de la vigilancia.

A todo evento, entiendo que para considerar legítima la extensión de la medida de vigilancia original (presuntamente dirigida a los responsables de las empresas EncroChat y Sky Global) a la totalidad de los usuarios de los sistemas manejados por dichas firmas, sería preciso fundamentar una sospecha razonable sobre la existencia de un *vínculo entre el servicio prestado por las compañías de mención y la actividad ilícita desarrollada por los usuarios*, de entidad suficiente como para considerar que existió una "empresa criminal conjunta" o, cuanto menos, una participación de los primeros en los ilícitos cometidos por los segundos.

Esta última es la hipótesis sostenida por las autoridades de los EE.UU. en la acusación dirigida contra el CEO y uno de los distribuidores de Sky Global, en cuyo marco afirman que la compañía facilitó deliberadamente la actividad criminal a partir de los servicios ofrecidos, que no sólo incluían el intercambio de mensajes encriptados presuntamente imposibles de monitorear, sino también -y especialmente- la posibilidad de eliminar remotamente la información contenida en los teléfonos si eran secuestrados por las fuerzas de seguridad. Al respecto, la postura de Sky Global es que cualquier plataforma de mensajería encriptada (incluyendo las de compañías importantes como Apple, Facebook -dueña de WhatApp- o Telegram) puede ser explotada para fines ilícitos. Si bien esto es cierto, la realidad es que ninguna de esas firmas ofrece como servicio el borrado remoto y deliberado de los datos en teléfonos que están en manos

[236] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12.

de la policía, ni tampoco permite que sus distribuidores lo hagan, por lo que el intento de la empresa de equiparar su situación con la de aquellas pierde sustento[237].

En sentido opuesto, si la finalidad última de los ataques informáticos a EncroChat y Sky ECC hubiese sido -como afirmaron los representantes legales de Sky Global en su presentación ante los tribunales estadounidenses- la de empujar a los usuarios de dichos servicios a enrolarse en el de An0m, para permitir que fuesen monitoreados por el FBI[238], el respeto de estas medidas al principio de proporcionalidad estricta sería difícil de sostener. Al respecto, vale señalar que, aunque las autoridades belgas reconocieron que uno de los propósitos de la operación contra Sky ECC era impedir que el sistema siguiese funcionando, no hay ninguna prueba que vincule a dicha operación -o la de EncroChat que la antecedió- con la desarrollada por el FBI y la PFA a través del sistema An0m, de la que no habrían tenido conocimiento al momento de actuar.

Otra posibilidad reside en considerar que el objetivo de las medidas de interceptación concretadas respecto de los usuarios de EncroChat y Sky ECC fue, desde el principio, vigilar *a los usuarios* de los mencionados sistemas (en el caso de An0m, no cabe duda de ello, toda vez que los responsables de la plataforma de mensajería encriptada eran los propios investigadores). En este supuesto, el análisis sobre la proporcionalidad de la injerencia sobre el derecho a la privacidad o el secreto a las comunicaciones es similar al de la hipótesis anterior, en cuanto se centra en la determinación de si la interceptación estuvo, o no, fundada en elementos de juicio que permitiesen, al momento de dictarse la autorización, inferir razonablemente que los destinatarios de la misma estaba involucrados en la comisión de delitos graves y si su concreción en forma masiva era, o no, el único medio de lograr los fines propuestos.

En cuanto al primer interrogante, cabe de inicio advertir que es evidente que ni las autoridades francesas ni las de ninguno de los restantes países que se beneficiaron con la evidencia obtenida del ataque informático a EncroChat tenía información sobre la posible comisión de delitos (o, de hecho, siquiera una investigación en trámite) con respecto a la mayoría de los usuarios del sistema, como para satisfacer la exigencia contenida en gran parte de los códigos procesales de esas naciones en punto a que la injerencia sobre el derecho a las comunicaciones se verifique en el marco de una causa penal y esté fundada en la sospecha de que una o varias personas concretas hayan cometido, estén cometiendo o tengan en su poder evidencia sobre la comisión de un hecho ilícito. Y la misma situación se verifica en relación con el ataque sobre el sistema Sky ECC. En este escenario, la interceptación de las comunicaciones de todos esos usuarios (más de cien mil, sumando ambas operaciones) se justificó argumentando que la mera tenencia y uso de un teléfono encriptado de alguna de esas dos compañías, por si sola, daba sustento a una sospecha razonable sobre la posible intervención en actividades delictivas.

La cuestión es, entonces, si dicha afirmación es, o no, razonable a su vez. Si bien no se han dado a conocer los fundamentos de las órdenes judiciales libradas para autorizar los hackeos de EncroChat y Sky ECC, las autoridades policiales y judiciales de los países involucrados han manifestado públicamente que, a su entender, la mayor parte de los usuarios -sino todos- de ambos sistemas estaban involucrados en conductas

[237] Cfr. WOLFF, Josephine: "One of the most unusual cybersecurity stories…". cit.
[238] Cfr. WOLFF, Josephine: "One of the most unusual cybersecurity stories…". cit.

ilícitas. Así, por ejemplo, la NCA británica aseguró que "todos" los usuarios eran criminales, mientras que -con mayor prudencia- las autoridades francesas y EUROPOL aludieron a un "alto porcentaje" de delincuentes entre los tenedores de equipos de EncroChat o Sky ECC[239].

Desde otros sectores se cuestionó dicha aseveración. En esa dirección, se invocó, por ejemplo, una comunicación de la Comisión Europea de abril de 2021 de la que se desprende que un año después de culminada la interceptación sobre EncroChat, "sólo" se habían iniciado 1.500 investigaciones y producido 1.800 arrestos, lo que equivalía apenas al 5,4% de los usuarios del mencionado sistema. Se apuntó también que, en lo tocante a los usuarios franceses, la proporción comprobada de actividad criminal era del 67,3% (317 de los 417 usuarios al mes de junio de 2020), cifra que consideraron exigua en comparación con los 60.000 usuarios que fueron objeto de vigilancia[240].

Más allá de que estos porcentajes relativamente bajos de sospechosos comprobados bien podrían explicarse aludiendo a la escasez de medios humanos y técnicos suficientes como para investigar en simultáneo a tantos miles de usuarios -y la consecuente conveniencia de enfocarse en perseguir a los sospechosos involucrados en los delitos más graves, o de desmantelar a las organizaciones criminales más poderosas-, entiendo que la discusión sobre cuál es el porcentaje final de criminales dentro del universo de los usuarios de EncroChat o Sky ECC *al cabo de la investigación* es, en última instancia, irrelevante, toda vez que se trata de un análisis '*ex post*' que no puede incidir en el juicio sobre si la autorización para proceder a la interceptación de dichos sistemas tuvo, o no, fundamento suficiente. Lo (único) que realmente importa, en tal sentido, es la evaluación efectuada '*ex ante*' por los magistrados autorizantes a partir de los elementos de juicio de que disponían *en ese momento*.

Lo cual supone un retorno al interrogante central. Esto es: si la mera tenencia y uso de un teléfono encriptado de EncroChat o Sky ECC constituía un motivo válido para sospechar que su titular estaba involucrado en una actividad ilícita. Los que se inclinan por la negativa señalan -como lo hizo un tribunal alemán, y como argumentó la propia empresa Sky Global- que la circunstancia de tener un elemento que puede ser utilizado para delinquir no autoriza, por si sola, a sospechar que se está cometiendo un delito. En esa dirección, se apunta que, de alguna manera, las funcionalidades incorporadas por EncroChat y Sky ECC en sus equipos constituyen una manifestación (quizás extrema) del principio de "Protección de datos por diseño" ("Data Protection by Design" o DPbD), que es a la vez una de las bases de la política de protección de datos propiciada en el art. 25 del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés)[241] de la Unión Europea. En esa dirección, Ibáñez López-Pozas destaca que, a su entender, en la legislación española no sería posible acordar esta medida por el mero uso de un teléfono móvil encriptado: sólo porque el servicio EncroChat, es más seguro que otros servicios que también están cifrados de extremo a extremo, como WhatsApp o Facebook Messenger, no puede convertirse en el punto de partida de medidas coercitivas de Derecho Penal. Tampoco puede justificarse la injerencia masiva por los precios de los

[239] Ver: EUROPOL: "Dismantling of an encryted network…", cit.).
[240] GOODWIN, Bill: "Berlin court finds EncroChat intercept evidence cannot be used in criminal trials", cit.
[241] Sobre el mencionado reglamento, ver: https://gdpr-info.eu/.

teléfonos, pues no difieren significativamente de los precios de los teléfonos móviles estándar de gama alta, que también pueden superar ampliamente los 1.000 euros[242].

En ese orden de ideas, se argumentó también que teléfonos como los de EncroChat o Sky ECC podrían resultar atractivos para usuarios preocupados por su privacidad, teniendo en cuenta -por ejemplo- las revelaciones de Edward Snowden sobre los sistemas de vigilancia masiva implementados por las agencias de espionaje de EE.UU. e Inglaterra[243], la circunstancia de que estas compañías surgieron en las postrimerías del escándalo de hackeo por parte de los tabloides ingleses[244]; o, más recientemente, el descubrimiento de que el sofisticado spyware "Pegasus", de la empresa de seguridad informática israelí NSO, estaba siendo utilizado por gobiernos de todo el mundo para interceptar -sin autorización judicial- las comunicaciones de políticos, periodistas y activistas[245]. Según esta hipótesis, en semejante escenario, contar con una plataforma de comunicación (supuestamente) inexpugnable podría razonablemente resultar de interés para políticos, celebridades, miembros de la realeza o empresarios preocupados por sostener la confidencialidad de sus asuntos[246].

Estos argumentos son, desde algún punto de vista, atendibles. Entiendo, sin embargo, que no resultan del todo convincentes para controvertir la hipótesis de las agencias de orden público en estos casos, que es que, si una persona tenía y utilizaba un teléfono de EncroChat o Sky ECC, *lo más probable* es que estuviese involucrada en una actividad ilícita (dado que, vale recordarlo, para justificar una medida de investigación como lo es la interceptación de las comunicaciones, no puede requerirse el grado de certeza que sólo puede adquirirse a partir de la evidencia que resulte de aquella y otras medidas). Por ende, el hecho de que los servicios de estas compañías *también* pudiesen haber sido aprovechados por celebridades, políticos, periodistas o empresarios preocupados por su privacidad *no le quita sustento a la sospecha que justificó la intervención* de las comunicaciones.

Al respecto, tengo para mí que el elemento de juicio clave para el análisis sobre la razonabilidad de la sospecha acerca de los usuarios de EncroChat y Sky ECC es la experiencia general respecto al modo en que *la generalidad de la población emplea sus teléfonos* en las sociedades modernas. Este elemento le otorga un contexto y sentido al análisis que, a mi modo de ver, estuvo ausente -por ejemplo- en la comparación que efectuó el magistrado alemán con el supuesto de la tenencia de herramientas de trabajo que también pueden ser utilizadas para robar[247]. De acuerdo con ello, lo decisivo no es

[242] Cfr. IBÁÑEZ LÓPEZ-POZAS, Fernando L.: "De las masivas interceptaciones de datos…", cit., pág. 13.
[243] Al respecto, ver *supra*, § 1.
[244] El caso se refiere al descubrimiento de que el tabloide ingles News of the World, propiedad del magnate de los medios Rupert Murdoch, había contratado los servicios de hackers para espiar comunicaciones privadas de famosos, miembros de la realeza y víctimas de delitos para obtener primicias. Una reseña de los principales eventos vinculados a este escándalo puede encontrarse en: https://edition.cnn.com/2013/10/24/world/europe/uk-phone-hacking-scandal-fast-facts/index.html.
[245] Con relación a esta cuestión, ver, en especial, los casos referenciados por el diario británico The Guardian en el marco del "Pegasus Project" (https://www.theguardian.com/news/series/pegasus-project).
[246] Ver: PARKIN, Simon: "'Every message was copied to the police'…", cit.
[247] Vale señalar, con relación a ello, que no es lo mismo evaluar si es sospechosa, o no (a los efectos de autorizar un allanamiento o un registro), la mera tenencia de barretas o cortadores de alambre *en abstracto*, que analizar si es sospechosa, o no, dicha tenencia en un contexto en que el tenedor no tenía

tanto -o no únicamente- el alto precio de los teléfonos y los servicios de EncroChat y Sky ECC a los que se aludió en la mayoría de los fallos que legitimaron el uso de la evidencia resultante de los hackeos, sino que ese precio *se pagase por un teléfono que sólo servía para intercambiar mensajes*, pero con el que *no se podía hacer ninguna otra de las actividades que el común de la gente hace con los modernos smartphones*: ni efectuar llamados, ni navegar por Internet, ni acceder a las redes sociales, ni sacar fotografías. Es esta última circunstancia la que -como bien señaló el Departamento de Justicia de los EE.UU., torna improbable que estos teléfonos fueran utilizados por ciudadanos comunes, incluso los más preocupados por su privacidad[248].

Cabe tener presente, asimismo, que -precisamente a partir de las revelaciones de Snowden-, las principales compañías tecnológicas han dotado a los equipos y aplicaciones de uso general de la población de funcionalidades dirigidas a resguardar la privacidad de los usuarios. Entre estas, la encriptación "punto a punto" de las comunicaciones de un modo que impide su desencriptación incluso a la propia empresa proveedora del servicio, así como el cifrado del disco completo de los smartphones de las dos empresas que cuentan con el mayor volumen del mercado (Apple y Google), circunstancia que hasta ha generado conflictos entre estas firmas y las agencias de orden público, por la imposibilidad de estas últimas de acceder a la evidencia contenida en los dispositivos[249]. En tal contexto, no puede menos que concluirse que sólo un porcentaje mínimo de los ciudadanos comunes puede llegar a estar lo suficientemente preocupado por su privacidad como para pagar un precio tan elevado para usar un teléfono que carece de la mayor parte de las funciones que han convertido a los smartphones en un elemento (casi) irrenunciable para la vida en la sociedad[250], sobre todo teniendo en cuenta que los smartphones más populares *ya ofrecen* una cuota importante de privacidad. La probabilidad de que eso ocurra es, por consiguiente, demasiado marginal como para controvertir la afirmación de que el uso de los equipos de EncroChat o Sky ECC era inherentemente sospechoso.

Como puede advertirse fácilmente, en el análisis desarrollado en los párrafos precedentes no me referí a la situación de los usuarios de An0m. Ello se debe a que la situación en orden a estos últimos difiere de la de los otros dos sistemas en que, en relación con EncroChat y Sky ECC, las agencias intervinientes interceptaron las comunicaciones de usuarios -en principio- desconocidos, mientras que en el caso de An0m, el FBI y la PFA distribuyeron equipos con la herramienta de interceptación ya

motivo alguno para llevar consigo dichas herramientas. Por ejemplo, en plena noche, en los alrededores de una vivienda desde la cual no se requirió ningún servicio que demandara del uso de dichas herramientas.

[248] Ver: Departamento de Justicia de los EE.UU. (DOJ), Declaración jurada en apoyo de pedido…, cit, pág. 5.

[249] Un conflicto de esta naturaleza tuvo lugar en el año 2015 entre Apple y el Departamento de Justicia (DOJ) de los EE.UU., en relación con la negativa de la firma a modificar el sistema operativo de uno de sus smartphones para permitir el acceso al contenido del dispositivo del responsable de un ataque terrorista en la ciudad de San Bernardino. Una reseña detallada de este caso puede encontrarse en: BLANCO, Hernán, *Tecnología informática e investigación criminal*, cit., págs. 570/580.

[250] La ubicuidad de los modernos smartphones y el carácter casi irrenunciable de su uso en las sociedades modernas fueron puestos de resalto por la Suprema Corte de los EE.UU. como fundamento para una necesaria actualización de las doctrinas aceptadas sobre el alcance del principio de la intimidad en sendos precedentes, dictados en los casos *Riley v. California* (134 S. Ct. 2743; 2014) y *Carpenter v. United States* (No. 16-402, 585 U.S.; 2018).

instalada a usuarios que esas mismas agencias escogieron (aunque indirectamente, a través de sus distribuidores), por sospechar que integraban organizaciones criminales.

Por consiguiente, si bien en lo que respecta a esta última operación, la afirmación de la PFA en punto a que la totalidad de los usuarios estaba involucrada en actividades criminales no puede comprobarse en forma fehaciente hasta que todos los mensajes interceptados sean analizados[251], lo cierto es que el cuidadoso sistema de selección implementado por las agencias intervinientes a fin de dotar de confiabilidad al sistema (que requería de una recomendación previa de cualquier nuevo usuario por parte de un delincuente que ya estuviese utilizando la plataforma) hacía que resultara casi imposible que uno de estos teléfonos llegase a manos de periodistas o ciudadanos comunes[252]. En sentido opuesto, no parece improbable que a pesar de la cantidad de usuarios objeto de vigilancia (más de 9.000), las agencias policiales intervinientes pudiesen invocar una sospecha razonable de intervención en actividades delictivas respecto de todos ellos. De hecho, y como consecuencia de la modalidad "solo por invitación" del proceso de reclutamiento de nuevos clientes de An0m, el Departamento de Justicia de los EE.UU. los considera a todos como integrantes de una única conspiración criminal[253].

Una última cuestión a analizar es si, en las circunstancias antedichas, puede considerarse respetuosa del principio de proporcionalidad la decisión de extender la interceptación de comunicaciones a la totalidad de los usuarios de los tres sistemas reseñados. Al respecto, cabe tener presente que el carácter trasnacional de las medidas adoptadas en estas operaciones trae aparejado que esta cuestión sea analizada, al mismo tiempo, conforme los principios de los países enrolados en el "Common Law" anglosajón (el Reino Unido, Australia y EE.UU.), en los que la prohibición de los "registros generales" ("general searches") y su contrapartida, el "requisito de especificidad" ("particularity requirement") se encuentran fuertemente enraizados; lo que no ocurre en las naciones cuyos ordenamientos encuadran en la tradición jurídica europea continental (Francia, Bélgica, Alemania, los Países Bajos, España, etc.).

En ese país, inicialmente, la doctrina relativa a la razonabilidad de los registros y secuestros se centró en la protección contra la intrusión física en los hogares, tal como se refleja en el precedente *Olmstead v. United States*[254], de la Suprema Corte. Sin embargo, en 1967 el referido tribunal implantó un nuevo estándar al expedirse *in re*: *Katz v. United States*[255], fallo en que se dejó sentado que "…*la Cuarta Enmienda protege personas, no lugares*"[256]. Ese mismo año, el máximo tribunal estadounidense estableció en forma expresa, en el precedente *Berger v. New York*[257], que el "requisito de especificidad" previsto en la 4ª Enmienda aplicaba también a los registros electrónicos.

En el supuesto de que los registros (en los casos en que nos ocupan, en la forma de una interceptación de las comunicaciones) supongan una injerencia sustancial en el derecho a la privacidad, la doctrina de los EE.UU. coincide en señalar que la 4ª Enmienda

[251] Cfr. PARKIN, Simon: "'Every message was copied to the police'…", cit.
[252] Ver: PARKIN, Simon: "'Every message was copied to the police'…", cit.
[253] Cfr. BAKER, Stewart / KLEHM, Bryce: "Legal Tetris and the FBI's An0m program", cit.
[254] 277 U.S. 438 (1928).
[255] 389 U.S. 347 (1967).
[256] Fallo citado, pág. 347.
[257] 388 U.S. 41 (1967).

de la Constitución de ese país exige que se establezca la existencia de sospecha razonable ("probable cause") *respecto de cada una de las personas cuya información sea capturada* en el transcurso de la medida, sin que pueda satisfacerse dicha exigencia argumentando que la evidencia probablemente aparezca en el cúmulo de información resultante del registro[258].

Esto se desprende también de lo decidido por la Suprema Corte estadounidense en el fallo *Ventura Ybarra v. Illinois*[259], en el que invalidó el registro efectuado respecto de todos los clientes de una taberna a partir del dato (provisto por un informante) de que el barman tenía en su poder heroína y "posiblemente" estuviese vendiéndola. En dicha oportunidad, el referido tribunal señaló que no podía considerarse válido el registro operado sobre Ventura Ybarra (uno de los clientes), desde que "*…los agentes [intervinientes] no sabían nada en particular sobre Ybarra, salvo que estaba presente, junto con otros parroquianos, en una taberna pública en un momento en que la policía tenía motivos para presumir que el barman podía tener heroína a la venta*"[260].

En una primera aproximación, la doctrina sentada en *Ventura Ybarra* podría suponer un obstáculo en el primer supuesto analizado en el presente apartado -esto es, el de una medida de interceptación adoptada en el marco de una investigación enfocada a los responsables de operar los sistemas de EncroChat y Sky ECC, que aun así se extendió a los usuarios de dichos sistemas-; aunque, como luego se ha visto, en realidad -y a diferencia del caso analizado en el precedente de mención- en relación con esos usuarios si podría fundarse una sospecha razonable. Esto último también aplica para la operación mediante la plataforma An0m, puesto que -como se ha visto- la medida siempre estuvo enfocada en los usuarios, y la forma de distribución de los equipos poco menos que garantizaba la existencia de sospecha razonable a su respecto. A lo que cabe añadir que, de todos modos, conforme lo establecido en el precedente *United States v. Verdugo-Urquidez*[261] de la Suprema Corte de EE.UU., la 4° enmienda no protege a las personas que no sean ciudadanas de ese país ni ostenten una "conexión sustancial"[262] con el mismo[263].

Sin perjuicio de lo expuesto, en la jurisprudencia estadounidense el caso que más similitudes presenta con las operaciones objeto de estudio en el presente trabajo es el caso Playpen, en 2014. En dicha oportunidad, el FBI, tras localizar los servidores de una página web de la "red oscura" dedicada a facilitar el intercambio de material de explotación sexual infantil en el estado de Virginia, obtuvo una orden judicial que lo

[258] Cfr. AMSTER, Haley / DIEHL, Brett: "Against geofences", cit., pág. 430 (énfasis añadido). Con cita del precedente *Marks v. Clarke* (102 F.3d 1012, 1029; Tribunal Federal de Apelaciones del 9° Circuito, 1996), en el que se estableció que una orden para registrar a "todas las personas presentes" en procura de evidencia de un delito solo puede obtenerse cuando existen razones para creer que *todos los presentes intervienen en la presunta actividad criminal*; y solo con respecto a un domicilio "dedicado exclusivamente a la actividad criminal" (énfasis añadido). En igual sentido: *Owens v. Lott* (372 F.3d 267, 276, Tribunal Federal de Apelaciones del 4° Circuito, 2004).

[259] 444 U.S. 85 (1979).

[260] Cfr. AMSTER, Haley / DIEHL, Brett: "Against geofences", cit., págs. 422/423 (citas omitidas).

[261] 494 U.S. 271 (1990).

[262] El tribunal, no obstante, no explicó cuando existe la "conexión sustancial" con los EE.UU. que se requiere para obtener la protección constitucional.

[263] Cfr. DONOHUE, Laura K.: "The Fourth Amendment in a digital world", en New York University Annual Survey of American Law, Vol. 71, 2017, pág. 666.

autorizó a asumir el control del sitio web durante aproximadamente un mes e *infectarlo con un virus espía que se descargó automáticamente en las computadoras de todas las personas que ingresaron al mismo* y descargaron archivos ilícitos, obteniendo de ese modo la verdadera dirección IP, geolocalización e información sobre los ordenadores de los usuarios de la página web ilegal. Medida que condujo a la apertura de 135 causas penales y a 350 arrestos solo en los EE.UU.

Si bien la operación desplegada en Playpen presenta algunas diferencias con las aquí analizadas tanto en orden a la modalidad del hackeo[264] como en lo tocante a la acreditación del estado de sospecha razonable requerido para obtener la autorización judicial[265]; es similar en punto al carácter masivo de la medida de interceptación y en que el magistrado autorizante no tenía modo de saber, al momento de dictar la orden judicial, ni quiénes ni cuantas personas iban a ser objeto de la misma. En tal contexto, uno de los principales agravios introducidos por las defensas -y rechazado por los tribunales estadounidenses- se centró en el supuesto incumplimiento de los requisitos de especificidad y sospecha razonable en la orden judicial. Ello, con sustento en que se utilizó una única orden judicial para autorizar la instalación de un spyware estatal en la computadora de cada persona que se logueó en el sitio de Playpen, en lugar de referirse a usuarios en particular. El fundamento de esta objeción no es que pudiese no existir "sospecha razonable" respecto de cada una de las búsquedas concretadas, sino que al autorizarse genéricamente el registro de todos los usuarios de una página que —al momento de librarse la orden— contaba con 150.000 miembros y recibía alrededor de 1500 visitas diarias, el permiso judicial alcanzó a demasiadas personas[266].

A diferencia de lo que ocurre en los EE.UU., en los países enmarcados en la tradición jurídica continental europea no existen antecedentes con los cuáles comparar una medida de vigilancia de la escala y características de la implementada con respecto a los sistemas de EncroChat o Sky ECC. A lo sumo, puede intentar contrastarse la problemática derivada de estos últimos casos con los estándares fijados, de modo general, por los tribunales europeos en precedentes relacionados con la infiltración estatal de los sistemas informáticos de los ciudadanos.

En relación con ello, adquiere relevancia la postura adoptada por el Tribunal Constitucional Federal de Alemania (VBerfG, por sus siglas en alemán) al analizar, en un fallo dictado en 2008[267], la constitucionalidad de la Ley del Land Nordrhein-Westfalen de defensa de la Constitución, de 20 de diciembre del 2006, que permitía al Defensor de la Constitución, observar y realizar descubrimientos en Internet, y acceder a sistemas

[264] Dado que el caso Playpen involucró el empleo de una modalidad conocida como "ataque de abrevadero" ("*watering hole*"), conforme la cual los usuarios afectados *deben llevar a cabo alguna acción* para que el spyware gubernamental se descargue en sus equipos (que puede ser, como en el caso, descargar un archivo ilícito o simplemente conectarse con la página web infectada); mientras que en los ataques de "cadena de suministro" como los realizados contra los clientes de EncroChat y Sky ECC, el programa espía *se descarga automáticamente* junto con las actualizaciones del sistema.

[265] Puesto que se recurrió, en el caso, a una "orden prospectiva", conforme la cual el cumplimiento del estándar de sospecha exigido por la 4ª Enmienda de la Constitución de los EE.UU. estuvo condicionado a un acto futuro de las personas afectadas por la medida de vigilancia: la descarga de material ilícito desde la página web de Playpen.

[266] Cfr. BLANCO, Hernán, *Tecnología informática e investigación criminal*, cit., págs. 499/500 (citas omitidas).

[267] BVerfG, 1 BvR 370/07 vom 27/2/2008.

informáticos[268]. En dicha oportunidad, el VBerfG consideró que la norma -que facultaba a las fuerzas de seguridad a infiltrar sistemas informáticos empleando fallos en la seguridad o instalando programas que permitían observar la utilización del sistema (e incluso dirigirlo)[269]- era contraria a la Constitución Alemana, puesto que suponía una injerencia desproporcionada respecto del derecho "a la integridad y confiabilidad de los sistemas informáticos", al que calificó como un derecho fundamental derivado del derecho al libre desarrollo de la personalidad[270].

En opinión del tribunal citado, las medidas de investigación previstas en la ley objeto de análisis -aunque pudiesen ser consideradas como idóneas y necesarias- incumplían con el requisito constitucional de proporcionalidad en sentido estricto, por cuanto conllevaban una injerencia en el derecho de elevada intensidad sin relación con el bien jurídico que se pretendía salvaguardar[271]. Ello, toda vez que le permitían al Estado poner en peligro la integridad del sistema informático y el acceso de terceros a sus funciones, prestaciones y contenidos[272]. Así las cosas, el VBerfG condicionó la legitimidad constitucional de una eventual norma que incorporase el uso de spyware estatal al cumplimiento de tres requisitos: a) la existencia de una autorización judicial previa para proceder a la infiltración secreta y remota en los diversos equipos electrónicos e informáticos; b) la existencia de *datos fácticos de un concreto peligro para un bien jurídico "especialmente destacable" (el cuerpo, la vida y la libertad de la persona o semejantes bienes de la Comunidad*, cuya amenaza afectaría a los Fundamentos o la propia existencia del Estado o de las personas); y c) las disposiciones necesarias para proteger el núcleo esencial del desarrollo de la vida privada[273].

Extrapolando estas exigencias a los hackeos masivos concretados en las operaciones contra EncroChat y Sky ECC (los que, de hecho, fueron legitimados por los tribunales alemanes), se aprecia que el cumplimiento del primero y el último requisito no presentan mayores dificultades, toda vez que -por un lado- la introducción del "implante técnico" contó, en efecto, con autorización judicial previa y -por el otro- ambos sistemas de mensajería encriptada eran utilizados mayoritariamente para conversaciones relacionadas con la actividad comercial (ilícita) de los usuarios. No esta tan claro, en cambio, que al momento de librarse la autorización judicial -es decir '*ex ante*'- los investigadores contasen con "datos fácticos" sobre la existencia de "un concreto peligro" contra bienes jurídicos "especialmente destacables". La circunstancia

[268] Cfr. GONZÁLEZ PASCUAL, María Isabel: "El Tribunal Constitucional Federal Alemán ante la incompatibilidad con los derechos fundamentales de la normativa nacional de origen europeo de prevención de delitos", en Revista de Derecho Contemporáneo Europeo, N° 34, Madrid, 2009, pág. 948.

[269] Esto es, una medida similar a la instalación de un "implante técnico", como en los casos de EncroChat y Sky ECC, o la distribución de equipos que ya contenían el programa espía, como ocurrió en el sistema An0m.

[270] Cfr. GONZÁLEZ PASCUAL, María Isabel: "El Tribunal Constitucional Federal Alemán…", cit., pág. 949. En esa misma línea, el Tribunal Supremo español reconoció la existencia de un "Derecho al entorno virtual" en la STS 342/2013, del 17 de abril.

[271] BVerfG, 1 BvR 370/07 vom 27/2/2008, parágrafos §§ 226 y 229.

[272] BVerfG, 1 BvR 370/07 vom 27/2/2008, parágrafos §§ 203/206.

[273] Cfr. ORTIZ PRADILLO, Juan Carlos, El 'remote forensic software' como herramienta de investigación contra el terrorismo", en ENAC, E-Newsletter en la lucha contra el cibercrimen, Cibex, 2009, N° 4, pág. 5 (énfasis añadido).

de que ello efectivamente era así solo se comprobó '*ex post*', una vez cumplida la medida.

En este escenario, la decisión de los tribunales alemanes de convalidar el uso de la evidencia proveniente de los hackeos a EncroChat y Sky ECC y la infiltración de An0m *no parece, a primera vista, el producto de una aplicación rigurosa de la doctrina sentada por el VBerfG* en su precedente de 2008. Sin embargo, esta primera impresión puede resultar engañosa, desde que también podría afirmarse que la evidencia que sí existía de antemano -en cuanto demostraba que los mencionados sistemas de mensajería encriptada eran utilizados de modo general por las principales organizaciones criminales de Europa- podría considerarse suficiente para acreditar la concurrencia de una "amenaza contra los fundamentos o la propia existencia del Estado". En especial, si se repara en que el recurso a ese método de comunicación impedía -en ausencia de medidas como las que finalmente se adoptaron- la vigilancia estatal y, por consiguiente, la investigación y persecución de los delincuentes más peligrosos del continente.

Siguiendo esa línea de razonamiento, bien podría considerarse aplicable lo expresado en otro tramo del ya citado fallo del VBerfG, en punto a que -conforme su propia jurisprudencia- el Estado *tiene la obligación de defender la integridad física y la vida de los particulares y puede, a tal efecto, adoptar medidas susceptibles de interferir en los derechos fundamentales*. Siendo que, a fin de determinar si dichas medidas se adecuan a la Constitución, es preciso sopesar primero la importancia de la injerencia en el derecho en cada caso para, a continuación, comprobar el respeto al principio de reserva de ley y de proporcionalidad[274]. Conforme a dichos parámetros, no luce aventurado concluir que la existencia de una sospecha fundada sobre la explotación de los sistemas de mensajería encriptada para facilitar la actividad delictiva organizada a gran escala, sumada a la imposibilidad de acceder a las comunicaciones por otra vía que no fuese el hackeo de dichos sistemas, alcanzaba para sostener que la injerencia sobre el derecho fundamental aludida, aunque considerable, cumplió de todos modos con el requisito de proporcionalidad estricta.

Al apuntado análisis jurídico se adiciona otra consideración de índole práctica, que es que -a diferencia del caso fallado en 2008, en que se analizó la constitucionalidad de las medidas previstas en la norma "en abstracto"- en *esta* oportunidad los tribunales alemanes evaluaron la legitimidad de la evidencia obtenida por las agencias de orden público de Francia, Bélgica, Australia y los EE.UU. *en relación con causas penales concretas involucrando delitos gravísimos* (narcotráfico, intentos de homicidio, etc.), con la intervención de las principales organizaciones criminales del mundo. Sin duda, esta circunstancia ha debido influir -si no resultar determinante- para no considerar desproporcionada la injerencia sobre el derecho a "la integridad y confiabilidad de los sistemas informáticos" reconocido en 2008, como lo evidencia -a mi modo de ver- la alusión expresa de uno de los tribunales intervinientes a la preocupación por no ofender el "sentido de justicia de los ciudadanos alemanes".

Sin perjuicio de lo expuesto, los parámetros más importantes al momento de analizar la legitimidad de las medidas adoptadas en el marco de las operaciones contra EncroChat y Sky ECC y la concretada mediante la plataforma An0m son los que surgen

[274] Cfr. GONZÁLEZ PASCUAL, María Isabel: "El Tribunal Constitucional Federal Alemán…", cit., pág. 950. Con cita de BVerfG, 1 BvR 518/02 vom 4/4/2006, parágrafo § 92.

de la jurisprudencia de los tribunales continentales -la Corte de Justicia de la Unión Europea (CJUE) y el Tribunal Europeo de Derechos Humanos (TEDH)-, en cuyos estrados seguramente terminará dirimiéndose la cuestión.

4.4. Los parámetros establecidos sobre la cuestión en la jurisprudencia de la Corte de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos.

Según explicó el TEDH en un documento reciente[275], frente a planteos vinculados a la posible conculcación del art. 8 del CEDH, el tribunal examina, en principio, tres cuestiones. En primer lugar, si se encuentra en disputa alguno de los cuatro intereses amparados en el artículo (vida privada, vida familiar, intangibilidad del domicilio y de la correspondencia o las comunicaciones) y si ha existido una interferencia a estos derechos, o si se han incumplido los deberes positivos de protección del derecho a la privacidad que pesan sobre los Estados miembros, aspectos que no se encuentran en discusión en lo tocante a las medidas objeto del presente trabajo, en cuanto involucraron la interceptación de las comunicaciones de los usuarios de EncroChat, Sky ECC y An0m[276]. En segundo lugar, se analiza si se verifica alguno de los supuestos en los que los Estados están legitimados para restringir el derecho a la privacidad, enumerados en el art. 8, parágrafo 2 del CEDH. En los casos bajo análisis, estos serían tanto la prevención del crimen como la seguridad pública, en atención al uso de los sistemas de mensajería encriptada por parte de organizaciones criminales de gran peligrosidad. Por último, se evalúa si las restricciones introducidas sobre derecho a la intimidad han sido establecidas "de acuerdo con la ley" y si son "necesarias en una sociedad democrática". Esta última es la cuestión que está llamada a ser objeto de controversia con respecto a la vigilancia desplegada sobre las personas que se comunicaban mediante los teléfonos de EncroChat, Sky EC y An0m[277].

La determinación de si la injerencia puede ser considerada "necesaria en una sociedad democrática" supone un juicio sobre su proporcionalidad en relación con los fines (legítimos) que alentaron la medida[278], aunque en algunos casos -que involucraban injerencias de muy alta intensidad- el TEDH ha evaluado si las mismas podían resultar

[275] Cfr. Tribunal Europeo de Derechos Humanos (TEDH), *Guía sobre el Artículo 8 del Convenio Europeo de Derechos Humanos*, Consejo de Europa, publicado el 31/8/2020, pág. 7, § 1.

[276] Al respecto, vale recordar que el TEDH ya ha establecido que la vigilancia de las comunicaciones y las conversaciones telefónicas se encuentra amparada por el art. 8 del CEDH (ver SSTEDH *in re*: *Halford v. Reino Unido*, § 44; *Malone v. Reino Unido*, § 64; *Weber and Saravia v. Alemania (dec.)*, §§ 76/79 y *Kennedy v. Reino Unido*, § 118).

[277] Al respecto, cabe señalar que entre las cuestiones planteadas ante el TEDH las aplicaciones *A.L. v. Francia* (N° 44715/2020) y *E.J. v. Francia* (N° 47930/2021), se encuentran si las injerencias al art. 8.1. del CEDH fueron "prescritas por la ley" y "necesarias" en el sentido del art. 8 §2, de conformidad con lo establecido en los precedentes *Weber y Saravia v. Alemania* §§ 93 y ss., y *Roman Zakharov v. Rusia*, §§ 228-234; y -en especial- si la legalidad de la injerencia debía evaluarse con arreglo a los criterios establecidos por el Tribunal en relación con la interceptación masiva (cfr., entre otros, lo expresado en *Big Brother Watch y otros v. Reino Unido*, §§ 332-364). Cfr. ZARAGOZA TEJADA, Javier Ignacio: "Operaciones encubiertas digitales y convencionales…", cit., págs. 213/214.

[278] Cfr. STEDH *in re*: *Dudgeon v. Reino Unido*, §§ 51/53.

proporcionales con independencia del propósito invocado para justificarlas[279]. El cumplimiento de esta exigencia de proporcionalidad demanda un equilibrio preciso entre los intereses contrapuestos del individuo y de la comunidad en su conjunto[280]. A tal efecto, el TEDH concede un cierto margen de discrecionalidad a los Estados miembros, los que de todos modos deben demostrar que existe una necesidad social "imperiosa" que demanda la interferencia sobre el derecho afectado[281], y -sobre todo- que *los fines perseguidos no podían cumplirse a través de medidas menos restrictivas*[282].

La verificación sobre el cumplimiento de estas exigencias, sumada a la de explicitar los motivos de la medida en las decisiones en las que se autoriza la vigilancia secreta de los ciudadanos constituye, para el TEDH, una garantía importante[283]. La revisión y supervisión de esta clase de medidas puede concretarse, según el tribunal, en tres fases distintas: cuando son dispuestas por primera vez, mientras se están llevando a cabo o cuando ya se han cumplido[284]. En su análisis, el tribunal toma en consideración las circunstancias del caso; la naturaleza, alcance y duración de las medidas; los motivos invocados para disponerlas; las autoridades competentes para autorizarlas, concretarlas y supervisarlas y los medios establecidos en la legislación para remediar posibles excesos[285]. En esa dirección, el TEDH ha señalado que, aunque -como se adelantó- se le concede cierto margen de apreciación a los estados en la elección de los medios para procurar el propósito legítimo de proteger la seguridad pública, deben no obstante existir salvaguardas para evitar posibles abusos[286].

Examinando los casos objeto de estudio a la luz de dichos parámetros, se advierte que lo relativo a las autoridades encargadas de autorizar, ejecutar y supervisar la vigilancia no luce, en principio, problemático, toda vez que las interceptaciones contaron con previa autorización judicial (aunque puede, como se ha visto[287], discutirse si los magistrados intervinientes estaban legitimados para permitir el hackeo de personas situadas fuera de su jurisdicción) y fueron ejecutadas por las agencias de orden público competentes. A mi modo de ver, tampoco existen dudas en orden a que la modalidad empleada (intrusión de todos los equipos a través de los servidores) constituía el único modo de acceder al monitoreo de las comunicaciones efectuadas mediante estos sistemas de mensajería encriptada. Cabe recordar, al respecto, que el TEDH ha reconocido la importancia que reviste la interceptación de las comunicaciones

[279] Cfr. SSTEDH, *in re*: *Mozer v. República de Moldavia y Rusia* [pleno], §§ 194/196 y *P.T. v. República de Moldavia*, §§ 30/33.
[280] Cfr. SSTEDH, *in re*: *Hämäläinen v. Finlandia* [pleno], § 65; *Gaskin v. Reino Unido*, § 42 y *Roche v. Reino Unido* [pleno], § 157.
[281] Cfr. SSTEDH, *in re*: *Piechowicz v. Polonia*, § 212 y *Paradiso and Campanelli v. Italia* [pleno], §§ 179-184.
[282] Cfr. SSTEDH, *in re*: *Klass y otros v. Alemania*, §51; *Association for European Integration and Human Rights y Ekimdzhiev v Bulgaria*, §§79/80; *Iordachi and Others v. Moldavia*, §51; *Kennedy v. Reino Unido*, §§31/32; *Roman Zakharov v. Rusia* [pleno], § 260 y *Dragojević v. Croacia*, § 94.
[283] Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 121, § 574.
[284] Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 120, § 573.
[285] Cfr. SSTEDH, *in re*: *Roman Zakharov v. Rusia* [pleno], § 232 e *İrfan Güzel v. Turquía*, § 85.
[286] Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 51, § 209. Ver también SSTEDH *in re*: *Weber y Saravia v. Alemania* (dec.), § 106 y *Karabeyoğlu v. Turquía*, §§ 101/103, § 106.
[287] Ver *supra*, § 3.2.

telefónicas, cuando se la concreta con respeto a la ley, para garantizar la seguridad pública y la prevención del crimen[288].

En cuanto aquí interesa, el mismo tribunal ha destacado, no obstante, que la protección ofrecida por el art. 8 del CEDH se vería inaceptablemente debilitada si se permitiese el uso irrestricto de técnicas científicas modernas en el proceso penal, sin sopesar cuidadosamente los posibles beneficios del empleo de las mismas con intereses relevantes vinculados a la vida privada de los ciudadanos[289]. En tal contexto, se aprecia que en relación con los casos objeto de estudio en este trabajo, las cuestiones más problemáticas son las que atañen a la motivación de las medidas adoptadas, su alcance y extensión y la existencia de remedios efectivos para subsanar los posibles excesos.

Al respecto, el TEDH ha señalado que es necesario que se encuentren establecidas de antemano y con claridad tanto la naturaleza de los delitos que pueden dar lugar a una orden de interceptación de comunicaciones como la definición de las categorías de personas que pueden llegar a ser sometidas a una vigilancia de esa clase[290], aunque aclarando que ello no implica que deban enumerarse en forma expresa los delitos específicos que pueden dar lugar a la vigilancia estatal, solo una descripción precisa de las características de los mismos[291]. Esta exigencia forma parte de la que impone que las restricciones a derechos fundamentales sean compatibles con el "estado de Derecho" ("rule of law") y no aplica únicamente a la letra de la ley procesal que prevea la medida en cuestión, sino también a su interpretación y aplicación por parte de los tribunales nacionales, la que debe ser razonable para cumplir con el requisito de previsibilidad[292].

En esa dirección, la jurisprudencia del TEDH exige también que la autorización de una medida de vigilancia secreta identifique "con claridad" a la persona o personas específicas que van a ser sometidas a vigilancia, ya sea mediante la referencia a nombres, domicilios, números telefónicos o cualquier otro dato relevante[293]. En línea con ello, el tribunal descalificó[294] una orden judicial que autorizaba la grabación de audio y video sin identificar a la persona objeto de la misma. En sustento de su decisión, el

[288] Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 121, § 578.
[289] Cfr. STEDH, *S. y Marper v. Reino Unido* [pleno], § 112.
[290] Cfr. STEDH, *in re*: *Roman Zakharov v. Rusia* [pleno], §§ 243 y 247.
[291] Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 125, § 598 y STEDH *in re*: *Kennedy v. Reino Unido*, § 159. En orden a ello, el TEDH consideró incumplido el requisito de previsibilidad en casos en que se permitía extender la vigilancia no solo a los sospechosos sino también a "…cualquier otra persona involucrada en un delito", sin ninguna explicación en punto a cómo debía ser interpretada dicha cláusula (ver SSTEDH *in re*: *Iordachi y otros v. Moldavia*, § 44; *Roman Zakharov v. Rusia* [pleno], § 245 y *Szabó y Vissy v. Hungría*, §§ 67 y 73).
[292] En orden a ello, el TEDH ha establecido que no se cumple el mencionado requisito cuando la ley no establece límites a la discrecionalidad concedida a la autoridad competente para disponer las medidas de vigilancia (*Karabeyoğlu v. Turquía*, §§ 67-69 y §§ 86-88); como así tampoco cuando existe riesgo de arbitrariedad en su implementación (*Bykov v. Rusia* [pleno], §§ 78-79). Así, por ejemplo, en el caso *Altay v. Turquía* (§ 57) el TEDH concluyó que la interpretación extensiva de la ley nacional por parte de los tribunales no cumplía con la exigencia de legalidad establecida en el art. 8 del CEDH (Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 11, § 19).
[293] Cfr. SSTEDH *in re*: *Klass and Others v. Alemania*, §51; *Liberty y otros v. Reino Unido*, §§64-65; *Dumitru Popescu v. Rumania*, §78; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, §80 y *Kennedy v. Reino Unido*, §160.
[294] En la STEDH dictada *in re*: *Hambardzumyan v. Armenia* (§§ 63-68)

TEDH explicó que la autorización judicial de una medida de vigilancia secreta no podía estar redactada en términos cuya vaguedad pudiese dar lugar a especulación o presunciones acerca de su contenido y -sobre todo- a la identidad de la persona objeto de investigación[295].

Frente a lo expuesto, surge el interrogante de si pueden considerarse cumplidos estos parámetros en relación con las operaciones concretadas con respecto a las plataformas EncroChat y Sky ECC, dado que, al momento de librarse las autorizaciones judiciales que dieron sustento a la intrusión informática de los servidores y la infiltración de los equipos de los usuarios, los magistrados autorizantes *no tenían modo de saber* -y, por ende, tampoco de consignar- *ni la identidad precisa de las personas que iban a ser objeto de la medida ni los delitos concretos que eran objeto de investigación* (más allá de la existencia de una sospecha razonable sobre la explotación de los sistemas de mensajería encriptada para facilitar la actividad del crimen organizado). No obstante ello, parece dudoso -a los efectos de tener por cumplido el requisito de previsibilidad- que los usuarios de los mencionados sistemas involucrados en hechos criminales (que, en principio, serían la mayoría) pudiesen albergar alguna duda en punto a que su actividad podía ser objeto de una medida de vigilancia, por más que estuviesen convencidos de que (por motivos técnicos, no jurídicos), la concreción de la misma no era factible respecto de los teléfonos provistos por EncroChat y Sky ECC.

Por añadidura, el TEDH ha establecido que la interceptación de comunicaciones solo es legítima en base a sospechas que puedan ser consideradas objetivamente como razonables[296], subrayando que la autoridad competente para autorizar el empleo de medidas de vigilancia secreta debe ser capaz de verificar la existencia de esta sospecha razonable con relación a las personas objeto de la medida, en particular si existen indicios fácticos que den apoyo a la sospecha de que esa persona está planeando, cometiendo o ya ha cometido delitos u otros actos que puedan dar lugar a una medida de esa clase[297]. En orden a ello, ha señalado también que no resulta válida la justificación retrospectiva de la vigilancia intentada por los tribunales intervinientes[298].

En paralelo, el Tribunal de Justicia de la Unión Europea (TJUE) ha fijado también estándares rigurosos en orden a la protección al derecho a la intimidad en una serie de casos dictados en relación con medidas de vigilancia de los ciudadanos *muchísimo menos restrictivas* del mencionado derecho que las implementadas en el marco de las investigaciones sobre los usuarios de EncroChat, Sky ECC y An0m, desde que no se referían al *contenido* de las comunicaciones, sino a los denominados "datos de tráfico" o "de envoltorio".

El primer precedente relevante del TJUE sobre el tema se dio en el caso *Digital Rights Ireland, Seitlinger y otros*[299], en el cual anuló la Directiva 2006/24/CE del Parlamento Europeo y el Consejo de Europa, que imponía a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar los datos necesarios para identificar el origen, el destino, la fecha, hora y duración de una comunicación

[295] Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 51, § 210.
[296] Cfr. STEDH, *Karabeyoğlu v. Turquía*, § 103.
[297] Cfr. TEDH, *Guía sobre el Articulo 8…*, pág. 121, § 574.
[298] Cfr. SSTEDH, *in re*: *Dragojevic v. Croacia*, §§ 98/98 y *Matanovic v. Croacia*, §§ 114/115.
[299] Asuntos C-293/12 y C-594/12, STJUE del 8/4/2014.

electrónica, el tipo de comunicación realizada, el equipo utilizado y la localización de dicho equipo[300]. Ello, por considerar que lo establecido en la norma continental violentaba los derechos consagrados en los arts. 7, 8 y 52(1) del CEDH al imponer una restricción al derecho a la vida privada y a la protección de datos personales que incumplía con el principio de proporcionalidad. Posteriormente, el referido tribunal ratificó su doctrina al expedirse *in re*: *Tele 2 Sverige AB y Watson*[301] y en *Privacy International*[302].

En esa dirección, el TJUE explicó que, aunque el propósito de la directiva -la lucha contra la delincuencia grave, para garantizar la seguridad pública- constituye, en efecto, un objetivo de interés general de la Unión Europea (UE)[303], debía no obstante comprobarse la proporcionalidad de la injerencia constatada[304] conforme la jurisprudencia del tribunal sobre el principio de proporcionalidad, que exige que los actos de las instituciones de la unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos[305]. Destacó, asimismo, que en atención al importante papel que desempeña la protección de los datos personales en lo que respecta al derecho fundamental al respeto de la vida privada, así como la magnitud y la gravedad de la injerencia, la facultad de apreciación del legislador de la UE resulta reducida y su control, estricto[306].

En el precedente citado, el TJUE reconoció que la conservación de datos establecida en la Directiva 2006/24 constituía una herramienta útil para las investigaciones penales y -por consiguiente- podía ser considerada como adecuada para lograr el objetivo perseguido[307]; como así también que la eficacia en la lucha contra la delincuencia grave (en especial la organizada) -que reviste una *importancia "primordial" para garantizar la seguridad pública*- puede *depender en gran medida de la utilización de técnicas modernas de investigación*. No obstante ello, terminó concluyendo que ninguno de esos dos factores podía justificar, por sí sólo, la necesidad de una medida como la prevista en la citada Directiva[308].

En este escenario, el tribunal explicitó los motivos por los que consideró que el "sistema de vigilancia masivo" establecido en la Directiva 2006/24 resultaba incompatible con los principios de necesidad y proporcionalidad, destacando que el mismo alcanzaba, en general, a todas las personas y formas de comunicación electrónica sin distinciones o límites fundados en el objetivo declarado de prevenir la delincuencia grave. Por consiguiente, suponía una restricción al derecho a la privacidad de la totalidad

[300] En relación con la citada directiva, ver: VILASAU, Mónica: "La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad", en IDP. Revista de Internet, Derecho y Política. Nº. 3, UOC, 2006, págs. 1/15.
[301] Asuntos C-203/15 y C-698/15, STJUE del 21/12/2016.
[302] Asunto C-623/17, STJUE del 6/10/2020.
[303] Dado que, como reconoció expresamente el tribunal, la Carta de Derechos Fundamentales establece el derecho de todas las personas no sólo a la libertad, sino también a la seguridad (parágrafo § 42),
[304] Cfr. STJUE *in re*: *Digital Rights Ireland*, cit., § 45.
[305] Fallo citado, § 46 (con cita de las SSTJUE *in re*: *Afton Chemical*, §45; *Volker y Markus Schecke y Eifert*, §74, *Nelson y otros*, §71; *Sky Österreich*, §50 y *Schaible*, §29.
[306] Cfr. STJUE *in re*: *Digital Rights Ireland*, cit., § 48.
[307] Cfr. STJUE *in re*: *Digital Rights Ireland*, cit., § 49.
[308] Cfr. STJUE *in re*: *Digital Rights Ireland*, cit., § 51 (énfasis añadido).

de la población europea, incluyendo a personas respecto de las cuales no se había acreditado un vínculo, siquiera remoto, con la actividad criminal.

Sin perjuicio de lo expuesto, en el precedente dictado *in re*: *La Quadrature du Net y otros*[309], el TJUE, si bien ratificó la ilegitimidad de las normas que prescriben la retención indiscriminada de datos de tráfico y localización, reconoció que cuando un Estado miembro enfrenta una amenaza seria a la seguridad nacional, genuina, presente o previsible, podría admitirse la implementación de medidas legislativas admitiendo la retención generalizada de datos por un período de tiempo que no exceda de lo estrictamente necesario. Ello, siempre y cuando dichas medidas estuviesen dirigidas a personas respecto de las cuáles existiesen motivos válidos para sospechar la posible intervención en "actividades terroristas".

Ahora bien: al momento de evaluar la aplicación de los parámetros establecidos por el TJUE con relación a las medidas de vigilancia masiva, entiendo necesario tener presente que en los casos objeto de este trabajo -a diferencia de los analizados por el mencionado tribunal- la interceptación de las comunicaciones de los usuarios de EncroChat, Sky ECC y An0m no estaba dirigida a obtener información que hipotéticamente en un futuro pudiese permitir la prevención de un eventual ataque terrorista, sino a obtener evidencia sobre *actividad delictiva grave en curso*, la que -conforme la *información con la que ya contaban* las agencias de orden público- estaba siendo cometida por organizaciones criminales sirviéndose de los sistemas de comunicación segura ofrecida por las mencionadas plataformas. Por consiguiente, aunque no se supiese con certeza si todos los usuarios estaban involucrados en delitos, ni en qué delitos en particular ni dónde estaban cometiéndose; si se sabía que la actividad de esas organizaciones criminales suponía una amenaza genuina y presente contra la seguridad de los ciudadanos, que la medida con toda probabilidad arrojaría resultados de enorme trascendencia para la lucha contra el crimen organizado trasnacional (como efectivamente ocurrió) y que la evidencia resultante de dicha interceptación no podía ser obtenida de otra manera.

5. CONFLICTO ENTRE EL DERECHO A CONTROLAR LA PRUEBA DE CARGO Y LA CONFIDENCIALIDAD DE LAS HERRAMIENTAS DIGITALES. IGUALDAD DE ARMAS.

5.1. Planteos de las defensas contra la confidencialidad de las herramientas informáticas utilizadas en EncroChat.

El recurso a medidas de investigación avanzadas como el govware, en especial cuando se implementa a través de una metodología nunca antes empleada por una autoridad estatal en el marco de un proceso penal, como ocurrió en el caso EncroChat y -presumiblemente- también en el de Sky ECC, naturalmente genera interrogantes en orden a la confiabilidad de la evidencia (informática) resultante. Más aún cuando -como en estos casos- dicha evidencia constituye la prueba central, dirimente, en la inmensa mayoría de los procesos iniciados contra los usuarios de los sistemas de comunicación antes mencionado.

[309] Asuntos C-511/18, C-512/18 y C-520/18, STJUE del 6/10/2020.

Al respecto, cabe tener presente que en lo tocante a la prueba digital -por tratarse de un tipo de evidencia que no puede ser capturada manualmente ni percibida en forma directa por los sentidos, sino que demanda del uso de herramientas informáticas tanto para su recolección como para su observación y análisis- la cuestión de la confiabilidad es determinante. Tanto más cuando se trata de información altamente volátil y muy fácil de manipular, destruir o replicar[310]. En tal contexto, la confiabilidad de las herramientas informáticas de recolección de evidencia *no puede ni debe presumirse*, toda vez que el campo de la informática forense carece del marco teórico, la metodología científica subyacente y el fundamento experimental con que cuentan otras áreas de la ciencia forense[311].

En los casos objeto de este trabajo, además, concurren dos circunstancias que le aportan una relevancia adicional a la cuestión de la confiabilidad del método empleado para la recolección de evidencia. En primer lugar, el carácter experimental del "implante técnico" utilizado en EncroChat y el desconocimiento sobre cómo funcionan los programas que se emplearon para recoger las comunicaciones efectuadas mediante los sistemas Sky ECC y An0m. En segundo, que la evidencia informática de cargo no provino de sistemas "en reposo" (en los que puede obtenerse sin mayores problemas una "imagen" digital que garantice la integridad del contenido), sino de sistemas "vivos" (es decir, en funcionamiento), en los que los datos se encontraban en constante transformación mientras la prueba se estaba recolectando[312].

Así las cosas, resulta indudable que el cumplimiento de los estándares requeridos para asegurar la confiabilidad de la evidencia digital se torna considerablemente más dificultoso cuando se trata de información preveniente de un hackeo[313]. Ello así, desde que, por un lado, la prueba resultante y los métodos utilizados para capturarla deberían poder ser testeados ante un tribunal al igual que cualquier otra evidencia proveniente de un proceso forense[314], a cuyo efecto, los expertos que asisten a la defensa tendrían que poder analizar la totalidad del proceso desarrollado para capturar los datos, *incluyendo el método utilizado para introducir el "implante"*, su funcionamiento, el mecanismo de "exfiltración" de la información, las características del servidor que recibió la evidencia y su tratamiento posterior[315]. En especial, teniendo en cuenta que la propia naturaleza del software y de la programación de computadoras determina que ciertos errores sean más pasibles de ser detectados a través de una evaluación "adversarial"[316].

---

[310] Cfr. United Nations Office on Drugs and Crime (UNODC), Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies, junio 2014, págs. 61/62.
[311] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., pág. 14.
[312] Ello, conforme los principios establecidos en las guías de "buenas prácticas" emitidas por organismos internacionales de reconocida autoridad en materia de evidencia digital (ACPO, Interpol, ENISA, ENFSI, ETSI, US SWGDE, ISO 17025, etc.).
[313] Cfr. SOMMER, Peter: "Evidence from hacking…", cit., pág. 7.
[314] Cfr. SOMMER, Peter: "Evidence from hacking: A few tiresome problems", en Forensic Science International: Digital Investigation, Vol. 40, 2022, pág. 1.
[315] Cfr. SOMMER, Peter: "Evidence from hacking…", cit., pág. 6 (énfasis añadido).
[316] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / LANDAU, Susan / OWSLEY, Brian: "Seeking the source: Criminal defendants' constitutional right to source code", en Ohio State Law Journal, Vol. 17, N° 1, 2021, págs. 17/18.

Por otro lado, sin embargo, es evidente que la agencia de orden público que haya obtenido la evidencia ostenta un interés legítimo en pretender que la metodología empleada se mantenga en reserva, para evitar que futuros objetivos aprendan como contrarrestarla[317], a lo que viene a sumarse, además, el *riesgo de proliferación* del software malicioso. En efecto, es importante tener presente que el riesgo de difusión y proliferación de vulnerabilidades y "exploits"[318] es inherente a su uso para la implementación de un spyware estatal. Ello, toda vez que -a diferencia de las armas convencionales- estas verdaderas "ciberarmas" a las que el Estado recurre para penetrar los sistemas informáticos no explotan ni son destruidas al ser utilizadas. Esta no es una preocupación meramente hipotética, tal como lo demostró la proliferación del código del virus "Stuxnet", el que, tras ser publicado en internet, se utilizó para el desarrollo de distintas variantes de spyware como "Duqu", "Flame" y "Gauss"[319]. Por consiguiente, no sólo debe tomarse en consideración la posibilidad concreta de que un criminal técnicamente avanzado que note la existencia del govware en su equipo pueda recurrir a la ingeniería inversa para conocer el código y utilizarlo contra el propio Estado o en perjuicio de terceros inocentes[320], sino también la de que actores maliciosos utilicen el código de las herramientas informáticas en manos del Estado con fines delictivos[321].

Debido a ello, es natural que las agencias de orden público que poseen y utilizan herramientas informáticas avanzadas hagan grandes esfuerzos por impedir que se divulgue información sobre su naturaleza y funcionamiento. Esto es precisamente lo que ha ocurrido en el caso EncroChat, en el que la Gendarmería francesa viene sosteniendo el secreto sobre todo lo relativo al implante técnico empleado para el hackeo de EncroChat. Ello, al amparo de lo establecido en el art. 230-2 del CPC, en cuanto sostiene la confidencialidad de las herramientas sometidas al secreto de defensa nacional a las que es posible acudir en el marco de investigaciones por delitos graves conforme lo establecido en los arts. 230-1 y 706-102-1 del CPC. Así, en virtud de lo dispuesto en la norma citada en primer término, la naturaleza de las herramientas secretas sólo puede hacerse pública en los casos previstos en el Código de Defensa, tratándose de decisiones que no tienen carácter jurisdiccional ni pueden ser objeto de apelación de ningún tipo[322].

Aun así, la decisión de las autoridades francesas de mantener en absoluta reserva todo lo tocante a la naturaleza y funcionamiento de la herramienta informática utilizada para concretar el monitoreo de los usuarios de EncroChat ha sido cuestionada por las

[317] Cfr. SOMMER, Peter: "Evidence from hacking…", cit., pág. 1.
[318] Un "exploit" es el código informático que se utiliza para explotar una "vulnerabilidad" (esto es, un error de programación que compromete la seguridad de un sistema o aplicación) a efectos de permitir la intrusión informática.
[319] Ver: LINDSAY, Jon R., "Stuxnet and the limits of cyber warfare", en Security Studies, vol. 22, N° 3, 2013, págs. 365/404.
[320] Cfr. GHAPPOUR, Ahmed: "Searching places unknown: Law enforcement jurisdiction on the dark web", en Stanford Law Review, vol. 69, N° 4, 2017, pág. 1111 (Énfasis añadido).
[321] Como ya ha ocurrido -por ejemplo- con el famoso virus "Wannacry" (que infectó miles de computadoras en 2017), que tuvo su origen en "exploits" sustraídos a la Agencia de Seguridad Nacional (NSA) de los EE.UU. en un ataque informático perpetrado uno año antes (al respecto, ver: BIDDLE, Sam, "Leaked NSA malware is helping hijack computers around the world", en The Intercept, publicado el 12/5/2017, obtenido en: https://theintercept.com/2017/05/12/the-nsas-lost-digital-weapon-is-helping-hijack-computers-around-the-world/).
[322] Art. 230-4 del CPC.

defensas de los imputados, con sustento en la indebida restricción del derecho de sus asistidos a controlar la prueba de cargo en su contra y la conculcación del derecho a la igualdad de armas consagrado en el art. 6° del CEDH. En sustento de esta última afirmación, las defensas argumentaron que la inexistencia de un recurso para controvertir la decisión de mantener en secreto las características de la herramienta utilizada en el CPC francés torna inconstitucional a la normativa que regula su uso. Como así también que, para que garantizar un juicio justo a los acusados, es preciso que las autoridades francesas expliquen cómo se llevó a cabo la interceptación de los mensajes intercambiados entre los equipos de EncroChat y certifiquen la autenticidad de la evidencia colectada[323].

En igual sentido, los letrados de varios imputados en un caso por narcotráfico en los Países Bajos alegaron ante los tribunales de esa nación que les resultaba imposible montar una defensa eficaz, debido a que el Ministerio Público Fiscal neerlandés no había entregado documentación detallando el funcionamiento del govware empleado para interceptar los mensajes de sus clientes. En tal contexto, consideraron que la operación contra el sistema EncroChat resultaba violatoria del art. 6° del CEDH[324].

En orden a estos planteos, cabe tener presente que -a diferencia de lo que ocurre en la legislación procesal francesa- la normativa vigente en los Países Bajos establece que las herramientas informáticas empleadas para concretar un hackeo estatal deben ser sometidas a una rigurosa inspección conforme los estándares fijados en la reglamentación[325]. Sin embargo, la legislación prevé que sólo los programas utilizados para la recolección de evidencia están sometidos a inspección, mientras que el software o "*exploit*" empleado para concretar la intrusión informática puede mantenerse en reserva[326].

De ese modo, la normativa procesal neerlandesa permite la adopción de la modalidad de hackeo legal denominada "lanzador/carga", propiciada por BELLOVIN y otros autores[327], la que consiste en el uso de una herramienta informática integrada por dos módulos: por un lado, el "exploit" mediante el cual se lleva a cabo la intrusión en el sistema objetivo (denominado "lanzador" o "dropper"); por el otro, el programa que recolecta la evidencia digital (al que se alude como la "carga" o "payload"). Esta modalidad saca provecho de la circunstancia de que, a los efectos de la cadena de custodia y la confiabilidad de la evidencia recolectada, sólo las características de este último programa resultan relevantes para la defensa, a lo que se suma que -dado que se trata de un software "genérico", que no depende del uso de una vulnerabilidad para funcionar- su código puede divulgarse sin comprometer la efectividad de futuras interceptaciones ni aumentar el riesgo de proliferación. El código del software "penetrador", en cambio, se mantiene en reserva, ya que su funcionamiento no incide sobre la integridad y autenticidad de los datos informáticos que recolecta el programa principal y -especialmente- su divulgación sería perjudicial para el Estado (disminuyendo su capacidad para interceptar comunicaciones) y el público (debido a la proliferación de

[323] Cfr. GOODWIN, Bill: "French Supreme Court raises constitutional questions…", cit.
[324] Cfr. GOODWIN, Bill: "Dutch prosecutor ordered to give evidence…", cit.
[325] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12.
[326] Cfr. EUROPOL / EUROJUST, *Third report of the observatory function…*, cit., pág. 12.
[327] Vere: BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan: "Lawful hacking…", cit., pág. 39.

"exploits" peligrosos para la seguridad informática) sin generar como contrapartida un beneficio para el derecho de defensa y el debido proceso[328].

De ello se sigue que si en lugar de remitirse a lo establecido en la legislación francesa, se hubiese aplicado la neerlandesa, se podría haber conciliado el interés estatal de mantener la confidencialidad sobre la naturaleza del "implante técnico" utilizado por la gendarmería francesa con el derecho de defensa de los imputados, lo que -como puede apreciarse- no ocurrió en el caso, dado que dicho implante no fue inspeccionado por las autoridades de los Países Bajos ni tampoco se le permitió a las defensas acceder a información sobre el mismo.

Asimismo, ante los tribunales del Reino Unido, donde la Ley de Investigación y Proceso Penal de 1996 impone al Ministerio Público Fiscal la obligación de compartir toda la información que pueda resultar relevante para la defensa[329], se afirmó que la decisión de Francia de no revelar información sobre el modo en que se concretó el hackeo a EncroChat generó un "agujero negro probatorio" que infringió los principios básicos sobre adquisición y control de la evidencia presentada en el proceso penal[330]. En opinión de algunos defensores, el secreto sobre el modo en que se produjo la intrusión en el mencionado sistema genera dudas sobre la confiabilidad de la información en la que se sustentan las acusaciones, lo que los ha llevado a plantear que se trata de evidencia obtenida en forma incorrecta e ilegal[331].

La falta de precisiones sobre esta cuestión quedó en evidencia en el modo en que se resolvieron los casos vinculados a EncroChat cuyas sentencias ya se publicaron, en los que la fundamentación del fallo *se basó en suposiciones sobre el momento en que se produjo la interceptación*. En efecto, los sentenciantes señalaron que en el caso del emisor de los mensajes aquella "probablemente" tuvo lugar antes de que oprimiese "enviar", como así también que la información "debió" ser capturada cuando no estaba "en tránsito", ya que de lo contrario hubiese estado encriptada[332]. Sin embargo, una nota periodística referida al uso de la evidencia proveniente del hackeo a EncroChat para sustentar una condena por homicidio pareciera indicar que al menos algo de información sobre el funcionamiento de la herramienta informática pudo haberse divulgado, en tanto se consignó que dos peritos que estudiaron el caso "en detalle" testificaron en el juicio (tras haber producido un reporte técnico conjunto), que "*…el implante y el sistema de procesamiento no eran confiables y que los implantes frecuentemente dejaban de operar y debían ser reiniciados*"[333].

---

[328] Cfr. BLANCO, Hernán: "El hackeo con orden judicial…", cit., pág. 485. Una disposición similar se encuentra establecida en el art. 588 septies (a)(2)(b) de la Ley de Enjuiciamiento Criminal (LEC) española.

[329] Cfr. SOMMER, Peter: "Evidence from hacking…", cit., pág. 3 (notas omitidas). La defensa, a su vez, debe hacer una presentación detallando qué información puede resultar relevante para la preparación de su caso

[330] Cfr. GOODWIN, Bill: "French Supreme Court raises constitutional questions…", cit.

[331] Cfr. GOODWIN, Bill "Encrochat: Appeal court finds 'digital phone tapping' admisible…", cit.

[332] Cfr. fallo *A, B, D & C v. Regina*, cit. § 34.

[333] Cfr. CAMPBELL, Duncan: "Two convicted in the first murder plot case involving Encrochat messaging system", en The Guardian, publicado el 14/3/2022, obtenido en: https://www.theguardian.com/world/2022/mar/14/two-guilty-of-james-bond-gun-plot-in-encrochat-conviction.

En paralelo a los planteos introducidos ante los tribunales nacionales de los países europeos afectados por la operación contra EncroChat, un grupo internacional de abogados defensores de Francia, Bélgica, Alemania, Países Bajos, Noruega, Suecia y el Reino Unido publicó una carta abierta dirigida al Parlamento Europeo[334], argumentando que la confidencialidad en torno a dicho hackeo les impedía a sus clientes obtener un juicio justo. Debido a ello, le solicitaron a dicha institución (o la Comisión Europea) la suspensión de los procesos de los acusados en relación con dicho sistema hasta tanto se brinde acceso a mayor información sobre la operación. Según los signatarios de la carta, lo ocurrido con relación a EncroChat carece de precedentes y violenta la doctrina sentada en la jurisprudencia del TEDH, generando un "preocupante precedente"[335].

No se han publicado hasta el momento noticias sobre planteos vinculados a la confidencialidad de los programas informáticos utilizados para recolectar la evidencia en los casos Sky ECC y An0m. Con respecto a este último, no obstante, corresponde recordar que en los EE.UU., la jurisprudencia sentada por la Suprema Corte en *Brady v. Maryland*[336] establece que el gobierno está obligado a revelar cualquier evidencia que pueda resultar relevante ("material") y favorable para el imputado en un caso penal, bajo pena de violentar el debido proceso. Esta obligación fue, no obstante, relativizada en los precedentes *Roviaro v. United States*[337] y *Jencks v. United States*[338], en los que se analizó el alcance del privilegio del Estado[339] —con sustento en la Ley de Procedimientos sobre Información Secreta (Classified Information Procedures Act)—, determinándose que no existía una regla fija, sino que en cada caso debía balancearse el interés público en proteger la fuente de información contra el derecho del individuo en preparar su defensa. Pero también que, si el Estado optaba por no cumplir con una eventual orden de producir la información requerida, el caso debía ser desestimado[340].

5.2. Respuesta de los tribunales nacionales europeos a planteos sobre violación al derecho de defensa e igualdad de armas.

En Francia, la *Cour de Cassation* (CdC) decidió, a mediados de 2021, referir el caso EncroChat al Consejo Constitucional (CC) a fin de que se expidiese en orden a si las medidas de secreto aplicadas con respecto a la operación eran compatibles con la carta magna de ese país[341]. En esa dirección, el máximo tribunal francés, aunque no se expidió sobre la cuestión de fondo, si destacó que la decisión de las autoridades de invocar el secreto de defensa nacional con relación a la operación completa -y no sólo a la recolección de datos informáticos encriptados- impedía la introducción en el debate

[334] La carta puede encontrarse en el siguiente link: https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf.
[335] Ver: Motherboard: "EncroChat lawyers say clients haven't had fair trials", cit.
[336] 373 U.S. 83 (1963).
[337] 353 US 53 (1957).
[338] 353 US 657 (1957).
[339] Cuya existencia, en casos civiles, ya había sido afirmado por la Suprema Corte estadounidense en *United States v Reynolds* (345 U S. 1, de 1953).
[340] Cfr. BLANCO, Hernán, *Tecnología informática e investigación criminal*, cit., págs. 159/151 (citas omitidas).
[341] Cfr. GOODWIN, Bill: "French Supreme Court raises constitutional questions…", cit.

adversarial de una gran cantidad de información relevante para verificar la regularidad de lo actuado, lo que -a su vez- podría suponer una restricción excesiva de los derechos y garantías invocados[342].

El CC se pronunció sobre el tema el 8 de abril de 2022[343], rechazando que la aplicación en el caso del "secreto de defensa" a fin de mantener oculta a los abogados la información sobre la operación de "piratería (informática) policial" habría violado el derecho de los acusados a un juicio justo. En ese orden de ideas, el CC concluyó que las disposiciones del CPC aplicables al caso[344] -que facultan a los investigadores a invocar el secreto de defensa para mantener en reserva ciertas operaciones de vigilancia- no conculcan el derecho a un recurso judicial efectivo. En sustento de esta apreciación, el consejo destacó, en primer término, que le correspondía al legislador nacional conciliar, por un lado, los derechos de la defensa bajo el principio adversarial y, por el otro, los objetivos estatales (constitucionalmente valiosos) de identificar a los perpetradores de los delitos y salvaguardar los intereses fundamentales de la nación, que incluyen el secreto de defensa nacional[345].

En tal contexto, el CC, aun reconociendo que las normas objeto de análisis tenían el efecto de vedar el debate adversarial con relación a la información sobre los medios técnicos empleados[346], entendió que la intención del legislador al adoptarlas fue permitirle a las autoridades encargadas de llevar adelante las investigaciones beneficiarse de herramientas efectivas para capturar y clarificar datos, sin debilitar el accionar de los servicios de inteligencia revelando las técnicas utilizadas por estos, a efectos de cumplir con los objetivos antes mencionados[347].

Asimismo, el CC puso de resalto que la invocación del secreto de defensa nacional sólo puede darse en relación con la implementación de una técnica especial de investigación autorizada por un juez de garantías o por el magistrado a cargo de la pesquisa, con fundamento en la necesidad de obtener información en orden a delitos de especial gravedad o complejidad; como así también que la citada técnica solo puede aplicarse bajo la autoridad y control del juez que la autorizó, que puede disponer su interrupción en cualquier momento[348].

En este escenario, el CC explicó que, aunque es real que "cierta información técnica" queda exenta del debate adversarial, lo cierto es que la orden escrita y fundada del magistrado debe obrar en el expediente bajo pena de nulidad, y contener el detalle del delito que motiva el uso de la herramienta informática, la ubicación exacta o

[342] Cfr. GOODWIN, Bill: "French Supreme Court raises constitutional questions…", cit.
[343] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, Conditions of recourse to the means of State services subject to national defense secrecy within the framework of certain criminal proceedings. Obtenida en: https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2022987qpc/2022987qpc.pdf.
[344] El CC enumeró, a tal efecto, los arts. 230-1 (texto conforme ley del 13/11/2014), 230-2 (texto conforme ley del 3/8/2018), 230-3 (texto conforme ley del 3/6/2016), 230-4 (texto conforme ley del 13/11/2014) y 230-5 (texto conforme ley del 15/11/2001) y 706-102-1 (texto conforme ley del 23/3/2019) del Código de Procedimiento Criminal francés (Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, §§ 1 y 7).
[345] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 12.
[346] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 14
[347] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 15
[348] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 16

descripción detallada de los sistemas de procesamiento afectados, así como la duración de la medida. A su vez, debe agregarse también al expediente un reporte sobre la instalación de la herramienta, consignando en particular las fechas y horarios en los que la operación comenzó y concluyó y describiendo o transcribiendo los datos considerados útiles para llegar a la verdad. Por último, señaló que "…*todos los elementos obtenidos como resultado de la operación están sometidos a un reporte de aceptación incluido en el expediente del procedimiento y acompañados por un certificado estampado por el encargado del cuerpo técnico interviniente que certifica la veracidad de los resultados transmitidos*"[349]. Recordó también que el tribunal (pero no las partes) puede solicitar la desclasificación de la información sometida a secreto de defensa bajo ciertas condiciones[350].

En base a estos argumentos, el CC concluyó que las normas cuestionadas garantizan un adecuado equilibrio entre los requisitos constitucionales en juego[351] y, por consiguiente, no violentan los derechos de los ciudadanos al remedio judicial efectivo, la vida privada, la libertad de expresión ni ninguna otra garantía amparada por la Constitución de Francia, por lo que las declaró constitucionales[352].

A priori, los argumentos ensayados por el CC para sostener la constitucionalidad de las disposiciones del CPC -conforme fueron aplicadas en el caso concreto de EncroChat- no parecen ofrecer una respuesta sólida a los planteos efectuados por las partes, en especial en lo tocante al derecho a controlar la prueba de cargo y la garantía de "igualdad de armas" protegida por el art. 6 del CEDH. Ello así, desde que, con respecto al primer derecho aludido, la incorporación al expediente de la resolución adoptada por el juez interviniente solo permite evaluar los fundamentos de la medida autorizada en términos de razonabilidad (existencia de sospecha suficiente) y proporcionalidad, pero *nada aporta a los efectos de que las defensas puedan analizar (y en su caso cuestionar) la efectividad del proceso de recolección de evidencia* y la confiabilidad de la prueba resultante. Por consiguiente, la cuestión de si los "implantes técnicos" utilizado en EncroChat o Sky ECC pueden garantizar, o no, la integridad, completitud y no manipulación de la prueba de cargo obtenida queda librada a la *confianza que pueda otorgársele a la certificación estampada por el funcionario del cuerpo técnico encargado* del hackeo, sin que medie un recurso para poder revisarla o cuestionarla, aspecto que consagra un notorio desbalance en perjuicio de las defensas.

Al respecto, expertos estadounidenses en la valoración de prueba informática han señalado que no resulta prudente dejar librada la conclusión acerca de la confiabilidad de una herramienta informática a la evaluación de un experto, aunque se trate de uno con probado conocimiento sobre el funcionamiento de la misma. Y ello, por diversos motivos, entre los que mencionan: la incapacidad de los programadores para advertir sus propios errores; la posibilidad de que las propias especificaciones del programa estén equivocadas (de modo tal que aunque el software la cumpla, de todos modos no funcione como es debido); la ineficacia de los datos utilizados para concretar la evaluación; y, por último, la evidencia empírica, de la que se desprende una

[349] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 17 (subrayado añadido).
[350] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 18.
[351] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 19.
[352] Conseil Constitutionnel, Decision No. 2022-987 QPC del 8/4/2022, § 20

multiplicidad de casos en los que se probó, en evaluaciones adversariales, que programas que eran considerados adecuados contenían defectos graves[353].

A lo expuesto se añade que, en la práctica, un fallo de la CdC francesa posterior al pronunciamiento del CC *puso en duda incluso la propia existencia del "certificado de autenticidad"* en el que este último fundó su tesis favorable a la constitucionalidad de las normas procesales aplicadas en el caso EncroChat. En efecto, el pasado 11 de octubre de 2022, el máximo tribunal penal de Francia anuló una resolución previa del Tribunal de Apelación de Nancy (que había convalidado la legitimidad de la evidencia recolectada por la gendarmería francesa), con sustento en la posible conculcación del derecho a confrontar la prueba de cargo y la "igualdad de armas" de los imputados, destacando -por un lado- que en el expediente no se había volcado información técnica suficiente con respecto al procedimiento utilizado para capturar la evidencia; y -por el otro- que el tribunal de apelación regional no había dado respuesta al planteo de la defensa sobre la *no presentación del "certificado de autenticidad"* exigido por las normas procesales aplicables[354].

El impacto casi catastrófico que se avizoraba ante la posibilidad de un eventual decisorio de la CdC que invalidase la evidencia proveniente de EncroChat a partir de la ausencia del "certificado de autenticidad" (teniendo en cuenta que, como ya se señaló *supra*[355], la casi totalidad de los tribunales europeos respondió a las objeciones de las defensas sobre la legitimidad de la prueba obtenida por la gendarmería francesa -y distribuida al resto de los países del continente- remitiéndose a las decisiones de las autoridades francesas que habían convalidado su recolección, con sustento en el principio de "confianza mutua") se vio mitigada por la decisión adoptada por ese mismo tribunal el pasado 6 de septiembre de 2023, oportunidad en la que convalidó una sentencia del Tribunal de Apelación de Metz que ratificó la validez de la evidencia de EncroChat incluso en ausencia del "certificado de autenticidad". En efecto, en el fallo ratificado por la CdC, el tribunal intermedio determinó no existían motivos para poner más información sobre el hackeo a disposición de las defensas, por cuanto -a su entender- la normativa procesal francesa no obligaba a los fiscales a presentar un certificado de autenticidad de los datos obtenidos, sino que dicha presentación solo resultaba exigible cuando la información hubiese sido desencriptada[356].

Asimismo, la CdC rechazó el pedido de las defensas de obtener más información con respecto al modo en que se llevó a cabo el hackeo, argumentando que las normas procesales referidas a la revelación de detalles técnicos sobre las medidas tecnológicas de investigación no resultaban aplicables a la operación EncroChat y que no era posible

[353] Ver: BELLOVIN, Steven M. / BLAZE, Matt / LANDAU, Susan / OWSLEY, Brian: "Seeking the source:...", cit., pág. 32 (citas omitidas).

[354] Ver: GOODWIN, Bill: "French Supreme Court rejects EncroChat verdict after lawyers question secrecy over hacking operation", en Computer Weekly, publicado el 12/10/2022, obtenido en: https://www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy.

[355] § 3.3.

[356] Cfr. GOODWIN, Will: "French supreme court dismisses legal challenge to EncroChat cryptophone evidence", en Computer Weekly, publicado el 6/9/2023, obtenido en: https://www.computerweekly.com/news/366551078/French-supreme-court-dismisses-legal-challenge-to-EncroChat-cryptophone-evidence.

afirmar "…*que todos los datos provenientes de* [dicho sistema] *hubiesen sido capturados en forma ilegal, ni que su recolección y posterior uso fuesen inválidos*"[357].

5.3. El derecho a controlar la prueba de cargo y la igualdad de armas en la jurisprudencia del Tribunal Europeo de Derechos Humanos.

Conforme se establece en la jurisprudencia del TEDH, el principio básico que rige la aplicación del art. 6 del CEDH es el de "justicia"[358] (entendido como equilibrio entre las partes contendientes –"fairness"-, antes que como referencia al logro de un resultado final que asegure la justicia material –"justice"-). El tribunal continental ha reconocido, no obstante, que no existe una regla general para determinar si un juicio es, o no, justo, sino que ello depende de las circunstancias de cada caso particular[359]. Y aunque la evaluación sobre el punto debe efectuarse, a priori, tomando en consideración la totalidad del proceso, y no un aspecto o incidente específico, el TEDH admite también la posibilidad de que, en algunos supuestos, un único factor sea lo suficientemente decisivo como para que la omisión de analizar su impacto -aun en una etapa preliminar del proceso- torne a este último incompatible con lo establecido en el art. 6 del CEDH[360].

La jurisprudencia del TEDH sobre evidencia digital es bastante escasa y ha sido calificada de "inconsistente"[361]. Esta renuencia del tribunal en fijar estándares con relación a la valoración de esta clase de evidencia es problemática, toda vez que resulta usual que los tribunales nacionales den por sentada la fiabilidad del testimonio de los expertos gubernamentales, lo que coloca a las defensas en una posición desventajosa a la hora de cuestionar las opiniones de aquellos[362]. Ello obliga a extraer los parámetros necesarios para analizar lo ocurrido en los supuestos en estudio de la doctrina sentada en el marco de casos que involucraron, por lo general, la producción de prueba física, cuyas características son muy distintas de las de la evidencia digital. En dicho marco, la jurisprudencia del TEDH establece que hacen falta tres requisitos para garantizar un "juicio justo": garantizar la capacidad para evaluar la "calidad" de la evidencia (por ejemplo, verificando si las circunstancias en las que fue obtenida echan dudas sobre su confiabilidad o veracidad); garantizar la oportunidad de cuestionar la autenticidad de la evidencia u oponerse a su utilización; y compensación por las falencias en la confiabilidad de la evidencia mediante la introducción de prueba suplementaria[363].

Para el TEDH, como regla, un adecuado cumplimiento del art. 6 § 1 del CEDH demanda que la defensa tenga acceso a toda la evidencia que se encuentre en poder de los acusadores con respecto al imputado[364]. Más específicamente, el inciso § 3 (b) de la

[357] Cfr. GOODWIN, Will: "French supreme court dismisses legal challenge…", cit.
[358] Cfr. STEDH *in re*: *Gregačević v. Croacia*, § 49.
[359] Cfr. STEDH *in re*: *Ibrahim and Others v. Reino Unido* [pleno], § 250.
[360] Cfr. Tribunal Europeo de Derechos Humanos (TEDH), *Guía sobre el artículo 6 del Convenio Europeo de Derechos Humanos*, Consejo de Europa, publicado el 31/12/2021, pág. 7, § 2, con cita de STEDH *Mehmet Zeki Çelebi v. Turquía*, § 51.
[361] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., pág. 13.
[362] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., pág. 13 (citas omitidas).
[363] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., pág. 7. Con cita de lo expresado en los precedentes *Dragojevíc v. Croacia*, § 129 y *Prade v. Alemania* §§ 34/35.
[364] Cfr. STEDH *in re*: *Rowe and Davis v. Reino Unido* [pleno], § 60.

norma citada exige que se garantice al acusado el tiempo y las facilidades adecuadas para la preparación de su defensa, lo que importa la disponibilidad de todo lo que puede resultar "necesario" para enfrentar el juicio e influir sobre el resultado del proceso[365]. En orden a ello, el TEDH ha señalado que la "igualdad de armas" entre acusación y defensa constituye un elemento esencial de un juicio justo, y que, para que la misma exista, es preciso que a cada parte se le ofrezca la oportunidad de presentar su caso en condiciones que no la coloquen en desventaja con relación a su oponente[366]. A su vez, este elemento está estrechamente relacionado con otro aspecto fundamental del derecho a un juicio justo en procesos criminales, que radica en que el mismo sea de naturaleza "adversarial". Según el TEDH, para que el proceso adquiera dicho carácter, ambas partes deben tener el conocimiento y la posibilidad de opinar con respecto a los argumentos esgrimidos y la evidencia presentada por la contraparte[367], con el fin de influir en la decisión final del tribunal[368].

En este escenario, el TEDH ha considerado que el art. 6 del CEDH no sólo puede conculcarse cuando se impide el control de la prueba de cargo, sino también cuando se niega el acceso a evidencia potencialmente útil como prueba de descargo[369]. Por consiguiente, el tribunal continental ha señalado que, con independencia de cuál sea el sistema de investigación criminal vigente en el país, si el acusado opta por una defensa "activa", debe estar facultado para buscar y producir evidencia "en las mismas condiciones" que el acusador estatal[370].

Aplicadas a los casos objeto del presente trabajo, estas facultades reconocidas por el TEDH habilitan a las defensas a requerir la información necesaria para analizar cuestiones que se han mantenido en reserva con respecto a las tres operaciones reseñadas, como ser -por ejemplo- la naturaleza de los "implantes técnicos" empleados para hackear los sistemas de EncroChat y Sky ECC; las circunstancias en que se produjo la intrusión informática en esta última plataforma o la identidad del "tercer país" al que recurrió el FBI en para que librara la autorización judicial para interceptar los mensajes intercambiados a través del sistema An0m. En relación con esta cuestión, el TEDH ha prestado especial atención a la importancia del material no revelado a las defensas y su posible uso en el juicio penal, destacando que debe ser objeto de un proceso adversarial no sólo la prueba directamente relevante para acreditar los hechos del caso, *sino*

[365] Cfr. SSTEDH *in re*: *Connolly v. Reino Unido*, N° 27245/95; *Moiseyev v. Rusia*, N° 62936/00, § 220 y *Leas v. Estonia*, § 80.
[366] Cfr. SSTEDH *in re*: *Öcalan v. Turquía* [pleno], § 140; *Foucher v. Francia*, § 34 y *Faig Mammadov v. Azerbajian*, § 19.
[367] Cfr. STEDH *in re*: *Rowe and Davis v. Reino Unido* [pleno], § 60.
[368] Cfr. STEDH *in re*: *Brandstetter v. Austria*, § 67.
[369] Al respecto ver, por ejemplo, la STEDH dictada *in re*: *Mirilashvili v. Rusia*, N° 6293/04, en especial §§ 140, 150 y 151.
[370] Ver, *mutatis mutandis*, las SSTEDH *in re*: *Dombo Beheer B.V. v. Países Bajos*, Serie A N° 274, § 33; *Perić v. Croacia*, N° 34499/06, § 19 y *Mirilashvili v. Rusia*, § 225. Desde luego, el art. 6 del CEDH no exige que se le conceda a la defensa las mismas atribuciones que al acusador estatal para obtener evidencia (ver: *Mirilashvili* v *Rusia,* § 225), pero sí que tenga la chance de buscar y producir prueba "bajo las mismas condiciones" que la fiscalía (cfr., *mutatis mutandi*, las SSTEDH *in re*: *Dombo Beheer B.V. v. Países Bajos*, § 33, Serie A N° 274 y *Perić v. Croacia*, § 19). La igualdad de condiciones no implica concederle a la defensa facultades de registro y secuestro, pero los términos del art. 6 § 3 (d) demandan que la parte tenga pueda conducir una "defensa activa", por ejemplo convocando a sus propios testigos o requiriendo la entrega de evidencia (cfr. *Khodorkovskiy y Lebedev v. Rusia*, § 728).

también la que pueda vincularse con la admisibilidad, confiabilidad e integridad (completitud) de aquella[371]. El tribunal de mención ha expresado, además, que para considerar conculcado el principio de proceso adversarial *no hace falta determinar que la omisión de comunicar la existencia de un documento relevante haya perjudicado a la defensa*, toda vez que resulta concebible la existencia de una violación incluso en ausencia de perjuicio[372].

Ahora bien: como contrapartida, el TEDH ha dicho también que al evaluar si un juicio es o no justo, debe sopesarse *la importancia del interés público en la investigación y castigo del delito* que se trate. Ello, a efectos de prevenir que el derecho establecido en el art. 6 del CEDH se aplique de un modo que imponga "dificultades desproporcionadas" a la implementación, por parte de las agencias de orden público, de medidas efectivas para combatir al terrorismo y *otros delitos graves* en cumplimiento de sus obligaciones conforme los arts. 2, 3 y 5 § de la citada convención (aunque aclarando que la protección del interés público no puede justificar medidas que "extingan la propia esencia" de los derechos de los ciudadanos)[373]. Al igual que la anterior -aunque en sentido opuesto-, esta última salvedad del TEDH también pareciera ajustarse a la medida de los casos en estudio, en los que el fundamento invocado -por ejemplo- por las autoridades francesas para mantener en reserva la naturaleza del "implante técnico" utilizado contra EncroChat es, precisamente, la necesidad de preservar la eficacia de las herramientas utilizadas para enfrentarse al crimen organizado trasnacional.

En esa misma dirección, el TEDH ha señalado que el uso de técnicas especiales de investigación (en particular, las técnicas encubiertas o subrepticias) no supone, *per se*, una injerencia sobre el derecho a un juicio justo, a la vez que reconoció que el acceso a las mismas constituye una necesidad para los estados, sobre todo en relación con la persecución del crimen organizado y en casos de corrupción[374]. Según el tribunal constitucional europeo, la cuestión relativa a la admisibilidad de la evidencia resultante constituye una materia a ser reglada por la legislación nacional, mientras que su confiabilidad debe ser evaluada por los tribunales locales. En este escenario, lo que le compete al TEDH es analizar si el proceso en su conjunto ha sido justo y se han respetado los derechos de la defensa, lo cual ocurre cuando *se le brinda la oportunidad de cuestionar la autenticidad y confiabilidad de la evidencia* producida mediante el empleo de técnicas especiales de investigación[375].

En orden a ello, se toma en cuenta tanto la "calidad" de la evidencia como las circunstancias en que fue obtenida, *como así también si dichas circunstancias pueden generar dudas con respecto a su autenticidad y confiabilidad*[376]. Con respecto al primer

[371] Cfr., *mutatis mutandi*, SSTEDH *in re*: *Windisch v. Austria*, § 28; *Dowsett v. Reino Unido*, § 41; *Verhoek v. Países Bajos*, *Rowe and Davis v. Reino Unido* [pleno], § 66; *Mirilashvili v. Rusia*, § 200; *Leas v. Estonia*, § 81 y *Matanović v. Croacia*, § 161 (énfasis añadido).
[372] Cfr. TEDH, *Guía sobre el artículo 6…*, cit., pág. 33, § 159, con cita de la STEHD *Bajić v. Macedonia del Norte,* § 59 (énfasis añadido).
[373] Cfr. TEDH, *Guía sobre el artículo 6…*, cit., pág. 7, § 3, con cita de la STEDH *Ibrahim y otros v. Reino Unido* [pleno], § 252 (énfasis añadido).
[374] Cfr. TEDH, *Guía sobre el artículo 6…*, cit., pág. 45, § 232.
[375] Cfr. SSTEDH *in re*: *Jalloh v. Alemania* [pleno], §§ 95; *Khan v Reino Unido*, §§ 35 y 37; *Allan v. Reino Unido*, §§ 43 y 47; *Bykov v. Rusia* [pleno], § 95 y *Khodorkovskiy y Lebedev v. Rusia*, § 700 (énfasis añadido).
[376] Cfr. TEDH, *Guía sobre el artículo 6…*, cit., pág. 43, § 219.

factor, el TEDH señala que, si bien la inexistencia de prueba adicional que respalde a la obtenida a través de técnicas especiales de investigación no impide necesariamente que haya un "juicio justo", cuanto más confiable resulte la evidencia principal, menos necesidad existirá de que este complementada por otros elementos de prueba[377]. En los casos objeto de estudio, resulta evidente que el margen que se les está concediendo a las defensas para efectuar planteos vinculados a la "calidad" de la evidencia de cargo obtenida de los sistemas EncroChat, Sky ECC y An0m resulta acotadísimo, en la medida en que rige una confidencialidad casi absoluta con relación a las herramientas informáticas utilizadas y las circunstancias en las que fueron empleadas.

En ese orden de ideas, cabe tener presente que el TEDH también ha establecido que el derecho a la revelación completa de la evidencia en poder del Estado *no es absoluto*, sino que, por el contrario, incluso en procedimientos penales, el art. 6 § 1 del CEDH admite ciertas restricciones al proceso plenamente adversarial, siempre y cuando estas resulten "estrictamente necesarias" para satisfacer determinados intereses públicos, entre los cuales enumeró a la *seguridad nacional y la necesidad de mantener en reserva ciertos métodos policiales de investigación* (esto es, justamente los que se invocan en los casos objeto del presente trabajo). Así pues, aunque teniendo presente que, como regla general, el libre acceso a la información contenida en el expediente es considerada como un elemento importante para garantizar un juicio justo (y, como contrapartida, la negativa a conceder dicho acceso ha sido tenida en cuenta como evidencia de la infracción a la "igualdad de armas")[378], puede de todos modos exigirse al acusado que brinde razones específicas en sustento de su solicitud de obtener determinadas pruebas, cuya validez estará sometida al escrutinio de los tribunales locales[379].

Por añadidura, se aprecia que en casos que involucran información sensible con posibles implicancias para la seguridad nacional, el TEDH ha aplicado un estándar mucho menos exigente para valorar la decisión de mantener en reserva la evidencia[380], otorgándole un amplio margen de discrecionalidad a los jueces nacionales para decidir si corresponde aceptar o rechazar el pedido de divulgación de la defensa[381] pero reteniendo para sí la facultad de evaluar, en forma independiente, si las razones de seguridad nacional invocadas resultaban, o no, atendibles[382].

El mismo tribunal ha apuntado, sin embargo, que no puede haber un juicio justo si las dificultades causadas al imputado por la injerencia sobre sus derechos *no se encuentran "suficientemente contrabalanceadas"* en el proceso judicial[383], lo que, a simple vista, no pareciera estar sucediendo en los procesos seguidos contra los usuarios de EncroChat, Sky ECC y An0m. En esa dirección, el TEDH, aun reconociendo que no

[377] Cfr. SSTEDH *in re*: *Bykov v. Rusia* [pleno], § 90; *Beraru v. Rumania*, § 75; *Dragojević v. Croacia*, § 129; *Niţulescu v. Rumania*, § 46 y *Matanovic v. Croacia*, § 150; entre otros.
[378] Así, por ejemplo, en *Beraru v. Rumania*, § 70.
[379] Cfr. SSTEDH *in re*: *C.G.P. v. Países Bajos*, *Commission decision; Janatuinen v. Finlandia*, § 45; *Leas v. Estonia*, § 81 y *Matanović v. Croacia*, § 157.
[380] Ver, por ejemplo, STEDH *in re*: *P.G. and J.H. v. Reino Unido*, § 69.
[381] Cfr. STEDH *Mirilashvili v. Rusia*, § 202.
[382] Cfr. STEDH *Mirilashvili v. Rusia*, §§ 195/196.
[383] Cfr. SSTEDH *in re*: *Doorson v. Países Bajos*, § 70; *Jasper v. Reino Unido* [pleno], §§ 51/53; A. *y otros v. Reino Unido* [pleno], § 205; *Van Mechelen y otros v. Países Bajos*, § 58; *Paci v. Bélgica*, § 85; *Rowe y Davis v. Reino Unido* [pleno], §§ 54 y 61 y *Kennedy v. Reino Unido*, §§ 184 y 186 (énfasis añadido).

existe en la CEDH una regla general que prohíba en términos absolutos fundar una condena en evidencia no examinada en un proceso adversarial[384], aclaró que dicha prueba debe ser tratada con "extremo cuidado"[385] y afirmó, en una serie de fallos, que cuando la condena se basa en grado decisivo en esos elementos, la restricción a los derechos de la defensa es tal que resulta incompatible con las garantías consagradas en el art. 6 del CEDH[386].

Evidentemente, en casos en los que la evidencia sobre la que gira la controversia nunca ha sido revelada -como parece ser el caso en los que aquí se analizan-, resulta imposible para el TEDH sopesar el interés público invocado contra el del imputado en obtener el material, motivo por el cuál su análisis debe centrarse en el proceso de toma de decisiones que culminó con la resolución de mantenerlo en reserva, a fin de determinar si se cumplió con la exigencia de ofrecer un procedimiento adversarial con igualdad de armas y se introdujeron salvaguardas para proteger los intereses del acusado[387]. A tal efecto, la jurisprudencia del TEDH demanda que se tome en consideración la relevancia del material reservado y el uso que se le ha dado en el juicio[388], en especial si se ha considerado el impacto que la evidencia para obtener una condena a la luz de los argumentos de la defensa[389]. Sin duda, este último aspecto guarda enorme relevancia en los casos objeto de análisis, en los que la prueba obtenida a partir de las operaciones referidas a los sistemas EncroChat, Sky ECC y An0m es, por lo general, la piedra basal en que se apoya la acusación contra los imputados.

Lo que si ha rechazado el TEDH es la legitimidad de un procedimiento en que esté a cargo de los acusadores decidir lo que puede o no ser relevante en el caso (así como sopesar la importancia que puede tener para la defensa con el interés público en mantener la información confidencial), sin que existan recaudos en el procedimiento tendientes a garantizar los derechos de los acusados. En opinión del tribunal, un procedimiento de esas características no puede respetar los requisitos emergentes del art. 6 § 1 del CEDH[390]. Al menos en lo que respecta al único caso sobre el que existe información sobre el punto (EncroChat), se aprecia que la decisión no quedó librada a la decisión de la parte acusadora sino que fue adoptada por el juez, que optó por no iniciar el procedimiento previsto en la normativa procesal francesa para requerir el levantamiento del "secreto de defensa" en orden al "implante técnico", con sustento en la existencia de un informe producido por el experto gubernamental (decisión cuya constitucionalidad, como ya se señaló[391], fue respaldada por el Consejo Constitucional de Francia, aunque luego, como se ha visto, la existencia del "certificado de autenticidad" ha sido puesta en duda).

---

[384] Cfr. SSTEDH *in re*: *Isgrò v. Italia*, § 34; *Lüdi* v. *Suiza*, § 47 y *Asch v. Austria*, §§ 28 y ss.
[385] Cfr. STEDH *S.N. v. Suiza*, N° 34209/96, § 53.
[386] Ver SSTEDH *in re*: *Unterpertinger v. Austria*, §§ 31/33; *Saïdi v. Francia*, §§ 43/44 y *Van Mechelen y otros v. Países Bajos*, § 55 (citados en *Mirilashvili v. Rusia*, § 216).
[387] Cfr. SSTEDH *in re*: *Dowsett v. Reino Unido*, §§ 42-43; *Leas v. Estonia*, § 78 y *Matanovic v. Croacia*, § 153.
[388] Cfr. SSTEDH *in re*: *Jasper v. Reino Unido* [pleno], §§ 54/55 y *M v. Países Bajos*, § 69.
[389] Cfr. TEDH, *Guía sobre el artículo 6…*, cit., pág. 37, § 180, con cita de *Rowe and Davis v. Reino Unido* [pleno], § 66.
[390] Cfr. SSTEDH *in re*: *Rowe and Davis v. Reino Unido* [pleno], § 63; *Natunen v. Finlandia*, §§ 47/49 y *Matanović v. Croacia*, §§ 158, 181/182.
[391] Ver *supra*, § 5.2).

Si bien lo concerniente a la problemática de la evidencia digital es una cuestión relativamente nueva, el TEDH ha establecido un vínculo entre el principio de igualdad de armas y el testimonio de expertos en una serie de precedentes anteriores, cuya doctrina resulta de aplicación analógica[392]. Así pues, conforme surge de dicha doctrina, la circunstancia de que se haya introducido en el proceso el reporte de un experto (en favor de la acusación) sin participación de la defensa, como tal, no es problemática *en la medida en que esta última parte tenga la oportunidad de cuestionar el reporte* ante el tribunal de mérito[393]. En efecto, el tribunal continental de derechos humanos ha señalado que cuando -como ocurrió en el presente caso- se decide que es necesaria la intervención de un experto para validar la confiabilidad de la evidencia, la defensa debe contar con la posibilidad de interrogar al experto y cuestionar sus conclusiones durante el juicio. Si bien el TEDH ha entendido que la lectura conjunta del art. 6 § 1 y § 3 (d) no establece un derecho absoluto a producir determinado tipo de prueba de expertos[394], existe abundante jurisprudencia en el sentido de garantizarle a la parte el derecho a examinar y cuestionar no sólo el informe técnico sino también la credibilidad de los que lo elaboraron a través de un interrogatorio directo[395]. Sin embargo, se deja librada a la discreción del juez nacional la decisión de aceptar o rechazar el testimonio de expertos[396], conforme el principio de economía procesal, quedando en cabeza de la defensa la carga de justificar en forma objetiva la necesidad de una segunda opinión experta[397].

En relación con la credibilidad de los expertos estatales, el TEDH ha señalado que la ausencia de neutralidad de un experto designado por un juez puede dar lugar a una violación a la "igualdad de armas"[398]. En orden a ello, aunque el tribunal ha aclarado que la circunstancia de que un testigo pertenezca a una dependencia estatal o una fuerza de seguridad, por si sola, no alcanza para demostrar parcialidad, sino que es preciso que las dudas sobre su neutralidad estén objetivamente justificadas[399], explicó también que, para confirmar o descartar la parcialidad invocada, deben tomarse en consideración factores tales como la posición del experto en el proceso y el rol que le tocó jugar en los procedimientos relevantes[400].

Resulta ilustrativo, en tal sentido, el análisis realizado por el TEDH en el caso *Khodorkovskiy and Lebedev v. Russia*, en el que, a partir del hecho de que los expertos intervinientes habían sido contratados por la acusación al comienzo de la investigación y llevaron a cabo su tarea en la sede del Ministerio Público Fiscal sin intervención de las defensas, consideró que su posición era más cercana a la de un "testigo de la acusación". Esto es, un cuadro muy similar al que se aprecia, cuanto menos, en el caso EncroChat, en el que el experto que (supuestamente) elaboró el informe validando la confiabilidad del mecanismo utilizado para capturar los mensajes *no fue elegido por el magistrado*

[392] Cfr. STOYKOVA, Radina: "The right to a fair trial as conceptual framework…", cit., pág. 13.
[393] Cfr. STEDH *in re*: *Khodorkovskiy y Lebedev v. Rusia*, § 704.
[394] Cfr. STEDH *Mirilashvili v. Rusia*, § 191.
[395] Cfr. SSTEDH *in re*: *Brandstetter v. Austria*, § 42; *Doorson v. Países Bajos*, §§ 81/82 y *Mirilashvili v. Rusia*, § 158.
[396] Cfr. STEDH *in re*: *H. v. Francia*, §§ 61 y 70.
[397] Cfr. STEDH *in re*: *Devinar v. Eslovenia*, §§ 48, 51 y 56/58.
[398] Cfr. SSTEDH *in re*: *Bönisch v. Austria*, §§ 30/35 y *Brandstetter v. Austria*, § 33.
[399] En las SSTEDH dictadas *in re*: *Mirilashvili v. Rusia*, § 176 y *Brandstetter v. Austria*, § 44.
[400] Cfr. STEDH *in re*: *Bönisch v. Austria*, §§ 31/35.

actuante, sino que se trató de un funcionario estatal perteneciente a la dependencia designada por ley para certificar el adecuado funcionamiento de una herramienta informática gubernamental secreta.

En ese marco, en *Khodorkovskiy and Lebedev v. Russia*, el TEDH concluyó que la decisión del Estado denunciado de no permitirle a la defensa interrogar los expertos de la acusación ni tampoco presentar peritos propios que pudiesen cuestionar las conclusiones a las que aquellos arribaron importó una infracción al derecho a "igualdad de armas". Ello, debido a que generó un desequilibrio entre la acusación y la defensa, al negarle a esta última la posibilidad de confrontar la credibilidad de los expertos de la acusación[401]. En sustento de esta apreciación, el tribunal continental de derechos humanos explicó que -a diferencia de lo que ocurre con los testigos de la defensa- no le es exigible al acusado demostrar la importancia de un testigo de cargo, puesto que, si los acusadores deciden que determinada persona es una fuente relevante de información y se apoyan en su testimonio en el juicio para procurar un veredicto de culpabilidad, debe presumirse que su presencia e interrogatorio en el debate es necesaria[402].

En esa misma dirección, el TEDH aclaró también que la circunstancia de que se haya agregado al expediente el informe escrito del experto no torna innecesario su testimonio en el debate, ya que de lo contrario no habría necesidad de interrogar a ningún testigo que haya aportado información por escrito durante la investigación preliminar. Destacó, al respecto, que incluso si no se aprecian inconsistencias notorias en el informe, el interrogatorio del experto puede revelar posibles conflictos de intereses, carencias en el material que tuvo a su disposición para trabajar o defectos en la metodología empleada para elaborar su reporte[403]. Asimismo, el TEDH estableció en el caso *Mantovelli*[404] que la facultad de cuestionar la confiabilidad de la evidencia aportada por los expertos no sólo incluye la oportunidad de participar en su interrogatorio, sino también de acceder al material en que se funda su reporte.

En este escenario, resulta claro que, conforme los estándares establecidos por el TEDH, no puede privarse a la defensa -ni siquiera en virtud de lo previsto en las reglas procesales sobre admisibilidad de evidencia vigentes a nivel local- de la oportunidad de cuestionar efectivamente las conclusiones del experto estatal, ya sea a través de opiniones o informes alternativos. Por consiguiente, aunque el principio de "juicio justo" no imponga, como regla, que los tribunales deban requerir la opinión de un experto solo porque una parte así lo solicite[405], la negativa a permitir una evaluación alternativa o independiente de la evidencia producida por el experto estatal puede considerarse una violación al art. 6 § 1 del CEDH[406].

Por otra parte, habida cuenta de lo dificultoso que puede resultar cuestionar las conclusiones del experto gubernamental sin la intervención de otro experto en el mismo campo, el TEDH ha establecido que, a los efectos de garantizar el derecho de la defensa

[401] Cfr. STEDH *in re*: *Khodorkovskiy y Lebedev v. Rusia*, §§ 730 y 735.
[402] Cfr. STEDH *in re*: *Khodorkovskiy y Lebedev v. Rusia*, § 712.
[403] Cfr. STEDH *in re*: *Khodorkovskiy y Lebedev v. Rusia*, § 714.
[404] Ver: *Mantovelli v. Francia*, §§ 33/34.
[405] Cfr. STEDH *in re*: *Khodorkovskiy y Lebedev v. Rusia*, § 721.
[406] Cfr. SSTEDH *in re*: *Stoimenov v. ex República Yugoslava de Macedonia*, § 38 y *Matytsina v. Rusia*, § 169.

a controlar la prueba de cargo, no resulta suficiente con encomendar -ante un eventual pedido de esa parte- un nuevo informe a otro especialista estatal, sino que es preciso concederle la oportunidad de introducir su propia evidencia técnica[407]. De lo que se sigue, a su vez, que si se le niega dicha posibilidad a la defensa, ello podría suponer una violación a la norma antes mencionado[408]. Lo mismo ocurre *si se impide la divulgación de los detalles técnicos en los que se sustenta el informe del experto estatal*, sin los cuáles la parte puede verse imposibilitada de cuestionar sus conclusiones[409] y llevar a cabo un análisis verdaderamente "adversarial" sobre el programa utilizado para recolectar la evidencia.

Contrastando los parámetros reseñados en los párrafos precedentes con las circunstancias de los casos EncroChat, Sky ECC y An0m, parece evidente que, por más que no exista hasta el momento ningún informe técnico que siembre dudas sobre la autenticidad de la evidencia recolectada mediante el hackeo del sistema[410], la ausencia de precedentes respecto del empleo de la herramienta empleada para interceptar los mensajes (cuya identidad, naturaleza y funcionamiento se desconocen) impide dar por cierto, sin más, que la misma garantice la autenticidad y completitud de la evidencia informática obtenida. Y ello, sin perjuicio de que -al menos en lo tocante a EncroChat- pueda existir un documento que certifique su confiabilidad (aun cuando su efectiva existencia haya sido puesta en duda[411]), desde que tampoco se han divulgado los fundamentos técnicos en los que dicha certificación encontraría sustento. Por consiguiente, el hecho de que las condenas que ahora mismo están dictándose con respecto a los usuarios de estos sistemas de comunicación se funden casi en exclusividad en la prueba conseguida de este modo, sin que las partes tengan la oportunidad de verificar si efectivamente se utilizó una herramienta idónea para asegurar la confiabilidad de la evidencia, pareciera contradecir los estándares fijados por el TEDH sobre el derecho a la igualdad de armas.

6. BIBLIOGRAFÍA.

ABELSON, Harold / ANDERSON, Ross / BELLOVIN, Steven M. / BENALOH, Josh / BLAZE, Matt / DIFFIE, Whitfield / GILMORE, John / GREEN, Matthew / LANDAU, Susan / NEUMANN, Peter G. / RIVEST, Ronald L. / SCHILLER, Jeffrey I. / SCHNEIER, Bruce / SPECTER, Michael / WEITZNER, Daniel J., *Keys under doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology Science and Artificial Intelligence Laboratory, publicado el 6/7/2017.

AMSTER, Haley / DIEHL, Brett: "Against geofences", en Stanford Law Review, Vol. 74, 2022, págs. 385/445.

[407] Cfr. STEDH *in re*: *Khodorkovskiy y Lebedev v. Rusia*, § 731.
[408] Cfr. SSTEDH *in re*: *Stoimenov v. ex República Yugoslava de Macedonia*, §§ 38 y *Mirilashvili v. Rusia*, § 190.
[409] Cfr. STEDH *Kartoyev y otros v. Rusia*, §§ 71/73 (énfasis añadido).
[410] El cual, vale aclararlo, difícilmente aparezca, desde que la ausencia casi total de información respecto a cómo se llevaron a cabo las operaciones o qué características tienen las herramientas informáticas utilizadas hace casi imposible cuestionar, con un mínimo de sustento, la evidencia resultante.
[411] Al respecto, ver *supra*, § 5.2.

BAKER, Stewart / KLEHM, Bryce: "Legal Tetris and the FBI's An0m program", en Lawfare, publicado el 22/7/2021, obtenido en: https://www.lawfareblog.com/legal-tetris-and-fbis-anom-program.

BBC News: An0m: Hundreds arrested in massive global crime sting using messaging app", publicado el 8/6/2021, obtenido en: https://www.bbc.com/news/world-57394831.

BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan, "Going bright: Wiretapping without weakening communications infrastructure", en IEEE Security & Privacy, vol. 11, N° 1, 2013, págs. 62/72.

BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan: "Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet", en Northwestern Journal of Technology and Intellectual Property, vol. 12, nro. 1, 2014, págs. 1/64.

BELLOVIN, Steven M. / BLAZE, Matt / LANDAU, Susan / OWSLEY, Brian: "Seeking the source: Criminal defendants' constitutional right to source code", en Ohio State Law Journal, Vol. 17, N° 1, 2021, págs. 1/73.

BIDDLE, Sam, "Leaked NSA malware is helping hijack computers around the world", en The Intercept, publicado el 12/5/2017, obtenido en: https://theintercept.com/2017/05/12/the-nsas-lost-digital-weapon-is-helping-hijack-computers-around-the-world/.

BLANCO, Hernán, *Tecnología informática e investigación criminal*, La Ley, Buenos Aires, 2020.

BLANCO, Hernán: "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre", en InDret, Vol. 1/2021, 2021, págs. 431/501.

BOFFEY, Daniel: "Colombia's cartels target Europe with cocaine, corruption and torture", en The Guardian, publicado el 11/4/2021, obtenido en: https://www.theguardian.com/world/2021/apr/11/colombias-cartels-target-europe-with-cocaine-corruption-and-torture.

BOJARSKI, Kamil, "Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations", en The European Review of Organized Crime, vol. 2, N° 2, 2015, págs. 25/50.

BUENO DE LA MATA, Federico: "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el Fortalecimiento de las Garantías Procesales y la Regulación de las Medidas de Investigación Tecnológica", en Diario La Ley, N° 8627, Sección Doctrina, 19/10/2015.

CAMPBELL, Duncan: "Two convicted in the first murder plot case involving Encrochat messaging system", en The Guardian, publicado el 14/3/2022, obtenido en: https://www.theguardian.com/world/2022/mar/14/two-guilty-of-james-bond-gun-plot-in-encrochat-conviction.

CAPRONI, Valerie: *Statement of the General Counsel of the Federal Bureau of Investigations before the House Judiciary Committee, Subcommitee on Crime, Terrorism, and Homeland Security*, Washington D.C., publicado el 17/2/2011.

COLLERAN, Kevin: "French legal challenge over EncroChat cryptophone hack could hit UK prosecutions", en Techlive, publicado el 8/5/2021.

CORFIELD, Gareth: "Encrochat hack evidence wasn't obtained illegaly, High Court of England and Wales rules – Trial judges will decide whether to admit it", en The Register, publicado el 13/11/2020, obtenido en: https://www.theregister.com/2020/11/13/encrochat_hack_judicial_review_judgment/.

COX, Joseph: "How police secretly took over a global pone network for organized crime", en Motherboard. Tech by VICE, publicado el 2/7/2020, obtenido en: https://www.vice.com/en_us/article/3aza95/how-police-took-over-encrochat-hacked.

COX, Joseph: "Court throws out messages obtained by FBI honeypot phone company An0m", en Motherboard. Tech by VICE, publicado el 30/11/2021, obtenido en: https://www.vice.com/en/article/pkppqk/court-throws-out-messages-from-anom-finland-spain.

COX, Joseph: "FBI honeypot company An0m shipped over 100 phones to the United States", en Motherboard: Tech by Vice, publicado el 12/1/2022, obtenido en: https://www.vice.com/en/article/epxp8w/fbi-anom-shipped-100-phones-united-states.

COX, Joseph: "A European country helped the FBI intercept An0m messages, but it wants to remain hidden", en Motherboard: Tech by Vice, publicado el 3/6/2022, obtenido en: https://www.vice.com/en/article/qjbggq/anom-third-country-europe-european-union-fbi.

DE HERT, Paul / BOULET, Gertjan, "Cloud computing and trans-border law enforcement access to private sector data. Challenges to sovereignty, privacy and data protection", en AA.VV., *Big data and privacy. Making ends meet*, Future of Privacy Forum & Stanford Center for Internet & Society, 2013, págs. 23/26.

DE LOS SANTOS, Germán: "Casi sin escuchas, los detectives van a la caza de celulares", en La Nación, publicado el 2/5/2020, obtenido en: https://www.lanacion.com.ar/seguridad/tecnologia-casi-sin-escuchas-los-detectives-van-a-la-caza-de-celulares-nid2360666.

DE ZAN, Tomasso, "E-evidence and cross border data requests in Italy", en AA.VV., *EUnited against crime: Improving criminal justice in European Union cyberspace*, Instituti Affari Internazionali, 2016, Roma, págs. 42/59.

DONOHUE, Laura K.: "The Fourth Amendment in a digital world", en New York University Annual Survey of American Law, Vol. 71, 2017, págs. 533/685.

DORTA, Irene: "La Audiencia Nacional avala a un juez francés que intervino el 'chat de los narcos'", en La Razón (España), publicado el 8/12/2021, obtenido en: https://www.larazon.es/espana/20211207/54rcryfuzzeczbjuf3zpv5tine.html.

Español News: "Francia dice que el 'secreto de defensa' en las operaciones de vigilancia policial es constitucional", publicado el 9/4/2022, obtenido en: https://espanol.news/francia-dice-que-el-secreto-de-defensa-en-las-operaciones-de-vigilancia-policial-es-constitucional/.

EUROJUST: *Cybercrime Judicial Monitor*, Eurojust Limited, N°. 2, noviembre 2016.

EUROJUST: "New major interventions to block encrypted communications of criminal networks", publicado el 10/3/2021

European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, *Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices*, European Union, 2017.

EUROPOL "Dismantling of an encryted network sends shockwaves through organized crime groups across Europe", publicado el 2/7/2020, obtenido en: https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

EUROPOL / EUROJUST, *Third report of the observatory function on encryption* (joint report), European Commision, 2021.

Fuentitech.com: "Berlin court overturned ban on EncroChat evidence in criminal trials", publicado el 3/9/2021, obtenido en: https://fuentitech.com/berlin-court-overturned-ban-on-encrochat-evidence-in-criminal-trials/217620/.

GABILONDO, Pablo: "El WhatsApp secreto que usaban los narcos se vuelve en su contra ante la justicia", en El Confidencial, publicado el 26/1/2022, obtenido en: https://www.elconfidencial.com/espana/2022-01-26/encrochat-whatsapp-narcos-audiencia-nacional_3363806/.

GELLMAN, Barton / POITRAS, Laura, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", en The Washington Post, publicado el 7/6/2013.

GELLMAN, Barton / SOLTANI, Ashkan, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", en The Washington Post, publicado el 30/10/2013.

GHAPPOUR, Ahmed, "Searching places unknown: Law enforcement jurisdiction on the dark web", en Stanford Law Review, vol. 69, N° 4, 2017, págs. 1075/1136.

GOODWIN, Bill: "Encrochat: Appeal court finds 'digital phone tapping' admissible in criminal trials", en Computer Weekly, publicado 6/2/2021, obtenido en: https://www.computerweekly.com/news/252495964/EncroChat-Appeal-court-finds-digital-phone-tapping-admissible-in-criminal-trials.

GOODWIN, Bill: "Police cracks world's largest cryptophone network as criminals swap EncroChat for Sky ECC", en Computer Weekly, publicado el 10/3/2021, obtenido en: https://www.computerweekly.com/news/252497565/Police-crack-worlds-largest-cryptophone-network-as-criminals-swap-EncroChat-for-Sky-NCC.

GOODWIN, Bill: "Berlin court finds EncroChat intercept evidence cannot be used in criminal trials", en Computer Weekly, publicado el 3/7/2021, obtenido en: https://www.computerweekly.com/news/252503524/Berlin-court-finds-EncroChat-intercept-evidence-cannot-be-used-in-criminal-trials.

GOODWIN, Bill: "Dutch prosecutor ordered to give evidence on EncroChat hack", en Computer Weekly, publicado el 13/7/2021, obtenido en: https://www.computerweekly.com/news/252503908/Dutch-prosecutor-ordered-to-give-evidence-on-EncroChat-hack.

GOODWIN, Bill: "French Supreme Court raises constitutional questions over EncroChat hacking secrecy", en Computer Weekly, publicado el 3/2/2022, obtenido en: https://www.computerweekly.com/news/252512850/French-Supreme-Court-raises-constitutional-questions-over-EncroChat-hacking-secrecy.

GOODWIN, Bill: "How diplomatic immunity silenced the prosecutor who coordinated Sweden's EncroChat probe", en Computer Weekly, publicado el 10/2/2022, obtenido en: https://www.computerweekly.com/news/252513203/How-diplomatic-immunity-silenced-the-prosecutor-who-coordinated-Swedens-EncroChat-probe.

GOODWIN, Bill: "French Supreme Court rejects EncroChat verdict after lawyers question secrecy over hacking operation", en Computer Weekly, publicado el 12/10/2022, obtenido en: https://www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy.

GOODWIN, Will: "French supreme court dismisses legal challenge to EncroChat cryptophone evidence", en Computer Weekly, publicado el 6/9/2023, obtenido en: https://www.computerweekly.com/news/366551078/French-supreme-court-dismisses-legal-challenge-to-EncroChat-cryptophone-evidence.

GONZÁLEZ PASCUAL, María Isabel: "El Tribunal Constitucional Federal Alemán ante la incompatibilidad con los derechos fundamentales de la normativa nacional de origen europeo de prevención de delitos", en Revista de Derecho Contemporáneo Europeo, N° 34, Madrid, 2009, págs. 945/966.

HENNESSEY, Susan, "The elephant in the room: Addressing child exploitation and going dark", en Hoover Institution, Stanford University, Aegis Paper Series, N° 1701, 2017.

IBÁÑEZ LÓPEZ-POZAS, Fernando L.: "De las masivas interceptaciones de datos a las masivas vulneraciones de derechos fundamentales: la respuesta del Tribunal de Justicia de la Unión Europea", en Diario La Ley, N° 10033, Sección Tribuna, Wolters Kluwer, 21/3/2022 (citado de documento electrónico obtenido en: https://mpr.bage.es/cgi-bin/koha/opac-detail.pl?biblionumber=221254&query_desc=an%3A%2222866%22).

International Association of Chiefs of Police (IACP), *Data, privacy and public safety: A law enforcement perspective on the challenges of gathering electronic evidence*, IACP, 2015 Summit Report.

KERR, Orin S. / MURPHY, Sean D., "Government hacking to light the dark web. What risks to international relations and international law?", en Stanford Law Review Online, vol. 70, 2017, págs. 58/69.

KERR, Orin S. / SCHNEIER, Bruce, "Encryption workarounds", en Georgetown Law Journal, vol. 106, N° 4, 2018, págs. 989/1019.

KLAUBERT, David: "Crypto service of the FBI: An0m chats can be used in court according to the Frankfurt District Court", en Teller Report, publicado el 25/1/2022, obtenido en: https://www.tellerreport.com/life/2022-01-25-crypto-service-of-the-fbi--anom-chats-can-be-used-in-court-according-to-the-frankfurt-district-court.SJmtuhpTK.html.

LINDSAY, Jon R., "Stuxnet and the limits of cyber warfare", en Security Studies, vol. 22, N° 3, 2013, págs. 365/404.

MARKS, Joseph: "Encrypted messaging apps present a dilemma for law enforcement", en The Washington Post, publicado el 18/11/2021, obtenido en: https://www.washingtonpost.com/politics/2021/11/18/encrypted-messaging-apps-present-dilemma-law-enforcement/.

MILLER, Greg: "The intelligence coup of the century", en The Washington Post, publicado el 11/2/2020, obtenido en: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

MONROY, Matthias: "German An0m investigations: The mysterious EU third state", en Security Architectures in the EU, publicado el 4/4/2022, obtenido en:

https://digit.site36.net/2022/04/04/german-anom-investigations-the-mysterious-eu-third-state/.

Motherboard: "EncroChat lawyers say clients haven't had fair trials", publicado el 18/2/2022, obtenido en: https://nationalcybersecuritynews.today/encrochat-lawyers-say-clients-havent-had-fair-trials-emailsecurity-phishing-ransomware/.

Nord News: "Criticism of the EncroChat evidence is growing", publicado el 23/3/2021, obtenido en: https://nord.news/2021/03/23/criticism-of-the-enchrochat-evidence-is-growing/.

NOSSITER, Adam: "When police are hackers: Hundreds charged as encrypted network is broken", en *The New York Times*, publicado el 2/7/2020, obtenido en: https://www.nytimes.com/2020/07/02/world/europe/encrypted-network-arrests-europe.html).

ORTIZ PRADILLO, Juan Carlos, "El 'remote forensic software' como herramienta de investigación contra el terrorismo", en ENAC, E-Newsletter en la lucha contra el cibercrimen, Cibex, 2009, N° 4, págs. 1/9.

PARKIN, Simon: "'Every message was copied to the police': The inside story of the most daring surveillance sting in history", en The Guardian, publicado el 11/9/2021, obtenido en: https://www.theguardian.com/australia-news/2021/sep/11/inside-story-most-daring-surveillance-sting-in-history.

PELROTH, Nicole / LARSON, Jeff / SHANE, Scott, "NSA able to foil basic safeguards of privacy on web" en The New York Times, publicado el 5/9/2013.

ROYER, Sofie / DEWITTE, Pierre: "Drawing the line between privacy by design and criminal liability", Kuleuven Law, publicado el 9/3/2021, obtenido en: https://www.law.kuleuven.be/citip/blog/drawing-the-line-between-privacy-by-design-and-criminal-liability/.

SALT, Marcos, "Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina", en Revista de Derecho Penal y Procesal Penal, Buenos Aires, Abeledo-Perrot, vol. 2013-6, págs. 1125/1134.

SALT, Marcos G.: "'Hacking legal' como medio de investigación en el proceso penal: Breves reflexiones sobre los desafíos jurídicos derivados de su aplicación trasnacional", en AAVV, *La investigación penal en el entorno digital. Estudios sobre el impacto de las nuevas tecnologías digitales en el proceso penal*, Hammurabi, Buenos Aires, 2023, págs. 251/300.

SEITZ, Nicolai, "Transborder search: A new perspective in law enforcement?", en Yale Journal of Law and Technology, vol. 7, N° 1, 2005, págs. 23/50.

ŠKORVÁNEK, Ivan / KOOPS, Bert-Jaap / CLAYTON NEWELL, Bryce / ROBERTS, Andrew: "My computer is my castle' New privacy frameworks to regulate police hacking", en Brigham Young University Law Review, Vol. 2019, N° 4, 2019, págs. 997/1081.

SLOBOGIN, Christopher: "Government dragnets", en Law and Contemporary Problems, Vol. 73, N°3, 2010, págs. 101/143.

SOMMER, Peter: "Evidence from hacking: A few tiresome problems", en Forensic Science International: Digital Investigation, Vol. 40, 2022.

STOYKOVA, Radina: "The right to a fair trial as conceptual framework for digital evidence rules in criminal investigations", en Computer Law & Security Review", Vol 49, 2023, págs. 1/26.

SYMONDS, Tom: "Encrochat: Secret network messages can be used in court, judges rule", en BBC News, publicado el 5/2/2021, obtenido en: https://www.bbc.com/news/uk-55953247.

Tech News Terminal: "Swedish Court Docket finds ambiguities in hacked EncroChat cryptophone proof", publicado el 11/5/2021, obtenido en: https://technewsterminal.com/swedish-court-docket-finds-ambiguities-in-hacked-encrochat-cryptophone-proof/.

The Guardian: "Dutch arrests after discovery of 'torture chamber' in sea containers", publicado el 7/7/2020, obtenido en: https://www.theguardian.com/world/2020/jul/07/dutch-police-arrest-six-men-after-discovery-of-torture-chamber.

The Guardian: "Police raids across Europe after encrypted phone network shut down", publicado el 10/3/2021, obtenido en: https://www.theguardian.com/technology/2021/mar/10/police-raids-across-europe-after-encrypted-phone-network-shut-down.

Tribunal Europeo de Derechos Humanos (TEDH), *Guía sobre el Artículo 8 del Convenio Europeo de Derechos Humanos*, Consejo de Europa, publicado el 31/8/2020

Tribunal Europeo de Derechos Humanos (TEDH), *Guía sobre el artículo 6 del Convenio Europeo de Derechos Humanos*, Consejo de Europa, publicado el 31/12/2021.

United Nations Office on Drugs and Crime (UNODC), *Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies*, junio 2014.

US Department of Justice (DOJ): "Sky Global executive and associate indicted for providing encrypted communication devices to help international drug traffickers avoid law enforcement", publicado el 12/3/2021.

VANCE Jr., Cyrus R. / MOLINS, François / LEPPARD, Adrian / ZARAGOZA, Javier, "When phone encryption blocks justice", NY Times OpEd., publicada el 11/8/2015.

VILASAU, Mónica: "La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad", en IDP. Revista de Internet, Derecho y Política. Nº. 3, UOC, 2006, págs. 1/15.

WAHL, Thomas: "Dismantled encryption networks: German courts confirmed use of evidence from EncroChat surveillance", en Eucrim, publicado el 20/3/2021, obtenido en: https://eucrim.eu/news/dismantled-encryption-networks-german-courts-confirmed-use-of-evidence-from-encrochat-surveillance/.

WAHL, Thomas: "Federal Court of Justice confirms use of evidence in EncroChat cases", en Eucrim, publicado el 19/5/2022, obtenido en: https://eucrim.eu/news/germany-federal-court-of-justice-confirms-use-of-evidence-in-encrochat-cases/#:~:text=After%20several%20Higher%20Regional%20Courts,first%20supreme%20court%20judgment%20in.

WOLFF, Josephine: "One of the most unusual cybersecurity stories of the year is getting more complicated", en Slate, publicada el 3/12/2021, obtenida en: https://slate.com/technology/2021/12/fbi-fake-encrypted-messaging-platform-anom-sky-global.html.

ZARAGOZA TEJADA, Javier Ignacio: "Operaciones encubiertas digitales y convencionales. Un análisis desde la perspectiva de los derechos fundamentales y del derecho comparado", en AAVV, *La investigación penal en el entorno digital. Estudios sobre el impacto de las nuevas tecnologías digitales en el proceso penal*, Hammurabi, Buenos Aires, 2023, págs. 209/249.

ZHUANG, Yan / PELTIER, Elian / FEUER, Alan: "The criminals thought the devices were secure, but the seller was the FBI", en The New York Times, publicado el 8/6/2021, obtenido en: https://www.nytimes.com/2021/06/08/world/australia/operation-trojan-horse-anom.html.