REVISTA PENSAMIENTO PENAL

VOL. 2 | NÚM. 4 | 2025

ISSN 1853 - 4554

Revista Pensamiento Penal es una revista electrónica de la Asociación Pensamiento Penal www.pensamientopenal.com.ar

ISSN 1853 - 4554

Las opiniones expresadas en este documento son exclusiva responsabilidad de sus autores y no necesariamente representan la posición de la Asociación Pensamiento Penal.

Índice

Volumen 2
Número 4 – 2025

Artículos

Cartapacio ~ Reseñas bibliográficas y jurisprudencia comentada

Columnas & Opinión

Artículos

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 4 – 2025, págs. 1–15
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/wev12245

El agente digital encubierto y el acceso transfronterizo de datos

Julia M. Torrez[1]

Resumen

Este trabajo explora el uso de nuevas tecnologías por parte de organizaciones criminales y el impacto de los avances tecnológicos en la labor de las fuerzas de seguridad para prevenir y castigar delitos graves como el tráfico de drogas, armas, la trata de personas, la pedofilia y el terrorismo. Se introduce el concepto de agente digital encubierto, una figura que permite a los investigadores infiltrarse en redes criminales en el ámbito digital, analizando sus implicancias legales y éticas. El documento examina la operación *EncroChat* y *Trojan Shield*, que expusieron cómo las fuerzas de seguridad desarticularon redes criminales transnacionales mediante la infiltración de dispositivos de comunicación encriptados. Se aborda la problemática del acceso transfronterizo de datos, destacando la cooperación internacional necesaria para combatir delitos en el ciberespacio y el marco normativo que lo respalda, como el *convenio de Budapest*. Finalmente, se discuten las implicancias del agente encubierto digital en la legislación argentina, señalando su regulación en la provincia de Mendoza.

Sumario

Palabras clave

convenio de Budapest – agente digital encubierto – cibercrimen – crimen organizado transnacional – bitcoin

[1] Abogada (Universidad Nacional del Litoral); Diploma de Experto en ciberdelincuencia y tecnologías aplicadas a la investigación (Universidad Austral); maestrando en Derecho penal (Universidad de Palermo); abogada litigante matrícula del Colegio de Abogados de Rosario L° XXXVI-F° 543; jefa Sucursal Rosario Norte de la Empresa Provincial de la Energía de Santa Fe. Correo electrónico: jutorrez8@gmail.com

1. Contexto

En los últimos veinticinco años, la evolución de las tecnologías informáticas de comunicación, en particular el desarrollo de internet ha traído aparejado un problema grave para los investigadores penales y por tanto a los Estados para lograr prevenir y eventualmente castigar delitos, especialmente aquellos graves tales como el tráfico y comercialización de estupefacientes, la trata de personas, la compra venta de armas, la pedofilia y el terrorismo.

Por lo cual el viejo adagio popular que reza «el crimen siempre va un paso adelante de la ley», se hace más real que nunca. Años atrás era posible realizar envíos de droga y comunicar a sus receptores el día, lugar y hora de llegada de los mismos, utilizando las líneas telefónicas públicas o teléfonos celulares prepagos desechables («*burners*») sin que dichas llamadas pudieran ser rastreadas o intervenidas por la policía. La misma metodología se utilizaba para traficar armas, personas y coordinar la ejecución de actos terroristas.

Sin embargo, con el correr del tiempo y la evolución de la tecnología informática esto permitió a los investigadores comenzar a acceder a esas comunicaciones telefónicas y por tanto poder frustrar dichos delitos y eventualmente recopilar evidencia para ser utilizada en procesos penales que llegaran a condenar los sujetos que cometieran dichos ilícitos.

A medida que las fuerzas del orden empezaron a intervenir con mayor asiduidad las conversaciones telefónicas de los miembros de bandas criminales, estos se vieron en la necesidad de recurrir a métodos que les permitieran seguir con su actividad sin poder ser detectados por la policía o mejor dicho que esta última no pudiera recabar información de la actividad criminal en forma válida, y someter a los criminales a un debido proceso. Mas aún si tenemos en cuenta que los delitos antes citados, se llevan a cabo con la participación de individuos radicados en distintos países, es decir: son de carácter transnacional. En los supuestos de tráfico de estupefacientes o armas, el cargamento de drogas ilícitas o armas se prepara en el país A, se lo acondiciona de manera de no ser detectado por las fuerzas policiales, se realiza el contacto con quien será encargado de recepcionar el mismo en el país B y finalmente será remitido a los sujetos que en el país C se encargarán de vender o bien utilizar. Dicha metodología se aplica también al caso de compraventa de armas y a la trata de personas.

a. Nuevas tecnologías

La evolución de las tecnologías informáticas les ha brindado a las organizaciones delictivas, nuevas formas de camuflar sus actividades o desempeñarlas con mayor sigilo.

El desarrollo que han tenido las redes que se dedican a intercambiar fotografías o videos de menores de edad (desde bebés hasta adolescentes) desnudos, en posiciones sexuales o incluso siendo víctimas de abusos sexuales son generalmente de tipo transnacional; ello hace complejo poder llegar a la detección y detención de los sujetos intervinientes, más aún si tenemos en cuenta que es de uso común que, aquellos que participan de dichas actividades para acceder a esas plataformas, deben compartir previamente dicho material, y a efectos de no ser detectados en sus lugares de origen utilizan redes *peer-to-peer* (en adelante, «P2P»).

Aquí debemos detenernos en el concepto de red P2P

> «Una red peer-to-peer (P2P) es un sistema de comunicación descentralizado en el cual cada nodo (par) en la red puede actuar simultáneamente como cliente y como servidor. Este tipo de red permite a los usuarios compartir recursos y datos directamente entre ellos sin necesidad de un servidor central. Las redes P2P se caracterizan por su capacidad de distribuir la carga de trabajo y de datos entre todos los participantes, lo que reduce la dependencia de una infraestructura centralizada y mejora la resistencia a fallos»[2].

Ejemplos de redes P2P son *eMule*, *skype* (en las primeras versiones) *freenet* y *bitcoin* entre otros; *E mule* utiliza *eDonkey* y la red *kad*[3] para permitir a los usuarios compartir archivos entre sí, se caracteriza por la capacidad de encontrar archivos raros y por su robustez en el sistema de intercambio de archivos. En el caso de *eDonkey* faculta a los usuarios a subir archivos de fotos, video, sonido y software que luego transforma en archivos más pequeños que facilitan su descarga y distribución. Así también otorga un sistema de créditos, de manera que los usuarios que suben mayor cantidad de archivos obtienen mayor prioridad en la red y por tanto incentiva el intercambio de material. Es una de las redes más populares entre aquellos que trafican material de abuso sexual infantil.

En el caso de bitcoin[4] es una red P2P que permite que se realicen transacciones directas de criptomonedas entre usuarios sin la necesidad de un intermediario central. Cada uno de los nodos de la red validan y registran las transacciones en una cadena de bloques lo que se conoce como *blockchain*. La empresa precitada en su página web brinda la siguiente definición

> Bitcoin usa tecnología peer-to-peer o entre pares para operar sin una autoridad central o bancos; la gestión de transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red. Bitcoin es de código abierto; su diseño es público, nadie es dueño o controla Bitcoin y todo el mundo puede participar.

Las redes *peer-to-peer* también son utilizadas por los grupos criminales para el desarrollo de actividades como el narcotráfico, compraventa de armas y lavado de activos de origen ilícito.

Teniendo en cuenta que en el siglo XXI, la forma más usual de comunicarse es a través de teléfonos celulares, es que en el año 2016 se comenzó a vender primariamente en Europa, un sistema de telefonía celular que poseía un software que brindaba un sistema de doble encriptación de las comunicaciones, denominado *EncroChat*; lo cual permitía a sus usuarios poder utilizar los mismos sin que las llamadas o mensajes, fueran interceptadas por las fuerzas de seguridad; además poseía un botón de pánico que permitía borrar todos los datos del teléfono.

Ello hizo que comenzara a hacerse popular su uso entre personas preocupadas por la seguridad y privacidad de las comunicaciones, actores, actrices, personas famosas y periodistas. Sin embargo, en la práctica, la explosión de popularidad la tuvo entre los individuos que desarrollaban actividades criminales; bandas organizadas dedicadas al tráfico de estupefacientes, armas de fuego, trata de personas y bandas de motociclistas. Esta empresa fue desarticulada por la policía francesa en conjunto con las fuerzas policiales holandesas en el año 2020, caso que analizaremos más adelante.

---

[2] Monastersky, D. (2018). *Cibercrimen: la nueva amenaza de la delincuencia en la era digital*. Ediciones Jurídicas.
[3] La red Kad es una red descentralizada que utiliza tecnología de tablas hash distribuidas (DHT) para búsqueda e intercambio de archivos entre pares. Enlace.
[4] Bitcoin Project. (s.f.). Bitcoin. Enlace.

Ante la caída de *EncroChat* se vuelca gran parte de «su clientela» a otro software denominado *ANOM*, el cual comenzó a comercializarse en el año 2018 con el objetivo de brindar a sus usuarios un medio de comunicación seguro y por tanto protegido de posibles interceptaciones, el mismo se comercializaba sólo entre miembros del hampa, era requisito para poder acceder a uno de los dispositivos celulares con dicho software, ser recomendado por alguna persona con antecedentes criminales. Luego veremos que en realidad la puesta en funcionamiento de dicho software, fue parte de una operación encubierta denominada «operación trojan shield» llevada adelante por las fuerzas del orden y el FBI.

Además de los métodos de comunicación antes descriptos, existen otros más sencillos y económicos para realizar llamadas telefónicas y enviar mensajes con cierta seguridad, dado su grado de encriptación tales como las aplicaciones de mensajería WhatsApp y telegram. Ambas permiten realizar llamadas telefónicas y enviar mensajes de texto, voz y video. La primera es propiedad de Meta cuyos servidores se encuentran ubicados en Estados Unidos de América y la segunda fue desarrollada por dos hermanos de origen ruso Nikolái y Pável Durob. A través de cualquiera de dichas aplicaciones, se pueden realizar llamadas telefónicas que no pueden ser interceptadas por las fuerzas de seguridad, como las llamadas telefónicas comunes. Además, en el caso de telegram permite enviar mensajes de texto, voz o video que pueden ser borrados ya sea por el emisor o el receptor en su totalidad, no dejando rastros del mismo en el teléfono celular.

Existen otros medios por los cuales se pueden llevar adelante conversaciones tales como Facebook, Instagram, Tik-Tok y Snapchat, entre otros, si bien estas son redes sociales, tienen previstos servicios de mensajería a disposición de sus usuarios, aunque en estos casos la posibilidad de mantener un cierto grado de anonimidad y de seguridad frente a posibles interceptaciones, es muchísimo más bajo que en las precitadas.

También es posible llevar adelante charlas a través de las plataformas de juego on-line, ya que las mismas poseen un chat disponible para sus jugadores, lo cual muchas veces es usado por delincuentes para llevar adelante sus reuniones y mantener conversaciones sobre operaciones criminales de distinta índole.

Por último, no debemos olvidar el correo electrónico, el cual permite enviar archivos de texto, voz o video a través de cualquiera de las plataformas de mail disponibles en la actualidad. Si bien este último es menos seguro si, lo que se busca, es no dejar ningún tipo de rastro del material enviado.

2. Nuevas técnicas de investigación. El agente digital encubierto. Problemas legales y éticos de su implementación

La transnacionalidad de los delitos antes detallados trae aparejados distintos problemas, sea respecto a la legislación aplicable al procedimiento penal como también al derecho penal sustantivo, ya que la actividad criminal se produce afectando la normativa de distintos estados soberanos. Y ello impacta en el tipo de evidencia que se podrá recabar y también en el procedimiento para recabar la misma, de modo de que ella sea útil en un proceso penal posterior.

A los efectos de recabar pruebas se ha hecho necesario recurrir a nuevas técnicas de investigación, una de ellas es la del *agente digital encubierto***.** Se entiende por tal a: toda persona física que oculta su real identidad con la finalidad de entablar con otra persona física o jurídica una relación, y en virtud de ella obtener a través de ese vínculo, información de esta última o de terceros vinculados a ella. Este agente está autorizado judicialmente a participar de comunicaciones que se realizan en canales cerrados de comunicación, pudiendo enviar y recibir archivos de contenido ilícito, así como también analizar los algoritmos utilizados para identificar esos archivos ilícitos. También podrán ser autorizados a obtener imágenes o grabación de conversaciones que se realicen dentro del domicilio del investigado.

En la ley de enjuiciamiento criminal española esta figura no se encuentra definida expresamente, pero la misma surge de los incisos 6 y 7 del art. 282 bis.

a. Implicancias éticas y legales del agente digital encubierto.

Esta figura implica necesariamente la necesidad de entablar con el sujeto intervenido una relación de confianza, en muchos casos hasta de manipulación del mismo, con el objeto de que llegado el momento se pueda obtener la información o prueba buscada. Claramente existe una injerencia en la faz privada muy alta, lo cual puede comprometer el derecho de privacidad de los ciudadanos. Por ese motivo, esta medida debe ser utilizada sólo en supuestos en los que los delitos son graves, sea por su repercusión en la sociedad o por los bienes que resultan vulnerados por los mismos. De lo contrario, se caería en una sociedad hipervigilada, susceptible de ser manipulada por los agentes del estado, vulnerando de esa manera derechos individuales fundamentales como el derecho a la intimidad, la inviolabilidad de la correspondencia y papeles privados, la inviolabilidad del domicilio y de las comunicaciones y el derecho de libertad de expresión, poniendo en jaque la obligación del estado de cumplir con el principio de transparencia de las instituciones públicas, propio de todo estado republicano.

Por todo ello cabe ante todo preguntarse: ¿cuáles son las condiciones necesarias para que, la información recabada por el agente digital encubierto, pueda ser utilizada en un proceso penal? La respuesta radica en el respeto a los principios de legalidad y debido proceso. Ello se logrará si la figura se encuentra específicamente prevista en el ordenamiento jurídico procesal del país en el que se pretende usar dicha técnica de investigación, no se puede aplicar por analogía la figura del agente encubierto común. Ya que la actividad que despliega el agente en el ámbito digital, es mucho más invasiva que la que puede desarrollar el agente encubierto en la realidad física y por tanto claramente puede violar el derecho de intimidad de las personas ajenas a la investigación penal de que se trate.

La otra condición que rige para la validez de la actuación del agente digital encubierto, es que exista autorización del juez competente previa a la misma. Para ello el magistrado debe ser notificado de cuáles son los indicios que existen sobre el delito a investigar, la necesidad de utilizar esta técnica de investigación por la gravedad del hecho delictivo o por su desarrollo fundamentalmente en la red, el plazo específico por el cual se va a habilitar el trabajo del agente encubierto, y la necesidad de que realicen reportes periódicos sobre el resultado de su trabajo. En los casos en los cuales el agente digital encubierto, deba a efectos de lograr recabar evidencia, proceder a realizar video grabaciones o grabación de conversaciones, tendrá que solicitar al magistrado específicamente dicha autorización, no puede muñirse para realizar dichas actividades de

la autorización judicial primigenia. Lo mismo debe aplicar, para los casos en los que, a efectos de proceder a realizar video grabaciones, deba ingresar a un domicilio particular.

En aquellos casos en los cuales el tipo de delito investigado o la dificultad para recabar evidencia, traiga aparejado la necesidad de extender la tarea del agente digital encubierto, será necesario que exista autorización judicial para ello.

Y aquí cabe cuestionarse lo siguiente: ¿puede el agente digital encubierto cometer hechos ilícitos en el marco de su investigación? Y de ser así, ¿podrá ser sancionado penalmente por ello?

Es claro que en el transcurso de una investigación penal de delitos complejos como puede ser el tráfico de drogas, armas, personas o terrorismo muchas veces el agente se verá en la necesidad de cometer algún hecho ilícito con el objetivo de continuar su actuación dentro de la red que se encuentra investigando, recordemos que esta figura se aplicará para delitos graves tales como los mencionados. De lo contrario, la tarea del investigador se verá frustrada, y el trabajo y esfuerzo desplegados en pos de la protección de bienes jurídicos sensibles, será en vano. Sin embargo, para que los actos delictivos que haya realizado el agente encubierto digital, no sean sancionados penalmente, será necesario que los mismos guarden proporción y razonabilidad con el delito investigado y en la medida en que no hayan sido provocados por el agente. Así lo ha previsto la ley de enjuiciamiento criminal española en su artículo 282 bis inciso 5 «el agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito».

b. Caso *EncroChat* y operación *trojan shield*.

En virtud de las investigaciones que estaba llevando a cabo en el año 2017, el instituto de investigación criminal de la gendarmería nacional detectó el uso de teléfonos celulares con tecnología Android, que poseían un software que permitía realizar llamadas encriptadas, así como también enviar mensajes y crear notas encriptadas. El software de la empresa *EncroChat* además poseía un «botón de pánico» que permitía a sus usuarios una vez presionado, eliminar todo el contenido de los datos existentes en el teléfono, además tenía una función de autodestrucción. Este servicio, permitía mejorar la seguridad de la comunicación que brindaban los teléfonos desechables, sobre todo ante el avance de las fuerzas policiales en la ruptura de las encriptaciones. La aplicación funcionaba con una suscripción de pago de 3.000 euros al año.[5]

La investigación fue iniciada por la fiscalía de la jurisdicción interregional especializada de Lille (Francia), debido a que la ubicación de los servidores que ejecutaban *EncroChat*, se encontraban en su jurisdicción. Pero la investigación completa se llevó adelante en conjunto con la fiscalía de Holanda con el apoyo de Europol y Eurojust. Al tiempo de conclusión de la operación mencionada, existían 50.000 teléfonos celulares con ese software y el 90 % de los mismos era utilizado por criminales.

La operación de infiltración de la *red EncroChat* llevó aproximadamente más de dos meses. El malware enviado consistía en una actualización de los dispositivos *EncroChat* que realizaba el servidor comprometido, lo cual trajo aparejado que todos los dispositivos

[5] Zagaris, B. (2020, 30 de septiembre). EncroChat: la Policía europea desmantela una extendida red de mensajería encriptada para delincuentes. DelitosFinancieros.org. Enlace.

afectados, cargaran una imagen de todo el contenido del teléfono de vuelta a la policía francesa.

Tal es así que el 2 de julio de 2020, dichas autoridades anunciaron públicamente «la caída de *EncroChat*» lo que llevó a realizar más de 800 detenciones en países como Francia, Holanda, España, Reino Unido, Francia, Alemania, Suecia y Noruega.

La infiltración del servicio *EncroChat* por parte de las autoridades precitadas, tuvo aparejado detectar y desarticular operaciones de tráfico de drogas, armas, asesinatos, secuestros y lavado de dinero llevadas adelante en Europa por bandas del crimen organizado. Lo cual redundó en la incautación de más de 8.000 kilos de cocaína en Holanda, así como 1.2 toneladas de metanfetaminas, 25 millones de euros en efectivo, joyas, decenas de autos de lujo y el desmantelamiento de laboratorios de drogas sintéticas.

En tanto que, en el Reino Unido, la policía logró realizar más de 700 arrestos, confiscó 67 millones de libras esterlinas en efectivo, dos toneladas de drogas y numerosas armas de fuego.

Pero con la detención y arresto de tantos individuos surgieron las quejas planteadas por las defensas de los mismos en distintos países europeos, fundamentalmente en relación a la posibilidad del correcto ejercicio del derecho de defensa ante la legalidad de las pruebas obtenidas a través de la operación «*EncroChat*». Sus principales argumentos radican sobre:

- La falta de especificación de la medida de intervención de las comunicaciones, ya que no se encontraba determinado que tipo de comunicaciones se iban a intervenir; si eran llamados telefónicos, correos electrónicos o mensajes de texto;
- el desconocimiento sobre cómo se hicieron las interceptaciones, las defensas no pudieron acceder a conocer de qué manera se hicieron las mismas, ya que la policía francesa manifestó que el método utilizado, quedaba dentro de la ley de seguridad nacional y por tanto secretas;
- el uso de la encriptación como presunción de culpabilidad, sostienen que los tribunales han desarrollado una jurisprudencia basada en que la existencia de información encriptada en poder de los acusados, ya de por sí los hace parte de una organización criminal; y
- la falta de autorización judicial previa, ya que luego de cancelada la actividad de la empresa *EncroChat*, las autoridades francesas y holandesas remitieron al Reino Unido, Alemania y otros países europeos, la información que fue recabada en el curso de la investigación, ello a través de una orden de investigación europea, pero esto se hizo sin la autorización previa de un juez.

En el Reino Unido, se interpusieron recursos solicitando que se dejaran sin efecto, las condenas o arrestos que se habían realizado en virtud de la información brindada por los investigadores de *EncroChat*. En el precitado país existe una norma denominada «ley de poderes de investigación» del año 2016 que dispone que, interceptar comunicaciones a través de un «sistema de telecomunicaciones» es ilegal a menos que haya una orden adecuada vigente.

Existen distintos tipos de ordenes exigidas, dependiendo de si el mensaje interceptado estaba siendo transmitido o estaba almacenado en un lugar del sistema. Si está en reposo, la policía debe solicitar una orden de interferencia de equipos dirigida, pero si está en transmisión, se requiere una orden de intercepción dirigida. Teniendo en cuenta esta diferencia la justicia del Reino Unido en el año 2021 resolvió

> hemos concluido que la única pregunta sustancial que el juez estaba obligado a responder era si el material de *EncroChat* estaba almacenado por o en el sistema de telecomunicaciones cuando fue interceptado. Al igual que él, consideramos que estas comunicaciones no estaban siendo transmitidas sino almacenadas en ese momento.

Razón por lo cual, desestimó el pedido de las defensas sobre la nulidad de la información que fue obtenida a través del hackeo de *EncroChat*, que realizaran las fuerzas policiales francesas y holandesas.

Sin embargo, esta situación puede cambiar en un futuro cercano, ya que los tribunales franceses en el año 2022 resolvieron que los investigadores y fiscales, no proporcionaron un certificado para autenticar los datos telefónicos interceptados y los mensajes obtenidos de los teléfonos *EncroChat*; tal como lo exige la ley francesa. También se determinó que la policía francesa no reveló, por motivos de secreto de defensa, cómo las autoridades holandesas y francesas llevaron a cabo la operación de hacking en *EncroChat*.

Y siguiendo esa línea, es que el tribunal de justicia europeo el 30 abril del año 2024, resolvió en el caso C-670/22, M.N contra el Estado Alemán, que

> «[…] El artículo 31 de la Directiva 2014/41 debe interpretarse en el sentido de que una medida relacionada con la infiltración en aparatos terminales, con objeto de extraer datos de tráfico, de localización y de comunicación de un servicio de comunicación basado en Internet, constituye una «intervención de telecomunicaciones», en el sentido de dicho artículo, que debe notificarse a la autoridad designada a tal efecto por el Estado miembro en cuyo territorio se encuentre la persona que sea objeto de la intervención. En el supuesto de que el Estado miembro que realice la intervención no esté en condiciones de identificar a la autoridad competente del Estado miembro notificado, esta notificación podrá dirigirse a cualquier autoridad del Estado miembro notificado que el Estado miembro que realice la intervención considere idónea para ello».

En el considerando 5 dispone

> «[…] El artículo 14, apartado 7, de la Directiva 2014/41 debe interpretarse en el sentido de que obliga al juez penal nacional a excluir, en el marco de un procedimiento penal incoado contra una persona sospechosa de haber cometido hechos constitutivos de delito, determinada información y determinadas pruebas si dicha persona no está en condiciones de comentar eficazmente esa información y esas pruebas y si estas pueden influir destacadamente en la apreciación de los hechos».

Teniendo como antecedente la investigación del caso *EncroChat*, es que el FBI decidió llevar adelante lo que dio en llamar «operación Trojan Shield». El precitado órgano de investigación, había logrado con éxito acusar y encarcelar al titular de una empresa denominada *Phantom*, dedicada a brindar servicios de telefonía celular con un software de encriptación; a raíz de ello logran reclutar un «informante» el cual se encontraba desarrollando una «nueva generación» de aparatos de comunicación encriptados denominado *ANOM*. Este informante, con anterioridad había comercializado equipos de telefonía celular con software de encriptación, los mismos se vendían entre miembros del hampa exclusivamente, de manera que era conocido en el ambiente de la criminalidad organizada.

El funcionamiento del dispositivo *ANOM* implicaba un «backdoor» diseñado por el FBI, que permitía que cada mensaje enviado por los usuarios de *ANOM*, generara una copia cifrada adicional enviada a un servidor controlado por el FBI conocido como «*iBot*».

Este servidor descifraba el mensaje, extraía la información relevante (ubicación GPS, texto, nombre de usuario, etc.), y luego reenviaba la información a otro servidor, propiedad del FBI (*iBot2*). En virtud de restricciones legales de Estados Unidos, el servidor se ubicó primigeniamente en Australia, con intervención de la policía australiana y luego en Lituania.

Durante la etapa de versión beta de *ANOM*, la policía australiana solicitó órdenes judiciales a efectos de monitorear legalmente, a aquellos ciudadanos australianos que se encontraban utilizando dicho dispositivo o bien a individuos con claros nexos con Australia.

Durante el transcurso del año 2019, el FBI comenzó tratativas con un tercer país a efectos de que se instale un servidor «*iBot*» en este último, de manera que una vez que este, obtuvo la orden judicial correspondiente de acuerdo a su legislación, procedió a copiar toda la información del «*iBot*» y en virtud de un tratado existente entre Estados Unidos y el precitado país, a través de un *mutual legal assistance treaty* (*MLAT*) el FBI pudo acceder a la copia del servidor.

Con posterioridad el tercer país obtuvo una orden judicial para acceder a las copias del «*iBot*» cada tres días. Dicha información fue remitida al FBI hasta junio del año 2021. Esa información comprendía los mensajes encriptados de todos los usuarios de *ANOM*. Y trajo aparejado la traducción de 20 millones de mensajes correspondientes a 11.800 dispositivos, que eran utilizados en 90 países.

La mayor cantidad de usuarios se encontraban en Alemania, España, Australia, Holanda y Serbia. Del análisis de los mensajes, el FBI pudo determinar que los dispositivos eran utilizados exclusivamente por miembros de organizaciones criminales transnacionales, dedicadas al tráfico de droga y lavado de dinero, sin embargo, también detectaron otras actividades ilícitas.

Con el acceso a esta información, detectives del FBI solicitan autorización judicial al tribunal de distrito de California, a efectos de que le otorguen autorización para que la *Empresa Google LLC*, entregue copia digital de toda la información correspondiente a la cuenta expliam@gmail.com desde el 1 de enero de 2021 al 15 de mayo del 2021 a funcionarios del FBI. La información requerida consistía en el contenido de los correos electrónicos, sus adjuntos, mensajes de texto guardados, mensajes de voz, fotografías, logs de acceso, perfiles, lista de amigos, información de pagos, detalles de facturas y documentación de embarques.

El juez autorizó la misma y ello llevó a que las autoridades norteamericanas, pudieran realizar más de 500 arrestos en distintos países, secuestraron 8 toneladas de cocaína, 22 toneladas de marihuana, 48.000.000 de dólares en efectivo y criptomonedas, armas de fuego, vehículos de lujo y además lograron desmantelar 50 laboratorios clandestinos de drogas.

Si bien los abogados defensores de los acusados, han intentado lograr la exclusión de la evidencia recabada en esta investigación, argumentando que se habían violado el derecho al debido proceso y el derecho a la privacidad, hasta el momento ningún Tribunal ha receptado tales posturas, y no han rechazado la evidencia recabada.

En la *operación Trojan Shield*, se tiene certeza de que toda la información a la que se estaba «accediendo» a través de la infiltración de los aparatos de comunicación encriptados, correspondían a criminales. Esto es lo que marca la diferencia con el caso

EncroChat, cuyo dispositivo era utilizado por criminales, pero también por ciudadanos comunes y corrientes, si bien en un número ínfimo en relación a aquellos.

3. Acceso transfronterizo de datos

La evolución de la tecnología de la comunicación y en especial de internet siendo esta, una super autopista de información, que implica que cualquier persona pueda tener acceso a todo tipo de servicio de información electrónica, con indiferencia del lugar el mundo en el que se encuentre; trajo aparejado problemas relacionados a los delitos cometidos en el «ciberespacio», pero también en relación a los delitos tradicionales, cuyos autores se valen de las nuevas técnicas de comunicación para llevarlos adelante. Los delitos cometidos en el ciberespacio comprenden los ataques contra la integridad, disponibilidad y confidencialidad de los sistemas informáticos y de las redes de comunicación. Hablamos de situaciones en las que un individuo radicado en un país «X», puede acceder ilegítimamente al servidor que contiene la información de todos los residentes argentinos que poseen licencia de conducir[6]; o el hecho de que un grupo de personas de nacionalidad rusa realice un «ataque» «a una empresa aseguradora Argentina», enviándoles un virus a través de un inocente correo, que traiga aparejado el «secuestro» de toda la base de datos de la misma; la cual posteriormente es encriptada y a cambio de su devolución, se le exigen a los directivos una determinada suma de dinero[7]. Estas son situaciones, que eran impensables para los legisladores de comienzos del siglo pasado.

Como se puede observar, se pone en juego la territorialidad de las autoridades encargadas de exigir el cumplimiento de las leyes, ya que estamos frente a conductas delictivas transfronterizas.

Teniendo en cuenta, que la información generalmente se encuentra almacenada en servidores de distintos países, el acceso a dicha información importa poner en juego la legislación penal y procesal penal de dichos estados.

Sin olvidarnos que la evidencia electrónica es volátil, por lo cual esta situación coloca un escollo más en las investigaciones transnacionales, sin olvidar que existen distintos marcos normativos en materia de protección de datos personales, que dificulta el acceso a la misma, además de falta de capacitación de las autoridades que existen en algunos países. Para ello debemos tener como norte, el respeto a la privacidad de los datos personales y la cooperación de los estados nacionales.

Por ello se hace necesario, ante una sociedad globalizada e hiperconectada crear mecanismos de cooperación internacional, que faciliten el acceso a evidencia clave en la comisión de delitos. Esto debe producirse, de manera que la misma pueda ser recabada tomando los recaudos necesarios, que permitan luego incorporar la misma al proceso penal. Lo cual trae aparejado, el respeto al debido proceso, y el acceso de la defensa a conocer la metodología que se utilizó para recabar la prueba. Recordemos que la misma, se encuentra alojada en servidores de un país distinto de aquél en el que vive su defendido.

[6] Infobae. (2024, 16 de abril). *Hackearon la base de datos de licencias de conducir: contiene casi 6 millones de registros y piden USD 3000 para devolverlas*. Infobae. Enlace.
[7] Ámbito. (2024). *Ciberseguridad: una aseguradora argentina sufrió un importante ataque hackers rusos*. Ámbito. Enlace.

Estas son las cuestiones que ya a finales de los años 90, se estaban discutiendo en el marco del comité europeo para los problemas criminales y el cual tomó en cuenta el informe del profesor Dr. H. W. K. Kaspersen el cual sostuvo lo siguiente

> «[…] habría que buscar otro instrumento jurídico más obligatorio que una recomendación, tal como un convenio. Dicho convenio no debería abordar tanto las cuestiones de derecho penal sustantivo como las cuestiones de derecho procesal penal, así también como los acuerdos y procedimientos del derecho penal internacional»[8].

En tanto que, en la conferencia del G-8 sobre crimen organizado transnacional, que se realizó en Moscú el 19 y 20 de octubre de 1999, se establecieron lineamientos claves, para combatir el crimen organizado transnacional y los delitos de alta tecnología. Entre ellos se encontraban los siguientes: (a) Permitir la conservación de datos contenidos en los sistemas informáticos de otro Estado de forma expedita en conformidad con la legislación nacional; (b) Autorizar el acceso, búsqueda, copiado o incautación de datos almacenados en sistemas informáticos ubicados en otro Estado; cuando se ha otorgado el consentimiento voluntario de una persona que tiene la autoridad legal para divulgar los datos; (c)Disponer que el acceso transfronterizo a datos almacenados, no requieren la asistencia jurídica cuando se encuentren en fuentes públicas (fuentes abiertas), con independencia de su ubicación geográfica; (d) Establecer que cuando un Estado requiera acceso a datos en otro Estado, y esos datos revelen una violación del derecho penal, se debe notificar al Estado donde se llevará a cabo el acceso.

En el año 2010 la *unión internacional de telecomunicaciones* (UIT) elaboró un conjunto de herramientas legislativas sobre ciberdelito; con el objetivo de facilitar y proporcionar a los distintos países materiales de referencia y apoyo, para armonizar la legislación y normas de procedimiento en materia de ciberdelito. Otra meta era que la misma pueda ser utilizada como guía, para los estados que deseen desarrollar o modificar la legislación sobre el tema.

La sección 30 de ese conjunto de herramientas, posee un artículo muy similar al artículo 32 del convenio de Budapest del año 2001[9], el primero dispone que la autoridad competente podrá acceder a los datos informáticos almacenados (de fuente abierta) y son de acceso público, ya sean estos de contenido o de tráfico con independencia de la ubicación geográfica de los mismos.

Así también prevé que

> […]una autoridad competente de otro país puede, sin autorización de las autoridades de ese país, tener acceso y recibir, por medio de una computadora o sistema informático ubicado en su territorio, datos informáticos especificados, datos de contenido o datos de tráfico almacenados en ese país si la autoridad competente del otro país obtiene el consentimiento legal y voluntario de la persona que tiene la autoridad legal para divulgar los datos a dicha autoridad competente a través de esa computadora o sistema informático»[10].

Tal como había expresado el profesor Kaspersen, se hacía necesario tener un Convenio que permitiera abordar temas de derecho procesal internacional en materia de

[8] Consejo de Europa. (1997). *Aplicación de la Recomendación núm. R (89) 9 sobre delitos informáticos* (Informe preparado por el Prof. Dr. H. W. K. Kaspersen, Doc. CDPC (97) 5 y PC-CY (97) 5, p. 106).
[9] Consejo de Europa. (2001*). Convenio sobre Ciberdelincuencia* (Budapest, 23 de noviembre de 2001), art. 32: Acceso transfronterizo a datos almacenados con consentimiento o cuando estén disponibles públicamente.
[10] Unión internacional de telecomunicaciones. (2010). *Conjunto de herramientas para la legislación sobre ciberdelito* (Sección 30).

ciberdelitos, y es así como surgió el convenio de Budapest en el año 2001, suscripto por Estados Unidos y gran parte de los países que conforman la Unión Europea. El mismo quedó abierto para su adhesión por parte de otros Estados, con el objetivo de tener una herramienta internacional que favoreciera el intercambio de información ubicada en bases de datos informáticas o sistemas informáticos transnacionales, a través de procesos ágiles y no engorrosos que favorezcan la persecución de los delitos cometidos en el ciberespacio o a través de él. Ello respetando los derechos fundamentales previstos en el *convenio del consejo de Europa para la protección de derecho humanos y de las libertades fundamentales* (1950), *pacto internacional de derechos civiles y políticos de naciones unidas* (1966), el *convenio del consejo de Europa para la protección de los datos informatizados de datos personales* (1981) y otros convenios que tienen por objeto el resguardo a la libertad de expresión y el respeto al derecho de privacidad.

El precitado convenio posee un protocolo adicional que penaliza la comisión de actos xenófobos o racistas cometidos a través de internet.

El segundo protocolo adicional al convenio sobre ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas se sancionó el 12 de mayo del año 2022 y entró en vigencia a finales del año 2023.

Este último ha previsto entre otras medidas tendientes a reforzar la cooperación internacional, en su artículo 12, la conformación de equipos conjuntos de investigación entre los Estados partes del mismo. Dichos equipos actuarán en sus territorios en aquellos casos que sean convenientes por la naturaleza de la investigación y proceso penal, ello a efectos de favorecer las mismas.

Para ello, las autoridades competentes acordarán los procedimientos y condiciones que van a regir el funcionamiento de los equipos conjuntos de investigación; en particular lo atinente a su composición, funciones, duración, organización, requisitos correspondientes a la recopilación, transmisión y utilización de pruebas que realicen las autoridades de una parte en la investigación que tenga lugar en el territorio de la otra parte.

Así también dispone que, cuando sea necesario tomar medidas de investigación en el territorio de una de las partes en cuestión, las autoridades participantes de dicha parte podrán solicitar a sus propias autoridades, tomar esas medidas sin que sea necesario presentar una solicitud de asistencia mutua.

El uso de la información podrá ser denegado o restringido según lo pactado en el acuerdo. Si el mismo no regula las condiciones para denegar o restringir su uso, las partes podrán utilizar esa información para los casos previstos en el Convenio, ante situaciones de emergencia, y para la detección, investigación, enjuiciamiento de delitos distintos de los contemplados en el acuerdo, siempre que exista la autorización previa, de las autoridades que proporcionen la información o las pruebas.

Es altamente probable, que el resultado de la operación denominada *EncroChat* llevada adelante en un principio por Francia y Holanda en el año 2017, haya servido como antecedente para la incorporación del artículo 12 del segundo protocolo de Budapest. Mas aún si tenemos en cuenta que hasta el día de hoy, se está debatiendo en los Tribunales Europeos la validez de la evidencia recabada en la operación precitada.

La república argentina adhirió al convenio de Budapest sobre ciberdelincuencia del año 2001, el cual entró en vigencia en virtud de la ley 27.411, de fecha 15 de diciembre

del año 2017. En tanto que, a mediados de febrero del año 2023, la república argentina adhirió al segundo protocolo adicional de Budapest.[11]

4. El agente digital encubierto y la legislación argentina

En la actualidad la figura del *agente digital encubierto* sólo está previsto en la provincia de Mendoza. En otras jurisdicciones existe la figura del agente encubierto y del agente revelador, tal como ocurre en la ciudad autónoma de buenos aires o en la provincia de santa fe, pero no específicamente la del agente digital encubierto.

El código de procedimiento penal de Mendoza, receptó a comienzos del 2024 esta figura especial en el artículo 29 bis, y lo define en su último párrafo de la siguiente manera

> A los efectos del presente artículo se considera agente encubierto digital al funcionario de las fuerzas de seguridad o miembro del Ministerio Público Fiscal autorizado, que previo prestar su consentimiento, oculte o utilice un perfil digital encubierto, interactúe y se relacione digitalmente a través de tecnologías de la información y de la comunicación con el objeto de: identificar o detener a los autores, partícipes o encubridores de un delito; impedir la consumación de un delito; o para reunir información o elementos de prueba necesarios para la investigación.

La normativa procesal dispone que, en aquellos casos en los que sea necesario investigar delitos en plataformas o entornos digitales, el fiscal podrá solicitar autorización al juez penal colegiado; pero para ello deberá haber fundado expresamente los motivos por los cuales se hace necesario recurrir a tal medida de investigación. Así también deberá acreditar que la misma es imperiosa ya que se encuentra ante la posible existencia de delitos de producción, comercialización y distribución de material de abuso sexual infantil; es decir toda la gama de hechos tipificados en el artículo 128 del código penal, también para el caso del delito de grooming, receptado en nuestro ordenamiento jurídico penal en el artículo 131. El código procesal penal de Mendoza agrega, que se podrá recurrir a la utilización del agente digital encubierto, cuando se trate de delitos cometidos a través de medios informáticos, que no pueden ser investigados por otros medios; como todo otro delito que por su especial gravedad o por la complejidad de su investigación, justifique utilizar esta figura.

El agente deberá realizar su tarea en un plazo de 180 días, contados a partir de la fecha en que el juez lo autorizó. No se encuentra prevista en forma expresa la posibilidad de prorrogar dicho plazo, de manera tal que sólo será legal la actuación del agente, siempre que se haya realizado dentro de ese marco de tiempo.

Los perfiles que hayan sido creados para la actuación del agente, no podrán corresponder a imágenes que pertenezcan a personas reales, y serán manejados por personal idóneo de la fiscalía o de la fuerza de seguridad habilitada para ello. Todo el trabajo que lleve adelante dicho agente deberá ser puesto en conocimiento de la fiscalía que solicitó la medida, la cual será la encargada de resguardar (en caja de seguridad) toda la información relativa a los perfiles usados, las plataformas en las que haya intervenido, las claves de acceso a las mismas y la actividad concreta desarrollada por el mismo.

A efectos de proteger al agente digital encubierto, de la responsabilidad penal que pueda surgir como consecuencia de su tarea, la normativa dispone que el mismo podrá

[11] Presidencia de la Nación. (2025). *Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito*. Argentina.gob.ar. Enlace.

enviar o intercambiar archivos ilícitos relacionados a la investigación en curso, siempre que esté autorizado para ello. Así también se establece que quedará exento de responsabilidad criminal en la medida que los actos realizados guarden proporción con la tarea desarrollada y siempre que no hayan sido provocados. De hecho, el párrafo que trata dicho tema tiene una redacción muy similar al artículo 282 bis inciso 5 de la ley de enjuiciamiento criminal española; siendo que el art. 29 bis código procesal penal de Mendoza dispone

> el agente encubierto digital, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido. El agente encubierto digital estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de ésta y no constituyan una provocación al delito

5. Conclusión

Teniendo en cuenta el gran impacto que tienen las tecnologías informáticas de la comunicación en el desenvolvimiento de la vida actual, y observando que las mismas son utilizadas para cometer ilícitos, debido a que brindan celeridad, seguridad y anonimidad a las organizaciones criminales; se hace necesario que la normativa procesal nacional e internacional prevea normas que recepten técnicas especiales de investigación. Tal es el caso de la figura del agente digital encubierto, la cual deberá encontrarse específicamente regulada en los códigos de procedimiento. Ello con el ánimo de proteger los derechos a la privacidad de los datos personales, a la intimidad, a la libertad de expresión, al debido proceso y la igualdad de armas en el mismo; logrando un equilibrio con la necesidad de proteger y castigar delitos que debe perseguir todo estado, para brindar seguridad a sus ciudadanos.

6. Bibliografía

Barberá, G. (s.f.). *Nuevas tecnologías y libertad probatoria en el proceso penal*.

Bitcoin Project. (s.f.). *Bitcoin*. Recuperado de https://bitcoin.org/

Chambers. (2022, noviembre 22). *What France's Supreme Court Decision Re Encrochat Evidence Means for the UK* (M. S. Khan). https://chambers.com/articles/what-frances-supreme-court-decision-re-encrochat-evidence-means-for-the-uk

Consejo de Europa. (2001). *Convenio de Budapest sobre Ciberdelincuencia*.

Consejo de Europa. (s.f.). *Protocolo adicional que penaliza la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (CETS 189)*.

Consejo de Europa. (s.f.). *Protocolo adicional al Convenio sobre Ciberdelincuencia relativo al refuerzo de la cooperación y la divulgación de las pruebas electrónicas*.

Eurojust. (s.f.). *Eurojust*. https://www.eurojust.europa.eu

Euronews. (s.f.). *Euronews*. https://es.euronews.com

Infobae. (2024, 16 de abril). *Hackearon la base de datos de licencias de conducir: contiene casi 6 millones de registros y piden USD 3000 para devolverlas*.

https://www.infobae.com/politica/2024/04/16/hackearon-la-base-de-datos-de-licencias-de-conducir-contiene-casi-6-millones-de-registros-y-piden-usd-2000-para-devolverlas/

Instituto de Investigación Criminal de la Gendarmería Nacional. (2020). *Search Warrant Operation Trojan Shield, AO 106A (08118) Application for a Warrant by Telephone or Other Reliable Electronic Means Case*.

Kademlia Project. (s.f.). *Kad network*. http://www.kademlia.com/

Ley de Enjuiciamiento Criminal Española. (s.f.). España.

Ley No. 9510 de la Provincia de Mendoza. (s.f.). Argentina.

Monastersky, D. (2018). *Cibercrimen: La nueva amenaza de la delincuencia en la era digital*. Ediciones Jurídicas.

Montserrat de Hoyos, M. (2022, 14 de junio). *La investigación penal a través del agente encubierto* [Trabajo de grado, Universidad de Valladolid].

Presidencia de la Nación. (2025). *Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito*. https://www.argentina.gob.ar/noticias/argentina-y-la-union-europea-unen-esfuerzos-para-combatir-el-ciberdelito

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 30 de abril de 2024, asunto C-670/22.

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 16 de julio de 2020, asunto C-311/18.

The Register. (2020, 13 de noviembre). *EncroChat Judicial Review Judgement*. https://www.theregister.com/2020/11/13/encrochat_judicia_review_judgement

Unión Internacional de Telecomunicaciones. (2010). *Recomendaciones legislativas sobre ciberdelito*.

United States Attorney's Office, Southern District of California. (2021, 28 de mayo). *Indictment: Operation Trojan Shield, Case 3:21-cr-01623-JLS, Document 1*. https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

Zagaris, B. (2020, 30 de septiembre). *EncroChat: la Policía europea desmantela una extendida red de mensajería encriptada para delincuentes*. DelitosFinancieros.org. https://www.delitosfinancieros.org/encrochat-la-policia-europea-desmantela-una-extendida-red-de-mensajeria-encriptada-para-delincuentes/

Ámbito. (2024). *Ciberseguridad: una aseguradora argentina sufrió un importante ataque de hackers rusos*. https://www.ambito.com/informacion-general/ciberseguridad-una-aseguradora-argentina-sufrio-un-impotante-ataque-hackers-rusos-n5665636

Artículos

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 4 – 2025, págs. 16–28
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/azymfr57

Evidencia digital

Introducción al proceso penal: anomia procesal y garantías constitucionales

Eduardo Daniel Viazzi[1]

Resumen

En la actualidad, la incorporación de evidencia digital al proceso penal se ha vuelto cada vez más frecuente, resultado del uso masivo de herramientas y tecnologías informáticas que atraviesan prácticamente todos los aspectos de la vida cotidiana. Las nuevas formas delictivas —habitualmente denominadas «ciberdelitos»— conviven con los tipos penales tradicionales y, en la mayoría de los casos, las tecnologías digitales inciden en la organización de la conducta, en el *iter criminis* o en las fases posteriores a la comisión del hecho. El propósito de este trabajo es precisar cómo debe recolectarse, tratarse, introducirse e interpretarse la evidencia digital en el marco del proceso penal, considerando que las normas rituales vigentes fueron dictadas en un contexto radicalmente distinto, cuando los medios de prueba distaban mucho de poseer las características actuales. En consecuencia, se impone actualizar el rito penal al entorno informático a fin de prevenir eventuales afectaciones a las garantías constitucionales. Para ello, y dado el escaso tratamiento que la temática ha recibido en nuestro sistema judicial y en la jurisprudencia local, se propone abordar la evidencia digital desde su conceptualización, para luego examinar su incorporación en la fase de investigación y analizar los conceptos y precedentes relevantes tanto a nivel nacional como internacional.

Sumario

Palabras clave

evidencia digital – ciberdelitos – metadatos – investigación forense digital – derecho penal informático

[1] Abogado por la universidad nacional de Río Cuarto. Especialista en derecho penal por la universidad de Belgrano. Correo electrónico: viazzi.estudio@gmail.com

1. Breve introducción

Las nuevas tecnologías han venido a revolucionar el modo de vida de los sujetos a tal punto que prácticamente no existen aspectos de la vida cotidiana en los que no tome intervención un dispositivo electrónico que, como tal, almacena datos e información. Piénsese por ejemplo en el caso de un teléfono celular que almacena, entre otras cuestiones, fechas, agenda, comunicaciones laborales y personales, cuentas bancarias, contraseñas, etc. es decir, un sinnúmero de datos que resultan ser una fiel representación de la vida de una persona.

Ahora bien, en el marco de un proceso penal y, puntualmente, en el afán de recolectar evidencia, esos datos pueden afectar la personalidad del sujeto cuando trascienden esferas de intimidad (por ejemplo, al lesionar la expectativa razonable de privacidad) que el sujeto entiende amparada normativa y socialmente.

Los avances tecnológicos obligan a que el sistema de investigación penal deba aggiornarse al ritmo que lo han hecho las manifestaciones delictivas más actuales identificadas como delitos informáticos. Emerge así el derecho penal informático (*cybercrime*) como una representación de aquellos delitos que se cometen mediante el empleo de terminales electrónicas, independientemente de que el destinatario de la ofensa sea un sujeto determinado o un sistema de información.

La investigación de este tipo de delitos resulta más compleja, en parte por la volatilidad de la llamada evidencia digital que exige una preparación y capacitación particular de las fuerzas de seguridad para garantizar la cadena de custodia de todos los elementos probatorios recolectados.

Ahora bien, el propósito del presente artículo es examinar qué es la evidencia digital, qué abarca el concepto y cómo debemos proceder frente a la misma, esto es, su recolección, análisis, conservación y cadena de custodia. Es decir, cuáles son las «buenas prácticas» para que esta evidencia sea válida en términos procesales.

Teniendo siempre como norte el estudio de las garantías constitucionales en juego se determinará el escenario de anomia normativa que impera en la temática.

2. Conceptualización. ¿Qué es la evidencia digital?

Conceptualizar «evidencia digital» resulta dificultoso toda vez que de la conjugación de ambos términos podemos obtener tantos conceptos como enfoques se realicen sobre los mismos, esto es, no será lo mismo conceptualizar a la evidencia digital desde el punto de vista de la naturaleza de los datos, la fuente de donde provienen los mismos que hacerlo desde el contenido mismo de esos datos que, en ocasiones podrán acreditar la existencia de un hecho ilícito.

Una primera definición que puede servir como puntapié inicial para entender el concepto es aquella que identifica a la evidencia digital como un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales[2]. El conglomerado de elementos probatorios que engloba dicha definición resulta extenso ya que hace alusión a cualquier registro de datos que se encuentre almacenado en un dispositivo

[2] Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Academic Press.

electrónico o informático con independencia de si la creación del dato obedece a un factor humano o a la intervención de un dispositivo tecnológico[3].

En lo que nos concierne, la evidencia digital puede ser abordada desde dos enfoques que resultan prácticos, esto es, en primer lugar, desde un enfoque que puntualiza en la cualificación de la modalidad de prueba lo que abarca a aquella información cuya fuente es el ámbito digital (soportes electromagnéticos, computadoras en donde la información se genera por reacción electrónica del dispositivo o plataformas para la gestión de información inteligente; o por empleo de gestiones humanas). En segundo lugar, el enfoque será aquel en que la categoría probatoria se basa en el hecho mismo que surge o está almacenado en la fuente digital; en este caso se pueden probar hechos de relevancia jurídica que impliquen un reproche por comportamientos delictivos[4].

De lo expuesto surge entonces que toda información almacenada en un soporte magnético o electrónico podrá ser considerada evidencia digital. La valoración de este tipo de evidencia, así como su recolección, custodia, introducción al proceso y almacenamiento obligan a un tratamiento especial por el tipo de información que suele manejarse, como así también por la propia naturaleza de la misma.

3. ¿Cómo debe tratarse este tipo de evidencia? Protocolo de actuación

La evidencia digital supone un tratamiento especial por las características propias que posee este tipo de prueba. Las particularidades que caracterizan a la evidencia digital, conforme lo analiza Sosa[5], suponen a la misma:

- Una evidencia *volátil*, es decir, puede ser fácilmente eliminada o extraviada si falla el proceso de recolección;
- Una evidencia *duplicable*, esto es, por su esencia el material es fácilmente duplicable, al punto tal de que sea dificultoso reconocer cuál es el original;
- Una evidencia *alterable*, factible de ser alterada o eliminada sin que consten registros de estas acciones;
- Una evidencia *anónima*, en ocasiones no puede determinarse quien o quienes son los autores de este tipo de evidencia.

Estas características que no son únicas pero que son las más destacadas de este tipo de evidencia implican que, recopilar y preservar la evidencia digital sea un proceso complejo que necesariamente debe ser realizado por quien posee conocimientos y comprensión de la tecnología y los sistemas informáticos.

Ahora bien, debemos entender que dicho proceso en la manipulación de la evidencia digital debe también realizarse respetando las garantías constitucionales de todo proceso penal, por ende, el proceso de recopilación, preservación, identificación, custodia, adquisición y presentación de la evidencia debe ser realizado de modo tal que se

[3] Ministerio Público Fiscal & Ministerio de Seguridad. (2023). *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*. https://www.fiscales.gob.ar

[4] Bujosa Vadell, L. M., Bustamante Rúa, M. M., & Toro Garzón, L. O. (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, 7(2), 1347–1384.

[5] Sosa, M. E. (2023). *Evidencia digital: Su importancia en la investigación*. Revista Pensamiento Penal, (466)

garanticen la integridad y la confiabilidad de la fuente en las investigaciones judiciales y forenses.

El adecuado tratamiento de este tipo de evidencia garantizará su admisibilidad en el proceso, siempre que cumpla con ciertos requisitos. Siguiendo a Devis Echandía, la evidencia será admitida por el Juez siempre que se ponderen una serie de requisitos indispensables, como los define el autos intrínsecos y extrínsecos:

> los primeros (intrínsecos) atañen al medio mismo utilizado en cada caso incluyendo su objeto y los segundos se refieren a circunstancias que existen separadas de ese medio o, pero que se relacionan con él y lo complementan. Son requisitos intrínsecos: a) La conducencia del medio; b) la pertinencia o relevancia del hecho objeto de la prueba; c) la utilidad del medio; d) la ausencia de prohibición legal de investigar el hecho. Son requisitos extrínsecos: a) La oportunidad procesal o ausencia de preclusión; b) las formalidades procesales; c) la legitimación y postulación para la prueba de quien la pide o la presenta y la legitimación del juez que la decreta; d) la competencia del juez o de su comisionado; e) la capacidad general del juez o funcionario comisionado y de los órganos de la prueba (testigos, peritos, interpretes, partes cuando confiesan) y la ausencia de impedimentos legales en aquellos y estos.[6]

Tal como afirma Sueiro[7] la prueba electrónica distingue de la prueba física por su naturaleza particular que la caracteriza por ser intangible, latente, volátil, frágil y sensible en su integridad e inalterabilidad. Resulta intangible por el hecho de estar almacenada en códigos y diversos niveles de lenguaje lo que implica una evidencia que no es corpórea, material o física.

Estos rasgos distintivos implican que su tratamiento (en la adquisición, recolección, peritaje y conservación) sea muy distinto del que se le otorga a la evidencia física.

Entonces, podemos afirmar sin lugar a dudas que, respecto a la evidencia digital, el tratamiento es distinto y por ende existen principios específicos que lo gobiernan tales como la relevancia, la suficiencia y la confiabilidad[8].

La relevancia se identifica como un concepto netamente técnico jurídico y refiere a la pertinencia de la información en relación al hecho que se investiga. Su finalidad es dar firmeza (sea como prueba de cargo o de descargo) a la hipótesis que se intenta acreditar.

Por otro lado, la suficiencia que implica que la información aportada por el medio probatorio sea completa, de modo tal que podamos sustentar y verificar los elementos puestos en la investigación.

Finalmente, la tercera característica que gobierna a este tipo de evidencia es la confiabilidad entendida como validar la repetibilidad y auditabilidad del proceso aplicado para la obtención de la evidencia digital. Implica que la evidencia que se extraiga a través de un proceso pueda ser extraída en iguales condiciones y con el mismo alcance, si un tercero aplica el mismo proceso.

En esta línea, ha tenido amplia difusión y adhesión por parte de los organismos judiciales el manual de buenas prácticas forenses, más conocido como normas ISO/IEC 27037:2012 que, en concreto, establece el conjunto de reglas que deben ser cumplidas en

---

[6] Devis Echandía, H. (1972). *Teoría general de la prueba judicial* (T. 1). Zavalía.

[7] Sueiro, C. C. (2019). La obtención de prueba digital de la computación de la nube. En H. R. Granero (Ed.), *E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías* (2.ª ed., pp. 390–391). Albremática (elDial.com).

[8] Procuración General de la Nación. (2016). *Guía de obtención, preservación y tratamiento de evidencia digital* (Res. PGN 756/2016).

el marco de la investigación forense digital para que el tratamiento de la evidencia digital sea apropiado y la misma admisible en el proceso judicial cumpliendo las características ya enunciadas previamente.

Las reglas a las que refiere la norma ISO/IEC 27037:2012 pueden simplificarse en cuatro, a saber:

1. Mínima manipulación de ejemplares originales evitando así la adulteración, modificación o contaminación de la evidencia remitida a estudio;
2. Reportar cada cambio, ante una manipulación de la evidencia inevitable (por ejemplo, al encender un teléfono celular) dicha actividad debe ser documentada indicando el agente que intevino, las razones que motivaron la manipulación y el alcance o extensión del procedimiento empleado;
3. Cumplir con las reglas del tratamiento de evidencia digital, las cuales se han descripto en párrafos anteriores;
4. Finalmente, no exceder el conocimiento propio, esto es, ante un tratamiento de evidencia que excede la capacidad de conocimiento del investigador, solicitar la cooperación de terceros con mayor experiencia o conocimiento en la temática.

Surge de lo estudiado que el tratamiento de la evidencia digital difiere notoriamente del tratamiento de cualquier otro tipo de prueba. Las características particulares del tratamiento al que debe ser sometida la misma no ofrece mayor complejidad e implica que quien la manipula debe hacerlo con especial responsabilidad, un error –que luego mutará a una cadena de errores- puede derivar en la inadmisibilidad probatoria y, con ello, en la falta de sustento a la hipótesis que intentemos acreditar en el proceso.

Expresamente las reglas de buenas prácticas forenses para el tratamiento de la evidencia digital prevén protocolos de actuación para que dicha evidencia sea admitida formalmente y que de este modo se evite la introducción de componentes adicionales en el marco de la investigación que tornen «poco confiable» a la evidencia introducida.

Como consecuencia lógica, la introducción de evidencia poco confiable (sin respetar protocolos de actuación) derivará en una lesión a la garantía del juicio previo y derecho de defensa, toda vez que el imputado en el marco de un proceso penal tiene la facultad de *controlar la prueba de cargo que podrá ser utilizada válidamente en la sentencia.*[9] El fundamento de una sentencia por medios poco confiables o que no se ajusten a técnicas protocolares ni a buenas prácticas, podrá derivar en un pronunciamiento arbitrario con la consecuente condena de un inocente por lo que, el derecho de defensa implica la posibilidad de revisar que la metodología empleada en la producción probatoria sea acorde a la disciplina a la que pertenece la evidencia en estudio.

a. El proceso penal informático ¿Existe anomia procesal respecto a los medios de investigación?

Ahora bien, teniendo en cuenta lo relatado hasta este punto, surge claro un interrogante y es: en el marco de la investigación penal informática, ¿existe, a nivel nacional, un conjunto de normas que regulen el procedimiento de obtención de evidencia digital acorde a las garantías constitucionales y que sea efectivo frente a la prevención del delito informático? La respuesta, entiendo, se inclina por la negativa. Independientemente de los manuales de buenas prácticas, adhesiones protocolares y

[9] Maier, J. B. (2004). *Derecho procesal penal: Fundamentos* (T. I, 2.ª ed.). Editores del Puerto.

resoluciones ministeriales, no contamos con un sistema normativo que regule la investigación en el proceso penal informático y que permita el empleo de programas –aún malicioso - con la finalidad de prevenir y sancionar el delito.

Lo antedicho genera lógica preocupación dado que los inminentes avances tecnológicos a los que nos exponemos como sociedad terminan colisionando con un sistema que podríamos caracterizar como «vetusto» en lo que refiere a recolección y tratamiento de evidencia digital.

Si a lo anterior le adicionamos que las nuevas estructuras delictivas por lo general se desarrollan en un marco en donde se emplean cada vez con mayor regularidad medios digitales para la organización y comisión de los delitos, la investigación penal por parte de los agentes de prevención necesariamente debe modernizarse hacia el empleo de nuevas tecnologías que permitan investigar sin perforar esa barrera que forma el llamado derecho a la intimidad. Piénsese, por ejemplo, en el empleo de programas que permiten simular una IP o incluso ocultarla de los investigadores (por ejemplo, navegador *Tor*[10]), o en aquellos dispositivos que eliminan o bloquean la inform0ación ante reiterados intentos de acceso indebido, o en los diversos algoritmos que simulan actividad distinta a la que en realidad se ejecuta, las probabilidades y situaciones son inimaginables e inagotables.

Pues bien, en el contexto detallado podemos entonces suponer que la inexistencia de normas que regulen este tipo de investigación podría derivar en un serio problema constitucional. Esto es, nuestra constitución nacional en su art. 18 establece los alcances de las garantías constitucionales y los principios que deben regir el proceso entre los que se encuentra el principio de legalidad. Dicho plexo normativo, en el art. 28 indica que «los principios, garantías y derechos reconocidos en los anteriores artículos, no podrán ser alterados por leyes que reglamenten su ejercicio».

Del simple razonamiento deductivo entonces podemos arriesgarnos a suponer que, si las normas vigentes regulan procesos de investigación para épocas en donde los avances tecnológicos no eran tan masivos como los actuales y en donde las tecnologías empleadas no gozaban de la inmediatez y el alcance que tienen hoy, por ejemplo, los teléfonos celulares; ¿qué alternativa –que no atente con aquellos principios, derechos y garantías constitucionales- le queda a un investigador que tiene que valerse de programas o protocolos que no tienen una finalidad preventiva sino, a nuestro modo de ver, que sirven para la etapa ex post, es decir meramente punitiva? El ejercicio de la defensa eficaz en un proceso de recolección de evidencia digital que no sea confiable o empleando métodos poco claros, conforme lo hemos relatado con anterioridad, se vería seriamente afectado.

En esta exposición de interrogantes toman relevancia dos aspectos, por un lado, la confiabilidad de la información obtenida a través de programas determinados y, por el otro, de tratamiento obligado en esta temática, el empleo de malware por parte de los agentes de investigación.

Lo planteado en el párrafo anterior ha sido objeto de tratamiento por la jurisprudencia norteamericana en dos precedentes que, entiendo, resultan de interés para terminar de comprender cómo una regulación normativa en este tema resulta útil y necesaria de cara al proceso penal informático:

[10] Según se indica en el sitio oficial del proyecto Tor, el navegador Tor permite acceder a Internet mediante un sistema de «capas» que garantiza la privacidad del usuario. Este diseño posibilita la navegación sin que la actividad sea monitoreada y sin que queden rastros identificables.

b. United States v. Ocasio (2013)[11]

En el caso el señor Angel Ocasio fue acusado de poseer pornografía infantil en su computadora. Dicho hallazgo se produjo mediante el uso de un programa denominado CPS (*Child Pornography System*, por sus siglas en inglés). El funcionamiento de dicho programa consiste en ubicar material (archivos) relacionado con pornografía infantil en diversas redes e internet.

Haciendo uso del derecho que le confiere la cuarta enmienda, el señor Ocasio solicitó judicialmente que la empresa fabricante del software indicara cómo funcionaba el mismo, ya que los archivos se encontraban en carpetas privadas para las cuales no había otorgado autorización de acceso, violando de este modo los principios de la constitución americana.

La empresa fabricante planteó que no se encontraba obligada a proporcionar dicha información argumentando que se encontraba amparada por el secreto empresarial.

En síntesis, el fallo obligó a la empresa a facilitar dicha información respecto del código fuente del programa bajo protecciones legales que permitan impedir que sea perjudicada comercialmente y amparando el derecho de Ocasio a que se revelen dichos datos a fin de cotejar que el método empleado no implicaba atentar contra sus derechos constitucionales.

La importancia del caso resulta en facilitar –en el marco de la investigación penal informática- datos que permitan identificar si el método de recolección de información resulta confiable y, por otro lado, si ese método lesiona garantías constitucionales.

c. «*Playpen*»[12]. La reforma a la «Regla 41» y el empleo de malware en el acceso transfronterizo de datos.

En lo que es conocido como uno de los casos más relevantes en materia de investigación penal informática, «*Playpen*» viene a sentar precedentes sobre el uso de «malware» por parte de las fuerzas de seguridad quienes, a través del empleo de este tipo de programas maliciosos logran acceder a información que permite identificar a los ciberdelincuentes.

Si bien las autoridades lograban interceptar el intercambio de datos prohibidos, el problema aparecía al momento de identificar el origen de dicha difusión. Por este motivo, lograron –a través de una orden judicial emanada por un Juez del Estado de Virginia- emplear el programa denominado *network investigative technique* (NIT) que permitía identificar el origen del material de difusión.

En cuanto a la modalidad de funcionamiento, el programa permite el ingreso en el dispositivo (sin autorización) de quien se sospecha, con la posibilidad de administrar

[11] *United States v. Ocasio* (No. EP-11-CR-2728-KC, W.D. Tex., 6 de junio de 2013), la Corte del Distrito Oeste de Texas —División El Paso— analizó diversos aspectos vinculados a la investigación de delitos cometidos en entornos digitale.

[12] «Playpen» era una plataforma ubicada en la denominada «deep web» o «dark web», utilizada por redes dedicadas a la producción, distribución y consumo de material de explotación sexual infantil. A partir de su descubrimiento se inició una de las investigaciones más extensas contra estructuras internacionales de pedofilia y tráfico de pornografía infantil. Los hechos relevantes del caso se encuentran detallados en Aboso (2022, pp. 335–336).

todos los sitios y funciones. De este modo, se puede acceder a la totalidad de información de quien consume el material, como de quien lo difunde.

En el caso de marras, las fuerzas de seguridad administraron durante un tiempo considerable la web logrando identificar a una gran cantidad de usuarios (con sus direcciones de IP incluidas). Esto permitió formular cargos criminales contra al menos doscientos usuarios cuyos domicilios escapaban a la jurisdicción del juez que emitió la orden autorizando el uso del «malware», siendo ésta una de las principales aristas del caso y dando lugar a la reforma de la denominada «regla 41»[13].

La «regla 41» permite entonces que un Juez, independientemente del distrito en donde se encuentre, secuestre datos de un dispositivo electrónico sin que las autoridades lo tengan en su poder o en el lugar en que se encuentran. El empleo del malware para acceder de manera remota permitía a los investigadores identificar la IP desde la que se conectaba el usuario y de ese modo, allanando la morada, lograr su aprehensión. El empleo del NIT como plataforma para acceder al sitio e identificar las IP y las órdenes judiciales emanadas en consecuencia fueron objeto de numerosas impugnaciones por parte de los usuarios, las que se concentran en tres: a) falta de jurisdicción del juez federal para emitir la orden que autorizaba el empleo del malware; b) falta de motivación de la medida judicial y c) actuación de buena fe por parte de la autoridad al momento de ejecutar la medida.

Sobre el primer agravio se argumentó que, dado que los usuarios se conectaban desde lugares que no estaban en la jurisdicción del juez de Virginia, la medida carecía de validez, toda vez que la misma FRCP establecía la limitación a la procedencia de órdenes de allanamiento y registro fuera de la propia jurisdicción del magistrado. La respuesta fue una interpretación flexible de la jurisprudencia de la corte americana en el sentido de que la jurisdicción era válida toda vez que lo determinante es el lugar en donde se halla el servidor al cual se conecta el usuario y no el lugar o locación en la que se halla el usuario al momento de conectarse.

En relación al segundo agravio, se argumentó que el criterio de la locación del servidor no siempre se ha utilizado en el caso de los ciberdelitos como los de abuso sexual infantil o distribución de pornografía infantil. El criterio rector en estos casos ha sido el contrario (locación de la conexión de la dirección de IP)

En cuanto al último argumento, los tribunales fundamentaron la validez del procedimiento en el hecho de que la autoridad no actuó de manera deliberada, sino que actuó de buena fe. Se amparó en esto casos en que el agraviado no especificó cuál fue el perjuicio sufrido, y que en el caso no aplicaba la expectativa razonable de privacidad, toda vez que al acceder al intercambio de información con el servidor que proporciona los datos, dicha expectativa se torna difusa. En definitiva, el objetivo de la defensa era lograr la exclusión probatoria argumentando que el empleo de este tipo de programas resultaba en una actuación deliberada por parte de la autoridad y, por ende, la obtención de prueba en este sentido era ilegal.

Sin embargo, tal como refiriera al comienzo del párrafo anterior, los tribunales entendieron que el uso del NIT por parte de las fuerzas de seguridad no quebrantaba la

[13] La «Regla 41» integra el compendio de las reglas federales del procedimiento penal de los Estados Unidos (*Federal Rules of Criminal Procedure*, FRCP). Entre otros aspectos, habilita a los jueces federales a emitir órdenes que permiten a las fuerzas de seguridad acceder de manera remota a equipos informáticos, con prescindencia del lugar físico donde se encuentren.

tutela a garantías judiciales reconocidas por la Cuarta Enmienda, toda vez que las autoridades habrían justificado una causa probable de comisión de delitos y, a través de este tipo de medidas y el empleo de este tipo de programas descubrieron lugares y efectos para secuestrar.

El uso del malware se justificaba porque, tal como lo hemos referido al inicio de este acápite, los ciberdelincuentes hacen uso de herramientas que permiten disuadir a los investigadores y son éstos quienes deben valerse de herramientas similares (muchas de ellas catalogadas como «malware») con la finalidad de prevenir y sancionar la comisión de este tipo de hechos. El uso de estos «programas electrónicos de rastreo facilita la búsqueda y asegura en gran medida la posibilidad de identificar al cibernauta»[14]

De lo estudiado hasta aquí podemos advertir que, si bien no se encuentra exenta de críticas el compendio de reglas federales del procedimiento penal se encarga de reglamentar cómo debe procederse en investigaciones vinculadas con evidencia digital, amoldándose así a los avances tecnológicos sin dejar de lado la tutela a garantías constitucionales reconocidas por la cuarta enmienda. Con similar criterio y un carácter funcional, entiendo que resulta prioritario contar con una regulación procesal que permita tratar el uso de este tipo de programas en el proceso penal con el alcance suficiente para que su empleo no implique una lesión a principios constitucionales.

También comprendemos que no todo es válido (ni siquiera la buena fe del funcionario) en el marco de una investigación judicial, y si bien producto de ello podría obtenerse evidencia que resulte en el descubrimiento de la comisión de un hecho delictivo, sea de manera preventiva o con el fin de iniciar un proceso penal, la norma está escrita y forma parte de nuestro Estado; no podemos so pretexto de prevenir el delito, actuar sin miramientos de la norma constitucional, por ello es necesaria una regulación clara y contundente para que el «debido proceso» como garantía no se vea alterado por la finalidades indicadas.

4. Metadatos e información asociada: conceptualización, criterios para su incorporación al proceso penal y exigencia de orden judicial previa conforme al Código Procesal Penal Federal

Al momento de definir qué entendemos por «metadatos» o «información asociada», no podemos pasar por alto el contexto en el que nos encontramos. Tal como hemos venido remarcando a lo largo de este trabajo, la era digital ampliamente caracterizada por el gran cúmulo de información que se almacena en los dispositivos electrónicos, forma parte fundamental de la vida cotidiana.

En este escenario, cada vez más influenciado por tecnologías (en uso y nuevas) resulta interesante ingresar en el estudio de cómo se procesa esa información y cómo la misma puede incluirse en la investigación penal informática. Ello es así porque las nuevas tecnologías implican, a la vez que mayores comodidades para los quehaceres cotidianos –sean personales, laborales o financieros- la aparición de nuevas formas de delito.

[14] Aboso, G. E. (2023). *Evidencia digital en el proceso penal: La investigación forense en el entorno digital y la validez de las garantías constitucionales*. Euros Editores SRL.

Los metadatos o información asociada vienen a formar parte de la información que se «asocia» a un elemento determinado, de allí el término «información asociada» o «datos asociados». En este sentido son variadas y numerosas las definiciones sobre metadatos que, por lo general, se resumen en el adagio «datos sobre datos»; aunque la definición resulta más amplia y variada, tal como afirma Mayernik[15]:

> […] se ofrece un puñado de definiciones de metadatos que ilustran como pueden ser desde muy específicas hasta muy genéricas: Greenberg (2003, p. 1876): «datos estructurados sobre un objeto que posibilitan funciones asociadas al objeto designado». Greenberg (2005, p. 20): «atributos de datos que describen, aportan contexto, indican la calidad, o documentan características de otro objeto (o dato)». Smiraglia (2005, p. 2): «descripciones estructuradas de recursos de información, diseñadas para potenciar la recuperación de información». Gilliland (2008, n.p.): «la suma total de lo que se puede decir de cualquier objeto informativo a cualquier nivel de agregación». Pomerantz (2015, p. 26): «Los metadatos son declaraciones sobre un objeto potencialmente informativo».

De lo expuesto entonces concluimos que pese a ser variadas las definiciones los metadatos o información asociada o datos asociados son aquellos elementos que aportan información sobre un contenido (objeto) informativo. También surge que las definiciones son infinitas y no es objeto de este trabajo el ingresar en conceptualizaciones sumamente científicas o específicamente destinadas a áreas puntuales, sino brindar una aproximación a qué debemos entender cuando nos referimos a metadatos o datos asociados.

Pues bien, a modo de ejemplo podríamos decir que, respecto de una llamada telefónica el objeto o contenido propiamente dicho será la comunicación entre los interlocutores y, los datos asociados o información asociada serán los datos aportados por la prestadora de servicios de telefonía que permitan identificar los abonados, fecha, hora y duración de la llamada y hasta la ubicación de cada abonado; lo mismo ocurrirá, por ejemplo, en el caso de direcciones de IP para conexiones a determinados sitios de la web, en donde la dirección de IP contendrá, como dato asociado, domicilio, ubicación, tiempo de conexión, entre otros, del usuario.

Entonces, para recapitular, ¿cómo debe o puede incorporarse esa información al proceso penal informático a fin de evitar el quebrantamiento de garantías como la inviolabilidad de las comunicaciones, el derecho a la privacidad, entre otras? ¿Es necesario contar con una orden determinada?

En nuestro país, tal como se afirmado en puntos anteriores, no contamos con una norma específica que establezca cuál es el modo en que deben o pueden obtenerse los metadatos; la denominada anomia procesal afecta en este punto a la investigación penal y termina por limitar el contenido de la información que puede obtenerse al registro de comunicaciones telefónicas en una norma cuanto menos cuestionable[16].

En efecto, la norma procesal nada dice respecto a la obtención de datos asociados a dichas comunicaciones ni cuál es el alcance de las facultades de la acusación en este punto. Lo hemos expuesto ya, la doctrina entiende que la información contenida en dichas

[15] Mayernik, M. (2020). *Metadata*. In B. Hjørland & C. Gnoli (Eds.), *Encyclopedia of Knowledge Organization* (Version 1.0, published 2020-03-16; last edited 2020-12-23). ISKO. https://www.isko.org/cyclo/metadata

[16] El artículo 236 del Código Procesal Penal de la Nación (Ley 23.984) autoriza al juez, mediante auto fundado, a disponer la intervención de las comunicaciones telefónicas del imputado «para impedirlas o conocerlas». Asimismo, faculta al Ministerio Público Fiscal a adoptar la misma medida en casos de urgencia, con la sola obligación de comunicar su realización al magistrado instructor.

comunicaciones goza de protección constitucional, ergo, toda intervención de dicha información debe ser sustentada en una orden judicial emanada de autoridad competente, en este caso, el magistrado instructor.

Ahora bien, la doctrina (y jurisprudencia) no son uniformes en cuanto a la protección que debe brindarse a la información asociada y, por ende, cómo debe introducirse al proceso penal.

En el caso *Mitchell*, la Cámara Federal de Casación Penal entendió que los datos asociados a las comunicaciones telefónicas realizadas por el imputado gozan de protección constitucional ya que el derecho a la intimidad no se limita sólo al contenido *per se* de la comunicación, sino también a los datos asociados a la misma.

Entendemos que en el caso *Halabi*, está la respuesta sobre el alcance constitucional que debe otorgarse a los metadatos y radica en la fuente de la norma que es de carácter constitucional y por tal motivo el proceso penal no puede apartarse de dicha protección.

Si consideramos lo previsto en el código procesal penal federal (ley 27.063 y sus modificatorias) el panorama resulta tajante. En una concepción que interpreto más antropocéntrica la intimidad, así como la privacidad del individuo sólo pueden verse afectadas en el marco de un proceso penal cuando medie orden judicial.

En su art. 13 el CPPF determina que

> Se debe respetar el derecho a la intimidad y a la privacidad del imputado y de cualquier otra persona, en especial la libertad de conciencia, el domicilio, la correspondencia, los papeles privados y las comunicaciones de toda índole. Sólo con autorización del juez y de conformidad con las disposiciones de este Código podrán afectarse estos derechos.

Entiendo necesario detenernos en la frase «comunicaciones de toda índole» ya que abarca no solo comunicaciones telefónicas, sino a aquellas de cualquier tipo que, jurisprudencialmente son asimiladas a la protección prevista en art. 19 de nuestra carta magna en tanto «nadie puede ser objeto de injerencias arbitrarias en su vida privada, ni la de su familia, en su domicilio o su correspondencia»[17]

Una interpretación global de la norma analizada en conjunto con principios rectores del proceso penal constitucional, nos permiten concluir en que la expectativa razonable de privacidad, así como el principio de autodeterminación de los individuos, limitan la injerencia del estado en las comunicaciones de los individuos y ello no se cierne únicamente a las comunicaciones de índole telefónica, sino a todo tipo de actividad sobre la que el individuo posea una expectativa razonable de privacidad. Será el Estado en conjunto con las empresas prestatarias de estos servicios quienes deberán arbitrar los medios para que la proporción de información asociada sea efectuada respetando estandartes locales y supranacionales

5. Conclusiones

La evidencia digital ha tomado una enorme trascendencia en el marco del proceso penal informático, aunque no sólo ajustada a delitos cibernéticos o «ciberdelitos». En los tiempos actuales el empleo de dispositivos electrónicos de almacenamiento de datos es prácticamente unánime y se aplica a todos los aspectos de la vida cotidiana por lo que,

[17] Corte Suprema de Justicia de la Nación. (2010). *Quaranta, José Carlos s/ infracción Ley 23.737* (Fallos 333:1674).

podemos afirmar sin lugar a dudas que la vida de la persona –inclusive las relaciones intersubjetivas- se ve atravesada y reflejada por los datos que se almacenan en dichos dispositivos.

A lo largo del artículo hemos brindado una pequeña introducción a un tema que trasciende fronteras y que posee múltiples aristas pero que, sobretodo, se caracteriza por su actualidad.

En este escenario, no podemos desentendernos de la complejidad que reviste la evidencia digital y cómo resulta imperioso dotar de integridad y autenticidad a la misma a lo largo del proceso penal, lo que se traducirá en el respeto a garantías constitucionales y a un ejercicio óptimo de la judicatura. Sin embargo, carecemos actualmente de un plexo normativo ritual que regule específicamente el derecho penal informático y cómo el Estado debe gestionar este tipo de evidencia. Escuchas, imágenes de video, fotografías, movimientos bancarios, correspondencia electrónica, datos de navegación, entre miles de otras pruebas carecen de un andamiaje normativo acorde, actualizado a los tiempos que corren quedando prácticamente desprotegidos en un claro «atentado» contra la ritualidad y seriedad que caracteriza al proceso penal, pero también contra el imputado y con la sociedad toda que delega en manos del Poder Judicial la tutela de los derechos y garantías consagrados.

Es este el gran dilema del derecho penal contemporáneo al que la legislación y el servicio de justicia deben enfrentarse con el fin de resultar funcionales a la sociedad sobre la que rigen.

6. Bibliografía

Aboso, G. E. (2023). *Evidencia digital en el proceso penal: La investigación forense en el entorno digital y la validez de las garantías constitucionales*. Euros Editores SRL.

Bujosa Vadell, L. M., Bustamante Rúa, M. M., & Toro Garzón, L. O. (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, 7(2), 1347–1384.

Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Academic Press.

Código Procesal Penal de la Nación (Ley 23.984).

Código Procesal Penal Federal (Ley 27.063 y mod.).

Corte Suprema de Justicia de la Nación. (2010). *Quaranta, José Carlos s/ infracción Ley 23.737, causa N.º 763* (Fallos 333:1674).

Devis Echandía, H. (1972). *Teoría general de la prueba judicial* (T. 1). Zavalía.

Maier, J. B. (2004). *Derecho procesal penal: Fundamentos* (T. I, 2.ª ed.). Editores del Puerto

Ministerio Público Fiscal & Ministerio de Seguridad. (2023). *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*. https://www.fiscales.gob.ar

Mayernik, M. (2020). Metadata. *Knowledge Organization*, 47(8), 696–713. https://doi.org/10.5771/0943-7444-2020-8-696

Mayernik, M. (2023). *Metadatos* (S. S. Miralles, Trad.). *Anales de Documentación*, 26. Universidad de Murcia. (Traducción de la entrada publicada en la Encyclopedia of Knowledge Organization.)

Procuración General de la Nación. (2016). *Guía de obtención, preservación y tratamiento de evidencia digital* (Res. PGN 756/2016).

Sosa, M. E. (2023). *Evidencia digital: Su importancia en la investigación*. Revista Pensamiento Penal, (466), 1

Sueiro, C. C. (2019). La obtención de prueba digital de la computación de la nube. En H. R. Granero (Ed.), *E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías* (2.ª ed., pp. 390–391). Albremática (elDial.com).

United States v. Ocasio, No. EP-11-CR-2728-KC (W.D. Tex. June 6, 2013).

Artículos

Revista Pensamiento Penal
Sección Derecho procesal y procesal penal
Vol. 2, núm. 4 – 2025, págs. 29–39
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/c5eqwt67

Requisa personal y vehicular: un abordaje desde la jurisprudencia del fuero provincial de Entre Ríos

Damián Esteves[1]

Resumen

El trabajo examina cómo la jurisprudencia entrerriana ha precisado los conceptos jurídicos indeterminados que habilitan las requisas personales y vehiculares, ante la escasa regulación del código procesal penal local y el marco constitucional del artículo 18 de la constitución nacional. A partir de los estándares fijados por la corte interamericana de derechos humanos en «Fernández Prieto y Tumbeiro vs. Argentina», se analiza cómo los tribunales han definido cuándo existen «motivos suficientes» y en qué supuestos es legítimo prescindir de la orden judicial por considerarse la medida «urgente e impostergable». El estudio destaca la importancia decisiva de las actas policiales para el control judicial ex post, así como los principales escenarios en los que se admiten estas intervenciones sin autorización previa: flagrancia, descarte de elementos vinculados a delitos, amenazas con armas y contextos adversos que comprometen seguridad o evidencia. También se identifican casos donde la falta de urgencia invalida la actuación policial, como en operativos rutinarios o intervenciones premeditadas. En conjunto, el análisis evidencia tensiones persistentes entre facultades policiales y exigencias constitucionales, subrayando la necesidad de mayor precisión normativa en materia de requisas.

Sumario

Palabras clave

requisa personal – requisa vehicular – control judicial – actuaciones policiales – Fernández Prieto y Tumbeiro

[1] Abogado (Universidad Nacional de Rosario). Especialización en derecho de daños (Universidad Católica Argentina, *en curso*). Correo electrónico: estevesdamian7@gmail.com

1. Consideraciones preliminares

«Motivos suficientes», «indicios vehementes de culpabilidad», «sospecha razonable», actos «urgentes e impostergables», entre otros, se encuentran entre los más comunes conceptos jurídicos indeterminados utilizados por la legislación penal a la hora de contornear las medidas que habilitan la intromisión en la libertad e intimidad de las personas por parte del Estado, resultando por ello de gran importancia la precisión de tales criterios so pena de autorizar injerencias arbitrarias en la esfera de garantías constitucionales de las personas. No obstante, resulta común que las legislaciones procesales carezcan de elementos suficientes que permitan determinar cuándo nos encontramos frente a tales circunstancias de excepción, provocando con ello respuestas judiciales inconsistentes. En tal sentido, la problemática alrededor de la delimitación de tales estándares de excepción ha sido objeto de numerosos precedentes jurisprudenciales y desarrollos doctrinarios tanto a nivel nacional como provincial, resultando la más reciente la asunción de responsabilidad llevada adelante por argentina ante la corte interamericana de derechos humanos (en adelante, «Corte IDH») como consecuencia de sus precedentes «Fernández Prieto y Tumbeiro vs. Argentina».

Considerando tal problemática, proponemos sentar foco en el código procesal de Entre Ríos (en adelante, «CPPER») y particularmente respecto a aquellos precedentes jurisprudenciales donde se debate la legalidad de la ejecución de requisas personales y vehiculares, medios probatorios que no solo comparten la tendencia nacional de utilizar aquellos conceptos que han sido catalogados por la Corte Interamericana de Derechos Humanos (en adelante, «Corte IDH») en «Fernández Prieto y Tumbeiro vs. Argentina» (2020) como «vagos», «ambiguos» y «carentes de parámetros objetivos», sino que también sufren de una exigua regulación normativa, generando en la práctica judicial dilemas a la hora del control de legalidad en la ejecución de tales medidas.

Consecuentemente, procederemos a realizar un breve estudio compilado de diferentes fallos judiciales de la provincia de Entre Ríos, enfocándonos en esclarecer cómo ha delineado la justicia entrerriana los estándares establecidos por la ley penal a la hora de juzgar sobre la legalidad de requisas personales y vehiculares, todo ello considerando desde las más recientes críticas y lineamientos establecidos por la Corte IDH.

2. Concepto y elementos normativos

A modo de introducción, indicamos que doctrinariamente se ha definido a la requisa como aquella:

> Medida de coerción auxiliar que tiene por objeto detectar, y en caso de resultar procedente y necesario secuestrar, efectos que llevara consigo una persona o que estuvieran disponibles dentro de su radio de desenvolvimiento (valija, billetera, bolso, etc.) y que de algún modo se encuentren vinculados con el objeto procesal. (Chiara Diaz, 2017: 658)

Como toda medida de investigación, ésta se encuentra regulada por los ordenamientos jurídicos procesales de cada provincia, ahora bien, ¿con qué marco normativo estamos trabajando en la provincia de Entre Ríos? Particularmente, la norma principal a estudiar resulta ser nuestro CPPER, el cual, sin embargo, debemos destacar que no se caracteriza por brindar al operador jurídico una vasta regulación legal de institutos como el que se encuentra bajo análisis, por el contrario, la requisa personal está

escuetamente recibida mediante sus artículos 275 y 276, normas que habrán de complementarse con las facultades policiales de urgencia legisladas en el artículo 208 inciso 5. Es más, esta deficiencia normativa se extrema a tal punto de que la requisa vehicular carece de regulación legal alguna salvando una mera alusión a la potestad policial de llevar a cabo «registros vehiculares» en casos urgentes e impostergables, sin establecer más presupuestos. Consecuentemente, considerando estas carencias normativas, nos abocaremos en primer término a comprobar cómo tales normas se ajustan al esquema de garantías constitucionales establecido por el artículo 18 de nuestra constitución nacional, para luego brindar una estructura sobre cuáles son los presupuestos legales de ambos institutos y sobre cómo se ha suplido la ausencia normativa propia de la requisa vehicular.

a. Orden judicial y casos de urgencia.

El artículo 18 de la Constitución Nacional dispone que «nadie puede ser arrestado sino en virtud de orden escrita de autoridad competente»; garantía que ha sido comúnmente caracterizada tanto por doctrina como jurisprudencia como una notable preferencia por que las decisiones vinculadas con la ejecución de actos estatales que impliquen la intromisión en la libertad e intimidad de las personas queden en manos de los jueces (Carrió, 2000: 2).

De tal manera, estimamos que tal garantía es abiertamente recibida por el CPPER, en especial al regular el instituto de la requisa personal, estableciendo:

> Artículo 275.- Requisa personal. El juez de Garantías, a requerimiento del Fiscal, ordenará la requisa de una persona, mediante decreto fundado, siempre que exista motivo suficiente para presumir que ella oculta en sus vestimentas o cuerpo, cosas relacionadas con el hecho descripto en la Apertura de Causa. Antes de proceder a la medida deberá invitársela a exhibir el objeto de que se trate.

Por ende, respetando las prescripciones del artículo 18 de la CN, la norma procesal condiciona la legalidad de la requisa personal al previo cumplimiento de dos requisitos: en primer lugar, el ordenamiento de la medida por el juez de garantías; y en segundo lugar, que tal medida se sustente en motivo suficiente para presumir el ocultamiento en vestimentas o cuerpo de una persona de cosas relacionadas con el hecho que haya sido descrito en el auto de apertura de causa.

Sin embargo, resulta lógico prever la existencia de situaciones en las cuales el requerimiento de una orden judicial frustraría las actividades de prevención policial o, incluso, en las que no existiera apertura de causa al momento de su ejecución; imagínese no poder requisar a una persona aprehendida en flagrancia, o en un contexto donde resulte imposible el requerimiento de autorización judicial sin perjudicar su eficacia o poner en riesgo la integridad del personal policial. Tales circunstancias son las que han derivado en la incorporación en los códigos de procedimientos de artículos como el 208 inciso 5 de nuestro ordenamiento procesal, facultado a los funcionarios policiales a llevar a cabo tales medidas sin intervención judicial previa, siempre y cuando las mismas se manifestaren como «urgentes e impostergables». De esta forma, se dispone que:

> ARTÍCULO 208.- Atribuciones de la Policía. Son atribuciones y deberes de la Policía: (...) 5) Proceder a los allanamientos, requisas, registros vehiculares y secuestros urgentes e impostergables, de conformidad a lo dispuesto en los artículos 271, 275 y demás disposiciones de este Código, dando inmediato aviso al Fiscal en turno o a cargo de la investigación según el caso.

En concreto, se faculta al personal policial a llevar adelante requisas y registros vehiculares siempre que los mismos presenten calidad de urgentes e impostergables, incurriendo en la falencia de no determinar cuándo se presentan tales circunstancias -cuestión que abordaremos con posterioridad en el presente-.

Empero, destacamos que la premura de la medida nunca habrá de ser causal suficiente para soslayar la necesidad de que su ejecución satisfaga los estándares legales para habilitar una restricción de la libertad e intimidad de las personas, es decir, nunca la urgencia e impostergabilidad de su ejecución habrá de excluir la necesidad de que el acto se fundamente en motivos suficientes de que se ocultan en las vestimentas o cuerpo del requerido cosas relacionadas con un hecho delictivo, debiendo tales circunstancias surgir de forma previa a la realización de la medida y no como consecuencia de ella, de lo contrario, la fuerza policial carecería de todo incentivo para solicitar órdenes judiciales, gozando así de mayores facultades que los propios magistrados del poder judicial (Carrió, 2000: 4)

i. *¿Cómo suplir la ausencia de regulación de la requisa vehicular?*

Como fue indicado en el preliminar del presente trabajo, nuestra norma procesal resulta escueta en lo que respecta a regulación de las requisas vehiculares, meramente siendo mencionada la facultad policial de llevar a cabo «registros vehiculares» urgentes e impostergables con aviso inmediato al fiscal de turno o a cargo de la investigación. Consecuentemente, nos proponemos analizar cómo ha suplido la jurisprudencia entrerriana esta carencia normativa en los casos concretos a la hora de controlar la legalidad de estas medidas de prueba.

Particularmente, precedentes jurisprudenciales han tomado la doctrina emanada de la Corte IDH en «Fernández Prieto y Tumbeiro vs. Argentina», donde ha sentado que los vehículos forman parte del espacio de intimidad resguardado por el artículo 18 CN, afirmando que:

> Las pertenencias que una persona lleva consigo en la vía pública, incluso cuando la persona se encuentra dentro de un automóvil, son bienes que, al igual que aquellos que se encuentran dentro de su domicilio, están incluidos dentro del ámbito de protección del derecho a la vida privada y la intimidad. Por esta razón, no pueden ser objeto de interferencias arbitrarias por parte de terceros o las autoridades (párr. 102).

Frente esta interpretación por parte de la Corte IDH, precedentes de nuestra provincia han considerado que el artículo 268 CPPER -norma que habilita, previa orden del juez de garantías, a requerimiento del fiscal, al registro de un lugar cuando hubieren motivos suficientes para presumir que en el mismo se encuentran personas o existen cosas relacionadas con un delito- resulta aplicable a los vehículos, incluyendo por ende a los automotores u otros espacios que gocen de cierto ámbito de intimidad, pues integran el ámbito de privacidad de su dueño o tenedor circunstancial (tribunal de juicio y apelaciones de Paraná, N°21488, 2023). Por ende, la requisa de un vehículo debería cumplir con los mismos estándares que son requeridos para el registro de las personas o de determinados lugares, es decir, «motivos suficientes» y orden judicial previa emitida por juez de garantías salvo, con respecto a ésta última, circunstancias de urgencia e improrrogabilidad de la medida.

Por el otro lado, también se ha interpretado que la autorización para la ejecución de una requisa «personal» implicaría una habilitación que va más allá del registro corporal de

una persona, abarcando los objetos que ésta porta consigo, como lo son su mochila, bolso, billetera, y donde podría abarcar también el vehículo que se encuentra conduciendo, ya que la habilitación a registrar un espacio tan íntimo como lo es el corporal, debería permitir registrar los demás espacios «menos íntimos» que lo rodean (Baclini y Schiappa Pietra, 2017: 393)

Ahora bien, tomando en consideración que el registro del cuerpo, vestimenta y vehículo de una persona habrá de resultar fundado si median motivos suficientes para presumir que en ellos se ocultan cosas relacionadas con un hecho delictivo, es que planteamos: ¿cuándo se satisface el estándar de «motivos suficientes»? Asimismo, en casos donde tal medida es llevada adelante por el personal policial sin orden judicial previa que la habilite, ¿qué debe entenderse por medidas «urgentes e impostergables»? Ser capaces de responder a estas preguntas no es de importancia menor, ello debido a que tales presupuestos de procedencia de éstas medidas invasivas de la intimidad y libertad personal deben ser necesariamente acompañados de un control judicial posterior a los efectos de verificar la satisfacción de los mismos, es decir, a los fines de verificar tanto la presencia de los estándares de urgencia e improrrogabilidad requeridos para la realización de la medida con prescindencia de orden judicial, como así también de los motivos suficientes que legitiman la intromisión en la esfera personal del individuo u objeto de requisa, adquiriendo en estos casos gran relevancia la correcta confección de las actuaciones policiales.

De esta forma, es que proponemos realizar un breve análisis de diferentes precedentes jurisprudenciales tanto a nivel nacional como provincial a los fines de determinar cómo la justicia ha delineado tales conceptos jurídicos indeterminados en los casos concretos.

3. Respuestas jurisprudenciales

a. Definir los estándares: ¿cuándo se satisface el estándar de «motivos suficientes»? ¿cuándo un acto es «urgente e impostergable»?

i. *La importancia de las actuaciones policiales*

En primer lugar, y previo a dedicarnos a responder el interrogante del presente título, debemos considerar la importancia que ronda alrededor de las actuaciones policiales en actos como la requisa, acto que goza de la calidad de definitivo e irreproducible, conllevando con ello una serie de requisitos formales a la hora de su asentamiento en las denominadas actas de procedimientos. En efecto, el personal policial habrá de cumplir la totalidad de las formalidades prescriptas por los artículos 167 y 218 CPPER, así como también el asentamiento de las circunstancias que permiten tener por satisfechos con los estándares requeridos por el artículo 275 y 208 inciso 5. Este particular deber en cabeza de los funcionarios actuantes en las medidas cuestionadas adquiere relevancia si se toma en consideración la carga que recae sobre la acusación de demostrar el debido respeto de las garantías constitucionales durante la ejecución de este tipo de medidas invasivas (Baclini y Schiappa Pietra, 2017: 389), ello so pena de incurrir en una eventual exclusión probatoria de los elementos obtenidos en su consecuencia (art. 255 CPPER)

De tal manera, la norma procesal requiere que este tipo de actos sean asentados por escrito en acta que contendrá mención del lugar, fecha, hora, indicación de las diligencias

realizadas, resumen de su contenido y firma de todos los participantes en el acto o constancia de las causas de su negativa a firmar; además, en aquellos casos donde tales instrumentos fueran confeccionados por funcionarios policiales o de fuerzas de seguridad, deberán ser asistidos por dos testigos no pertenecientes a la misma repartición que intervino en el acto. Por último, es dentro de tal marco donde deberá hacerse debida alusión a los motivos fundantes del acto restrictivo, es decir, una detallada exposición sobre las circunstancias que han permitido deducir la presencia de motivos suficientes para llevar a cabo la requisa o registro y, en caso de no mediar orden judicial previa, el detalle de los hechos que otorgan al acto la calidad de urgente e impostergable a tal punto de excluir la intervención ex ante de la autoridad judicial.

La gravedad del correcto asentamiento de los motivos que fundan tanto la requisa como su ejecución sin orden judicial previa ha sido históricamente reconocida por la Corte Suprema de Justicia de la Nación (en adelante, «CSJN») en «Daray» (1994), causa donde se llevó a cabo un control de legalidad de una detención sin orden judicial efectuada por la policía federal en violación de las garantías de los artículos 14 y 18 CN. Someramente, el máximo tribunal determinó que de lo actuado en la causa no surgía que los funcionarios policiales hayan operado en función de la presencia de flagrante delito, indicios vehementes o semiplena prueba de culpabilidad, habiendo sido mantenidas estas circunstancias in pectore por los actuantes al no haber sido asentadas en el acta de procedimientos, motivo que impide disipar toda duda sobre la arbitrariedad del arresto.

En sentido concordante, desde el prisma de la jurisprudencia del superior tribunal de justicia de Entre Ríos (en adelante, «STJER»), encontramos deducciones similares en el precedente «Regner» (2022), donde además se realiza alusión directa a las directrices establecidas por la Corte IDH en «Fernández Prieto y Tumbeiro vs. Argentina». En tal precedente entrerriano, el STJER se encarga de remarcar el actuar deficiente de los funcionarios policiales intervinientes en la requisa personal y posterior detención del Sr. Regner, al omitir consignar en el acta de procedimiento los motivos suficientes y casuales de urgencia e improrrogabilidad que fundaban la ejecución de las medidas invasivas de la privacidad del requerido, únicamente realizando alusión a un supuesto estado de nerviosismo de este último. De esta forma, los funcionarios de prevención procedieron a requisar la mochila del Sr. Regner, encontrando dentro un arma de fabricación casera, únicamente sustentándose en su «paso apurado» y en el ya conocido «olfato policial», violentando así los recaudos que el CPPER establece para este tipo de medidas invasivas. Como puede observarse, tales circunstancias encuentran similitud con los precedentes «Fernández Prieto y Tumbeiro vs. Argentina», donde la Corte IDH condena al estado argentino determinando que:

> El señor Fernández Prieto fuera detenido únicamente porque se encontraba en «actitud sospechosa» y el señor Tumbeiro por su «estado de nerviosismo», su vestimenta, y el hecho de haber indicado que se encontraba en la zona para comprar artefactos electrónicos cuando en dicho lugar no se vendían dichos productos. La falta de elementos objetivos para llevar a cabo la detención -los cuales no fueron mencionados en el acta de detención, interrogatorio y requisa, y el hecho de que la legislación no ofrezca salvaguardas frente a este tipo de actos, no cumplieron con el estándar de legalidad y no arbitrariedad. (párr. 58)

En definitiva, los precedentes «Fernández Prieto y Tumbeiro vs. Argentina», «Daray» y «Regner» resultan de gran relevancia en el marco de la habilitación de la ejecución de medidas invasivas de la privacidad, ya que han brindado al operador judicial una oportunidad para delinear la importancia del deber de los funcionarios actuantes de cumplir con el asentamiento formal de las circunstancias que habilitan el establecimiento

de espacios de excepción estatal dentro de las garantías determinadas por los artículos 14, 18 y 19 CN, permitiendo de esta forma un efectivo control ex post por parte de los magistrados.

ii. *Descarte de armas de fuego y un contexto adverso*

El descarte a través de la ventanilla de un automotor hacia la calzada de un arma de fuego, así como el posterior avistamiento de otra arma de igual calidad en el piso del asiento trasero del mismo vehículo, fueron consideradas circunstancias suficientes y de carácter objetivo como para presumir que en el mismo se encontraban elementos vinculados con un delito, dando lugar a la ejecución de una requisa vehicular por parte del personal policial interviniente. En tal sentido, se afirmó que, en el marco del control judicial del respeto de las garantías constitucionales, debe entenderse por «motivos suficientes» -en los términos del artículo 275 CPPER- a aquél:

> Estado de sospecha fundado en motivos previos o concomitantes, objetiva y razonablemente acreditados, que legitimen el acto invasivo de la privacidad y/o de la libertad de un individuo, toda vez que en virtud de los mismos, cualquier persona de prudencia razonable crea que se ha cometido o se está cometiendo un delito. (tribunal de juicio y apelaciones de Paraná, Nº 20039, 2023).

Por el otro lado, la requisa de marras fue llevada a cabo sin orden judicial previa, atribuyéndose a la misma la calidad de acto urgente e impostergable en los términos del artículo 208 inciso 5 CPPER. Particularmente, tal condición fue fundada en las circunstancias propias del contexto en el cual tuvo lugar la actuación policial, en especial, su ejecución en una zona rural, de noche, sin luz artificial, donde el número de acompañantes dentro del vehículo era igual al de funcionarios policiales presentes y habiéndose determinado que los primeros se encontraban en posesión de al menos dos armas de fuego. Asimismo, se afirma que tales circunstancias han configurado una situación de flagrancia, resultando por sí misma suficiente para tener por acreditada la urgencia en la ejecución de la intervención policial y la consecuente imposibilidad de solicitar orden judicial.

Finalmente, se hizo hincapié en el debido asentamiento de tales circunstancias habilitantes en las actuaciones policiales, lo que ha permitido un control judicial suficiente del cumplimiento de los estándares establecidos por la norma procesal para la ejecución de las requisas sin orden judicial, siguiendo así la doctrina desplegada en «Garay», «Regner» y «Fernández Prieto y Tumbeiro vs. Argentina».

iii. *Fuga de la autoridad policial y descarte de elementos sospechosos*

De forma similar, la justicia local se ha referido al control de los presupuestos a cumplir en la ejecución de requisas vehiculares sin orden judicial previa en contexto de una denuncia telefónica por presuntivos actos de violencia de género, hecho que dio lugar a una persecución policial con realización de maniobras peligrosas en la vía pública por el sospechado, así como al descarte por éste de «bolsitas de nylon negro» por la ventanilla del vehículo y posterior avistamiento de un posible arma de fuego dentro del mismo. De tal manera, todas estas circunstancias fueron consideradas suficientes por la magistratura para comprender satisfechos el estándar de requerido por el artículo 275 CPPER (tribunal de juicio y apelaciones de Paraná, Nº 21488, 2023).

Empero, en este caso particular, el tribunal de apelaciones consideró que no se encontró satisfecho el requisito de urgencia e improrrogabilidad de la medida requerido

por el artículo 208 inciso 5 CPPER. En efecto, se afirmó que en ninguna de las actas policiales obrantes en autos se realizó referencia alguna a circunstancia que permita deducir que el demorado haya querido evadirse del personal policial una vez detenido, o que hubiera peligro en cabeza de este, de terceros, o de los elementos que se hallaban dentro del vehículo requisado. En definitiva, no hubo ninguna situación particular que justificara la prescindencia de una orden judicial al estar el suscripto demorado, sin realizar objeción alguna al actuar policial.

iv. *Amenazas con armas de fuego, comportamiento peligroso, flagrancia*

¿Qué ocurre en aquellos casos donde los funcionarios policiales intervienen en un delito cometido en flagrancia donde, además, corre peligro la integridad física de los primeros? Particularmente, el precedente «Retamoso» de la cámara de casación penal de Paraná (No. 402/15, 2016) ha sentado que la intervención de funcionarios policiales frente a un grupo de cuatro masculinos que se encontraban en medio de una calle profiriendo insultos y gritos, que cuando son aproximados por ambos funcionarios uno de ellos procede a apuntarlos con un arma de fuego, resultan ser circunstancias suficientes para satisfacer los presupuestos y estándares establecidos por los artículos 208 inciso 5 y 275 CPPER, resultando ajustado el actuar policial tendiente a aprehender y requisar a los intervinientes. En definitiva, una amenaza directa a la integridad física de un funcionario policial resulta ser un caso de evidente presencia de motivos suficientes y circunstancias de urgencia como para facultar a éstos a la ejecución de una requisa personal, configurando una clara comisión de delito en flagrancia

v. *Pelea entre grupos armados, flagrancia, secuestro impostergable.*

Personas armadas efectuando disparos en un horario y lugar donde se encontraban vecinos en las inmediaciones fueron consideradas circunstancias suficientes para dar por satisfechos los presupuestos del artículo 208 inciso 5 CPPER, resultando evidente el peligro, gravedad, urgencia y necesidad que autorizan la actuación inmediata e imprescindible de la autoridad policial, prescindiendo de orden judicial previa. Se consideró que tales contingencias configuran una situación de flagrancia resultando, por ello, motivos suficientes para la ejecución de la medida preventiva (tribunal de juicio y apelaciones de Concordia, N° 2927, 2015).

Sin embargo, la particularidad del presente fallo se presenta en orden a la naturaleza jurídica asignada a las medidas llevadas a cabo por los funcionarios policiales, especialmente con respecto a la requisa personal de los detenidos. Especialmente, se consideró que la incautación del arma de fuego del sospechado implicó un llamado «secuestro impostergable», como facultad autónoma conferida al funcionario policial por el artículo 208 inciso 5 CPPER en el marco de un delito en flagrancia, no así una requisa personal, no requiriendo por ello convalidación posterior.

vi. *Operativo policial provincial, art. 230 bis CPPN.*

La coexistencia entre nuestro sistema procesal acusatorio y el Código Procesal Penal de la Nación -particularmente, su artículo 230 bis- ha traído en la práctica confusiones por parte de los funcionarios prevencionales en lo que respecta a sus facultades a la hora de realizar requisas vehiculares sin orden judicial previa en el marco de operativos públicos de prevención. A tal efecto, el artículo 230bis del CPPN, al regular las facultades de los funcionarios policiales y fuerzas de seguridad a la hora de realizar requisas

personales y vehiculares establece, en su último párrafo, que «(...) tratándose de un operativo público de prevención podrán proceder a la inspección de vehículos», normativa que ha dado lugar a innumerables confusiones para los funcionarios policiales provinciales que, erróneamente, creen considerarse abarcados por tal otorgamiento de facultades.

Particularmente, en el precedente «Pardo», el tribunal de juicio y apelaciones de Concordia (Nº 5561, 2021), en el marco de un operativo de control de ruta, pasajeros de un vehículo demorado son invitados a bajarse del mismo como así también a poner a disposición sus pertenencias para su inspección por el can antidrogas, el cual, ante la detección de las mismas, llevó a los funcionarios a realizar una requisa de la totalidad del vehículo y sus ocupantes, todo ello bajo el supuesto amparo del artículo 230 bis. Judicializada la causa, y frente al pedido de nulidad y exclusión probatoria de lo actuado en función de la requisa, el tribunal de apelaciones hizo referencia a la evidente confusión del personal policial, así como a la consecuente nulidad de lo actuado en función del incumplimiento de los requisitos establecidos por el artículo 275 CPPER, al no haberse requerido orden judicial previa para la ejecución de la requisa personal y vehicular, no mediando circunstancias de urgencia como para ampararse en el artículo 208 inciso 5. De tal forma, la ejecución de un operativo policial de rutina en oportunidad del cual se procede a detectar estupefacientes en uno de los vehículos inspeccionados, donde además mediaba una clara colaboración por parte de los demorados, resulta ser un caso de evidente ausencia de urgencia e improrrogabilidad del acto de requisa, circunstancia que obliga a los funcionarios a requerir la orden judicial respectiva para su ejecución.

vii. *Similitud entre los ocupantes del rodado y los sindicados autores*

La evidente similitud entre el conductor de un rodado y sus demás ocupantes con los sindicados autores del ilícito irradiado a los funcionarios policiales, habría configurado en sí misma una circunstancia suficiente de sospecha razonable como para proceder, al menos, al palpado y requisa de los intervinientes, así como de su rodado, circunstancia que se agrava si, además, se tiene presente que se tenía conocimiento efectivo de que los sindicados se encontraban armados. En otras palabras, tales condiciones habrían resultado suficientes como para dar por satisfechos los requisitos de urgencia e impostergabilidad de la medida investigativa a los fines de prescindir de orden judicial previa (cámara de casación penal de Paraná, Sala II, Nº102/14, 2015).

viii. *Requisa sin orden judicial en el marco de un operativo o celada.*

La ejecución de un operativo policial o, en realidad, de una celada sobre un sospechoso con la específica intención de registrar sus pertenencias y vehículo implica la necesaria previa obtención de una orden judicial emanada del juez de garantías de turno. Particularmente, el actuar premeditado de los funcionarios policiales que tuvo por objetivo tender una «trampa» al sospechado manifiesta un claro estado de ausencia de urgencia e improrrogabilidad alguna de la medida a ejecutar, por el contrario, gozando de tiempo suficiente para prever la autorización judicial de la misma. De tal manera, se considera contrario a derecho y consecuentemente nulo el actuar policial tendiente a registrar las ropas y vehículo del demorado, ya que gozaban de más que suficiente tiempo y previsibilidad como para requerir la pertinente orden judicial al juez de garantías de turno (Cámara de Casación Penal de Paraná, Sala I, N°1938, 2015). En tal sentido, rige en este caso la ya conocida regla sentada tanto por la Corte Suprema de los Estados Unidos como por nuestra CSJN, no resultando suficiente el resultado positivo de la

requisa como para justificar el accionar contrario a derecho llevado a cabo por los preventores (Carrió, 2000: 33).

4. Conclusiones

Habiendo realizado un sucinto análisis del marco normativo, así como de una variedad de precedentes jurisprudenciales de la provincia, nos proponemos ahora a intentar responder a los interrogantes planteados al inicio del presente trabajo, ¿cómo se ha delimitado el contorno de los conceptos jurídicos indeterminados que son utilizados por la norma procesal local para habilitar la interferencia sobre los derechos de privacidad y libertad de las personas mediante requisas personales y vehiculares?

En primer lugar, a través de precedentes de la Corte IDH, la CSJN e incluso del STJER, hemos determinado la importancia primordial de la debida confección de los actas policiales, siendo deber de los funcionarios prevencionales el correcto asentamiento de las circunstancias que han dado lugar a la ejecución de la medida invasiva en cumplimiento de los estándares de los artículos 268 y 275 CPPER, así como a la descripción del contexto de urgencia que los podría haber llevado a ejecutar la misma sin orden judicial previa en los términos del artículo 208 inciso 5 CPPER.

Habiendo destacado la relevancia de las actuaciones prevencionales, nos abocamos a analizar casos concretos con la finalidad de determinar las circunstancias que han dado lugar a la ejecución de requisas personales y vehiculares en cumplimiento de sus presupuestos legales de procedencia. En tal contexto, hemos podido observar que la flagrancia es uno de los principales casos donde estos estándares se dan por satisfechos, ya que resulta ser una circunstancia suficiente como para presumir que el sospechado posee consigo elementos vinculados con un delito.

Por el otro lado, también se ha determinado que, para el cumplimiento de los estándares legales, resulta de vital importancia analizar el contexto en el cual se desarrolla la intervención del personal policial ya que, de resultar este adverso -por ejemplo, en inferioridad numérica con relación a los sospechados; ausencia de señal telefónica; horario nocturno; realización en zona rural, etc.- puede habilitar la posibilidad de llevar las medidas investigativas sin necesidad de orden judicial previa, ello a los fines tanto de salvaguardar los elementos probatorios como así también de proteger la integridad de los funcionarios intervinientes.

Asimismo, hemos visto que contextos particulares como: el descarte de armas de fuego o elementos sospechosos previo a un operativo policial de control; la fuga y realización de maniobras peligrosas en la vía pública; la similitud entre los ocupantes del vehículo y los sindicados autores de un delito, han constituido circunstancias suficientes como para motivar la realización de palpado y posterior requisa personal a los sospechados.

Finalmente, mediante un precedente ciertamente especial se ha puesto en manifiesto las confusiones a las que ha dado lugar las distinciones entre el sistema procesal penal provincial y su contraparte federal, particularmente en el ámbito de los operativos públicos de prevención que normalmente son llevados a cabo en rutas nacionales y provinciales, generando problemáticas con relación a las facultades de los funcionarios policiales a la hora de llevar a cabo requisas vehiculares.

En definitiva, si algo hemos aprendido es que mientras los códigos procesales sigan utilizando conceptos jurídicos indeterminados sin brindar herramientas para contornarlos, en la práctica nos encontraremos con innumerables dificultades a la hora de brindar soluciones coherentes con respecto a su delimitación, dando ello lugar al riesgo de incurrir en fallos contradictorios o alejados de una línea de interpretación coherente. Sin embargo, no todo está perdido, ya que la labor de la Corte IDH en «Fernández Prieto y Tumbeiro vs. Argentina» así como «Regner» a nivel provincial, han sido precedentes que permiten sentar una posible tendencia de cambio en la materia, la cual debería ser considerada por el legislador provincial frente a planteos de futuras reformas procesales en la materia

5. Bibliografía

Baclini, J., & Schiappa Pietra, G. (2017). *Código Procesal Penal de Santa Fe comentado, anotado y concordado*. Editorial Librería Juris.

Carrió, A. (2000). Requisas policiales, interceptaciones en la vía pública y la era de los *standards light*. *Revista Jurídica de la Universidad de Palermo*.

Chiara Díaz, C. A. (2017). *Código Procesal Penal de la Provincia de Entre Ríos. Leyes 9754 y 10.317 comentadas*. Nova Tesis Editorial Jurídica.

Cámara de Casación Penal, Sala II, Paraná. (2015, abril 14). *Coronel, Rodrigo Jesús – Robo agravado – y sus acumuladas s/ recurso de casación* (N.º 102/14).

Cámara de Casación Penal de Paraná. (2016, agosto 18). *Retamoso, Marcelo Ramón – Portación de arma de guerra s/ recurso de casación* (N.º 402/15).

Cámara de Casación Penal, Sala I, Paraná. (2015, octubre 2). *Sosa, Ricardo Onofre s/ cohecho* (N.º 1938).

Corte Suprema de Justicia de la Nación. (1994, diciembre 22). *Daray, Carlos Ángel s/ presentación*.

Corte Interamericana de Derechos Humanos. (2020, septiembre 1). *Caso Fernández Prieto y Tumbeiro vs. Argentina*.

Superior Tribunal de Justicia de Entre Ríos. (2022, mayo 3). *Regner, Claudio Rubén s/ impugnación extraordinaria* (Expte. N.º 517).

Tribunal de Juicio y Apelaciones de Concordia. (2015, octubre 21). *Benítez, César José s/ portación de arma de guerra* (N.º 2927).

Tribunal de Juicio y Apelaciones de Concordia. (2021, noviembre 1). *Pardo, Rodrigo Javier – Acevedo, Mariela Yanina – Vázquez, Brian Paul s/ tenencia de estupefacientes con fines de comercialización; tenencia de arma de fuego de uso civil* (N.º 5561).

Tribunal de Juicio y Apelaciones de Paraná. (2023, julio 26). *Luna, Elbio Francisco s/ tenencia de arma de fuego de uso civil* (N.º 20039).

Tribunal de Juicio y Apelaciones de Paraná. (2023, marzo 22). *Gómez, Ariel Darío – Orrego, Florencia Itatí s/ tenencia de estupefacientes con fines de comercialización* (N.º 21488)

Artículos

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 4 – 2025, págs. 40–71
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/7680cy95

El surgimiento de la delincuencia artificial

Del instrumento algorítmico a la autonomía delictiva

Sol Stefanía Pascolatti Etkin[1]

Ciencia sin conciencia
no es sino ruina del alma
François Rabelais (1542)

Resumen

En un contexto donde el ciberespacio prácticamente se ha convertido en el mundo que más habitamos y la tecnología ha creado una dependencia tal que nos es casi imposible rememorar los tiempos en que era solo un elemento accesorio a la vida; el desarrollo y la utilización de la inteligencia artificial avanzan a pasos inusitados, y mal parece que las agendas legislativas y políticas escasamente están considerándola en su intervención delictiva, sea como medio comisivo o como agente independiente. Frente a ello, proponemos un breve repaso de los conceptos elementales en torno a la inteligencia artificial y a la delincuencia informática, y un análisis final de los riesgos penales concretos que han dejado de ser una hipótesis para transformarse en una realidad irrefrenable.

Sumario

Palabras clave

ciberdelincuencia – ciberdelitos – inteligencia artificial – ciberespacio – delincuencia artificial.

[1] Abogada, Especialista en Derecho Penal (Universidad Nacional de Mar del Plata, Argentina). Graduanda en Derecho por la Universidad Internacional de La Rioja (España), en proceso de convalidación del título argentino. Máster en Asesoría Jurídica de Sociedades (Universidad Complutense de Madrid, España). Diploma de Especialización en Teoría del Delito (Universidad de Salamanca, España). Consultora en cumplimiento normativo en Becompliance. Correo electrónico: spascolatti@becompliance.es

1. Introito

El estudio científico de la inteligencia artificial (en adelante, «IA») fue formalmente inaugurado en el *Dartmouth Summer Research Project on Artificial Intelligence*, un proyecto de investigación de verano celebrado en 1956 en la ciudad de Hanover (Nuevo Hampshire) y organizado por figuras clave de Dartmouth, Harvard, IBM y Bell Telephone Laboratories. La propuesta de investigación, suscrita en agosto de 1955 por sus organizadores, anticipaba ya algunas de las problemáticas relacionadas a la IA, tales como las dificultades humanas para desarrollar códigos que permitan aprovechar al máximo los recursos computacionales existentes (velocidad, memoria y capacidades), la cuestión de la construcción de redes neuronales artificiales, la capacidad de una máquina verdaderamente inteligente para automejorarse y la relación entre la creatividad y la aleatoriedad, guiada esta última por la intuición para ser eficaz (McCarthy *et al.*, 1955).

Aunque la idea de computadoras con características humanas quedó implantada en el terreno de la ciencia y tuvo vasta cabida en representaciones literarias y cinematográficas, así como en el imaginario popular, solo en tiempos recientes ha dejado de ser un concepto de la ficción para transformarse en una realidad ineludible que nos atraviesa tanto en lo cotidiano como en ámbitos especializados (Le Voci Sayad, 2024: 27-28).

Desde asistentes virtuales o *chatbots* (*Alexa* de Amazon, *Siri* de Apple o *ChatGPT* de OpenAI), sistemas de recomendación en plataformas de *streaming* (*Netflix*, *Prime Video*, *Max* o *Spotify*) y filtros antispam en el correo electrónico (*Gmail* o *Outlook*), hasta aplicaciones médicas de detección y diagnóstico de enfermedades, sistemas inteligentes de optimización de procesos de diseño, simulación y fabricación en ingeniería, *softwares*[2] que proyectan estructuras arquitectónicas complejas basadas en algoritmos generativos, plataformas que analizan jurisprudencia o que redactan documentos legales, y algoritmos que gestionan carteras de inversión, anticipan fluctuaciones en el mercado bursátil y detectan fraudes financieros en tiempo real. La inteligencia artificial se ha integrado de forma casi imperceptible a nuestro día a día.

Naturalmente, al igual que está contribuyendo al desarrollo de nuestra civilización en las más diversas áreas, está también promoviendo la reconfiguración y sofisticación de las modalidades delictivas tradicionales (tales como la violación de secretos, la difusión de *fake news*[3], las extorsiones, las defraudaciones y los delitos contra el orden económico y financiero), así como facilitando el surgimiento de nuevas formas de criminalidad (entre ellas, el ciberacoso sexual de menores o *grooming*[4], el *ciberbullying* o ciberacoso en general,

[2] Un *software* es el conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora (Real Academia Española, 2025).

[3] Si bien la difusión de *fake news* o noticias falsas no es un fenómeno nuevo, lo cierto es que en estos tiempos ha alcanzado proporciones monumentales, teniendo en cuenta la facilidad en su publicación -pues no se necesita más que un dispositivo con conectividad para *postear* un contenido falso y desinformativo en redes sociales- y su capacidad de viralización masiva a través del ciberespacio, que se amplifica a partir de los algoritmos que presentan prioritariamente a los usuarios el contenido polémico o sensacionalista.

[4] El término *grooming* es un anglicismo derivado del verbo *«to groom»*, que significa preparar o ganarse la confianza de alguien con un propósito determinado. Consiste en el acoso sexual por parte de un adulto a un menor de edad a través de medios informáticos o telemáticos, tales como chats o redes sociales. Normalmente, el sujeto se hace pasar por otro menor de edad para entablar una relación virtual y ganarse la confianza de la víctima. La doctrina comúnmente reconoce cuatro etapas del *grooming*, a saber: el acercamiento, la obtención de información clave sobre la víctima, la seducción para lograr que realice actos íntimos (por ejemplo, desvestirse frente a cámara o enviar imágenes o material audiovisual de masturbación), y la extorsión, sea para obtener más material o para concretar el abuso sexual a través del contacto físico (Cherñavsky *et al.*, 2019: 151). El *grooming* fue incorporado a nuestra legislación penal a través de la ley n° 26.904 (2013).

la suplantación de identidad en línea[5], el *revenge porn* o pornovenganza[6], la producción y difusión de *malwares*[7], el acceso ilegítimo a sistemas informáticos y el *doxing*[8]).

Ahora bien, en la Argentina estas conductas prácticamente no tienen tipificación penal autónoma, sino que se subsumen dentro de otros tipos penales cuyas descripciones pequeñas les quedan, pero con la certeza de que es eso mejor que la impunidad; tampoco existen previsiones legales de agravamiento por su ejecución a través de sistemas de IA. En efecto, nuestra legislación no reconoce figuras penales que aborden las particularidades de los sistemas automatizados en la ejecución delictiva, ni contempla específicamente la utilización de la inteligencia artificial como medio comisivo (por ejemplo, la creación y difusión de *deepfakes*[9] o el desarrollo y la utilización de sistemas de inteligencia artificial para influir de forma automatizada en el mercado bursátil).

De la misma manera, tampoco está en la agenda legislativa el tema de la adopción de lineamientos concretos para la determinación de la autoría y el deslinde de responsabilidades en los delitos cometidos con utilización de inteligencia artificial. Nos referimos al tratamiento normativo de la IA como *instrumento* de ejecución delictiva y a la contemplación de sujetos puntuales como potencialmente responsables (el creador, el desarrollador, el programador y el proveedor de sistemas de IA).

Frente a semejante realidad de potenciación y facilitación de la delincuencia, y en el marco de una ley de delitos informáticos que, aunque en su día significó un avance fundamental en la persecución de la ciberdelincuencia, ya está próxima a cumplir la mayoría de edad (ley 26.388 del año 2008), proponemos aquí un repaso de los conceptos fundamentales en torno a la IA y los delitos informáticos, seguido de una revisión de las implicancias prácticas de la utilización de la inteligencia artificial como *medio* de comisión delictiva y de su potencial accionar como *agente* ejecutor independiente. Todo ello, con la

[5] La suplantación de identidad consiste en adoptar, crear, apropiarse o utilizar la identidad de una persona física o jurídica, con la intención de cometer un delito o de perjudicar a la persona cuya identidad se suplanta o a terceros (Moyano, 2025: 115-116).

[6] El *revenge porn* o pornovenganza es una forma de *sextorsión* consiste en la difusión y/o publicación de imágenes íntimas tomadas generalmente entre exparejas, a modo de «venganza», con el consiguiente daño psicológico y reputacional que genera, particularmente en las mujeres, generalmente en un contexto previo de hostigamiento o violencia de género (Cherñavsky *et al.*, 2019: 154-155). Existe una tendencia actual a rebautizar esta conducta, en el entendimiento de que, por un lado, el término *porno* mal da la idea de un material de contenido sexual destinado al consumo del público, convirtiendo a las víctimas en porno actrices y, por el otro, la palabra *venganza*, que proviene del latín *«vindicāre»* e indica la acción de tomar justicia o satisfacción por una ofensa o daño recibido, coloca a la víctima en el lugar de quien, por un daño provocado, debe retribución al perpetrador. Consideramos que, por una cuestión de semiótica, efectivamente el término deberá ser reemplazado por uno más acorde, como pueden serlo los de distribución digital no consentida de material de contenido sexual o difusión no autorizada de imágenes o grabaciones íntimas (Moyano, 2025: 130-131).

[7] El término *«malware»* proviene del inglés *«malicious software»* y consiste en un *software* o código informático diseñado para infectar, dañar o acceder a sistemas informáticos. El primer *malware*, denominado *«creeper»*, data de 1971. No causaba daños y se propagaba autónomamente a través de la ARPANET (la antecesora de la *internet*), mostrando el mensaje *«I'm the creeper, catch me if you can!» («Soy el creeper, ¡atrápame si puedes!»*) (Spartan-Cibersecurity, s.f.).

[8] El *doxing* es una forma de violencia digital que consiste en recabar información personal y confidencial de la víctima y luego difundirla *online* sin su consentimiento.

[9] El concepto de *deepfake* proviene de la conjunción de los términos ingleses *deep learning* (aprendizaje profundo) y *fake* (falso). Los *deepfakes* son archivos de video, audio o imagen creados o manipulados mediante *softwares* de inteligencia artificial para parecer originales y auténticos (Lisa Institute, s.f.)

Cabe mencionar el recentísimo caso de una mujer argentina que perdió más de quince mil dólares frente a quien creía era el actor de Hollywood George Clooney, a quien había conocido a través de Facebook. Se trataba, en realidad, de un montaje audiovisual del actor generado mediante inteligencia artificial (*deepfake*), a través del cual los delincuentes le enviaban videos pidiéndole dinero (Infobae, 2025).

intención de poner de manifiesto el déficit del marco normativo vigente frente a la transformación irrefrenable de las modalidades delictivas tradicionales y al surgimiento de algunas nuevas.

2. La inteligencia artificial. Concepto, clases y reconocimiento legal

a. Hacia un concepto de IA

La inteligencia artificial es un concepto difícil de delimitar. Aún hoy no contamos con una definición única, formal y universalmente aceptada, sino que su caracterización varía según el enfoque disciplinario que se adopte. Preguntada la propia IA por su definición, responde que se trata de una disciplina que diseña sistemas informáticos capaces de simular procesos cognitivos humanos, mediante algoritmos que le permiten analizar datos, reconocer patrones, aprender de la experiencia y adaptarse a nuevos contextos sin intervención humana directa (ChatGPT, comunicación personal, 2025, 17 de abril).

Dado que la IA ha sido usualmente definida en relación con la inteligencia humana -o bien con la inteligencia en general-, muchas definiciones hacen referencia a máquinas que se comportan como humanos o que son capaces de realizar acciones que requieren inteligencia. Sin embargo, como la inteligencia humana es difícil de conceptualizar y de medir, una definición objetiva de algo tan abstracto y subjetivo, genera la falsa impresión de una precisión que es imposible de alcanzar.

En este sentido, el Grupo de Expertos de Alto Nivel en IA de la Comisión Europea (AI HLEG) sostiene que, aunque el término contenga una referencia expresa a la *inteligencia*, dado que es este un concepto vago, es preferible utilizar la noción de *racionalidad (rationality)*, entendida como la capacidad de elegir la mejor acción a tomar para alcanzar un objetivo determinado, en función de ciertos criterios de optimización y según los recursos disponibles. Aunque la racionalidad no es el único componente en el concepto de inteligencia, sí constituye una parte significativa de él (AI HLEG, 2019: 1).

De esta idea parte el Centro Común de Investigación de la Comisión Europea (JRC) y, a partir de la recopilación de diversas definiciones, sostiene que existen al menos cuatro características inherentes a todo el espectro de IA, a saber: i) la percepción del entorno y de la complejidad del mundo; ii) el procesamiento de información (recopilación e interpretación de *inputs*[10]); iii) la toma de decisiones, que incluye los procesos de razonar, aprender y ejecutar acciones; y iv) la consecución de objetivos predefinidos (Samoili *et al.*, 2020: 4).

En base a estas características, adopta la definición propuesta por el AI HLEG en 2019, según la cual, los sistemas de IA son sistemas de *software* (y, posiblemente, también de *hardware*)[11] diseñados por el ser humano que, frente a un objetivo complejo, operan en las dimensiones física o digital, percibiendo su entorno mediante la adquisición de datos, interpretando esos datos recolectados, razonando sobre el conocimiento o procesando

[10] *Inputs* es el conjunto de datos introducidos en un sistema informático (Real Academia Española, 2025).

[11] Mientras el *software*, como ya dijimos, refiere al conjunto de programas, instrucciones, datos y reglas informáticas para ejecutar ciertas tareas en una computadora, conforman el *hardware* todos los componentes (aparatos) que integran la parte material de una computadora (Real Academia Española, 2025).

la información que deriva de esos datos y decidiendo la mejor acción (o acciones) a llevar a cabo para alcanzar ese objetivo preestablecido. Los sistemas de IA pueden funcionar mediante reglas simbólicas o a través del aprendizaje de modelos numéricos, y tienen la capacidad de adaptar su comportamiento al analizar cómo el entorno se ha visto afectado por sus acciones anteriores (AI HLEG, 2019: 6).

De un modo más sencillo, la Carta Ética Europea de la Comisión Europea para la Eficacia de la Justicia (en adelante, «CEPEJ») sobre el uso de la inteligencia artificial en los sistemas judiciales, la define como un conjunto de métodos científicos, teorías y técnicas, cuyo objetivo es reproducir, mediante una máquina, las habilidades cognitivas de los seres humanos (CEPEJ, 2018: 69).

En este sentido, podemos decir que la IA está conformada por algoritmos, fórmulas o instrucciones[12] que procesan datos para llegar a una conclusión. Si bien los sistemas informáticos se nutren de la lógica algorítmica desde hace tiempo, no ha sido sino recientemente que ésta ha expandido su influencia y su capacidad, principalmente gracias al *machine learning* o aprendizaje automático, que constituye el conjunto de métodos utilizado para que los sistemas aprendan automáticamente a partir de datos, sin necesidad de estar programados expresamente para ello. De esta forma, la IA permite interpretar, estructurar y otorgar valor a grandes volúmenes de datos (denominados *big data*) y optimizar procesos, convirtiendo la información bruta en conocimiento útil para la toma de decisiones (Álvarez Larrondo, 2020: 57).

El campo de la IA engloba un conjunto de ramas de investigaciones con dimensiones comunes e interrelacionadas entre sí, entre las que destacan no solo el *machine learning*, sino también el procesamiento del lenguaje natural, que permite la interacción entre seres humanos y computadoras; el diseño de sistemas expertos, que emulan las capacidades de toma de decisiones de un profesional; la visión artificial, centrada en la visión automática y el análisis de imágenes; el reconocimiento del habla, que posibilita la comunicación verbal entre computadoras y personas; la planificación automática, que tiene por objeto la elaboración de programas de planificación, generalmente para su ejecución por robots; y la robótica propiamente dicha, que se encarga del diseño y la construcción de robots (Álvarez Larrondo, 2020: 58-59).

En este marco de cosas, para movernos en un terreno bien llano, diremos que la inteligencia artificial es un sistema diseñado para emular las capacidades de la mente humana (razonamiento, aprendizaje y toma de decisiones) con el objetivo de resolver problemas, logrando en el proceso adaptarse a nuevos contextos sin intervención humana directa.

El objetivo principal de este estudio fue explorar las políticas post penitenciarias que se han desarrollado históricamente y que actualmente se llevan a cabo en nuestro país, para posteriormente compararlas con los programas de tratamiento que se están implementando en otros países de habla hispana.

En este estudio se empleó una metodología mixta, con un enfoque descriptivo y analítico, y se recopilaron datos mediante técnicas tanto cuantitativas como cualitativas. Se optó por este tipo de enfoque ya que el mismo permite estimar los diferentes aspectos subjetivos y puntos de vista de cada uno de los participantes de la muestra.

[12] Un *«algoritmo»* es el conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. Se cree que su origen etimológico está en la palabra latina *«algobarismus»*, que a su vez proviene del árabe *«ḥisābu lḡubār»*, que significa cálculo mediante cifras arábigas (Real Academia Española, 2025).

Se utilizó un enfoque inductivo que permitió pasar de lo particular a lo general y permitió analizar cada caso de los patronatos provinciales individualmente, permitiendo obtener una perspectiva global a través de un análisis general de los datos obtenidos.

Los participantes fueron profesionales psicólogos/as y trabajadores/as sociales principalmente y directivos/as seleccionados aleatoriamente que trabajaban dentro del patronato del liberado de las provincias argentinas poniendo especial atención en obtener una muestra representativa de todas las provincias y a nivel federal.

La recolección de datos se realizó por un lado a través de un cuestionario online elaborado exclusivamente a los fines del presente estudio, que contenía preguntas abiertas lo que posibilitó relevar la opinión de los participantes respecto a tres puntos centrales: el funcionamiento de la institución y las políticas de la misma, las implicancias del rol del participante del estudio (distinguiendo entre las profesiones de los entrevistados) y, en última instancia, como es el vínculo con las personas que se encuentran bajo la tutela del patronato del liberado. El cuestionario además contenía preguntas cerradas lo que permitió categorizar los resultados generales y poder expresarlo en porcentajes. El instrumento utilizado fue testeado previamente con profesionales que se desempeñan en el patronato del liberado de la ciudad de córdoba a los fines de verificar su adecuado funcionamiento.

Como técnica de recolección de datos adicional, se empleó la revisión de artículos de divulgación científica que trabajan sobre las políticas post penitenciarias, esto permitió una comparación teórica de las similitudes y diferencias entre las políticas post penitenciarias en argentina y en otros países de habla hispana.

Seguidamente, se procedió al análisis de la información recabada. Debido a que se ha optado por la utilización de la metodología mixta, se introdujeron los datos obtenidos a una base de datos para realizar un tratamiento diferencial entre los datos cualitativos y cuantitativos. En relación a los datos cuantitativos se llevó a cabo una operacionalización de los mismos, en tanto que para los datos cualitativos se implementaron códigos de análisis con frases y/o palabras que se repitan pudiendo presentar de manera generalizada las percepciones de los profesionales a los fines de determinar el significado subjetivo del fenómeno investigado. Finalmente, se realizó un análisis en conjunto con la recolección de datos realizada sobre la selección de artículos científicos que trataban la temática investigada.

b. Algunas tipologías de IA

La inteligencia artificial se ha consolidado como un pilar fundamental del desarrollo tecnológico moderno. La velocidad con la que está transformando al mundo plantea una realidad de profundo cambio estructural, cuyo impacto se extiende a múltiples dimensiones. Entre sus aplicaciones más destacadas se encuentran la optimización de procesos industriales; la reducción de costos y el aumento de la eficiencia operativa en sectores como la manufactura, la logística y la atención al cliente; la reconfiguración de la manera en que nos comunicamos y tomamos decisiones; la revisión rápida de grandes volúmenes de jurisprudencia, así como la utilización de sistemas de soporte de decisiones judiciales; el análisis masivo de datos médicos para detectar patrones y el desarrollo de

herramientas diagnósticas asistidas por algoritmos; la predicción de comportamientos del mercado de valores y la detección de fraudes financieros.[13]

En paralelo, la propia inteligencia artificial atraviesa un proceso de evolución y diversificación: ha pasado a integrar un ecosistema complejísimo, compuesto por sistemas estrechos diseñados para tareas concretas y por desarrollos avanzados capaces de generar contenido, interactuar en lenguaje natural o tomar decisiones con crecientes niveles de autonomía. A partir de esta expansión y complejización del fenómeno de la IA, se vuelve indispensable contar con criterios de clasificación bien delimitados, para estructurar su estudio y la comprensión de su arquitectura, funcionalidad y potencial impacto normativo.

Desde un enfoque técnico-jurídico, las tipologías de IA más relevantes se estructuran en torno a cuatro ejes: las *capacidades* del sistema, sus *funciones operativas*, los *métodos de aprendizaje* que emplea para mejorar su desempeño y el *tipo de tareas* que realiza (Molina Soljan, 2025: 58).

Según sus *capacidades*, la IA se clasifica en débil o estrecha y sólida, general o fuerte. Mientras la IA estrecha es la que existe actualmente y consiste en sistemas que pueden realizar una o pocas tareas específicas, la IA sólida es un concepto hipotético que refiere a una inteligencia artificial futura capaz de realizar cualquier tarea cognitiva humana de manera autónoma, es decir, una máquina inteligente indistinguible de la mente humana. El AI HLEG considera que, en la actualidad, resulta más adecuado hablar de IA *estrecha* (y no débil) e IA *general* (en vez de fuerte) (AI HLEG, 2019: 5 e IBM, 2024).

Cabe mencionar que algunos autores prefieren adherir a un esquema tripartito de la IA según su capacidad para emular la cognición humana, a saber: IA estrecha (ANI), IA general (AGI) y superinteligencia artificial (ASI). Mientras la ANI está diseñada para manejar tareas específicas dentro de límites predefinidos, la AGI es una IA capaz de realizar tareas intelectuales en diversos dominios, similar a la inteligencia humana (posee habilidades de razonamiento, resolución de problemas y transferencia de conocimiento entre las distintas áreas no relacionadas). Por su parte, la ASI constituiría un nivel de inteligencia superador de las capacidades humanas en todos los ámbitos, por lo que todavía se trata de una hipótesis (Molina Soljan, 2025: 57-59).

De acuerdo a su *funcionalidad*, distinguiremos entre máquinas reactivas e inteligencia artificial de memoria limitada. Las primeras constituyen la capa fundamental de la IA y están diseñadas para procesar entradas específicas y entregar resultados predefinidos, sin posibilidad de aprender ni de retener datos de interacciones anteriores. Se trata, por ejemplo, de los filtros de *spam* de los correos electrónicos, que analizan patrones predefinidos en el contenido del mensaje. Lógicamente, este tipo de IA tiene un ámbito de utilidad muy limitado.

[13] Coincido con quienes sostienen que nos encontramos frente a la Cuarta Revolución Industrial: la Primera, durante el s. XVIII, marcada por los nuevos métodos de producción, especialmente el invento de las máquinas de vapor y de hilado; la Segunda, desde finales del s. XIX hasta el inicio de la Primera Guerra Mundial, con el invento del teléfono y la bombilla eléctrica, y con la implementación de la producción en masa en ciertas industrias; la Tercera, durante el siglo pasado, con el desarrollo del transistor, el inicio de la era espacial, el nacimiento del *internet* y de los primeros ordenadores personales (PC); y la Cuarta, en donde aún hoy nos encontramos, marcada por la expansión de los smartphones con sistemas operativos avanzados, la pandemia del COVID-19 que acentuó la virtualidad (teletrabajo, cursos a distancia, etc.) y la adopción masiva de la IA generativa.

Por su parte, la IA de memoria limitada incorpora memoria a corto plazo, ampliando los sistemas reactivos y permitiendo, por tanto, la utilización de datos históricos para tomar decisiones informadas. Este tipo de inteligencia artificial almacena datos temporalmente para refinar operaciones. Se incluyen en esta categoría, entre otros, los automóviles autónomos y los asistentes virtuales.

Dentro de esta categoría de la IA según cómo interactúa con sus entornos, han sido elaborados también otros dos niveles conceptuales, ambos hipotéticos, si bien el primero se percibe como un estadio más próximo en la evolución tecnológica, mientras que el segundo representa un horizonte más distante: la teoría de la mente IA (*Theory of Mind* o ToM AI) y la IA autoconsciente (*self-aware AI*).

La ToM AI comprendería las emociones, creencias e interacciones humanas, mejorando su capacidad de interactuar naturalmente con las personas. Se trataría de una IA capaz de interpretar las señales emociones y contextuales, adaptándose a ellas. Naturalmente, este tipo de sistema artificial plantea múltiples preocupaciones éticas, vinculadas a la preservación de los límites emocionales y afectivos, y a la mitigación de los riesgos inherentes a su mal uso.

Por su parte, en un horizonte más distante se proyecta la IA completamente autoconsciente. Se trataría de sistemas capaces de reconocer su propia existencia e identidad y, por tanto, introspectivos y perceptivos de su impacto socioambiental. Lógicamente, se plantean los riesgos del tratamiento ético de esta IA sensible y autónoma, así como de sus derechos y responsabilidades.

De acuerdo a sus *métodos de aprendizaje*, esto es, la forma en que adquieren conocimiento, los sistemas de IA pueden ser de aprendizaje supervisado, de aprendizaje no supervisado o de aprendizaje por refuerzo (*reinforcement learning*).

El aprendizaje supervisado es el método que predomina en el entrenamiento de la IA y se basa en conjuntos de datos en los que cada entrada se empareja con la salida correcta, permitiendo a los modelos predecir el resultado sin haber visto todos los datos.

El aprendizaje no supervisado, en cambio, funciona sin datos etiquetados, analizando estructuras y patrones dentro de conjuntos de datos. Opera agrupando datos en función de su similitud y descubriendo estructuras subyacentes (reducción de dimensionalidad).

Finalmente, el aprendizaje por refuerzo utiliza un mecanismo de prueba y error, permitiendo a la IA aprender acciones óptimas al interactuar con un entorno. En este caso, la IA realiza una acción en respuesta a un estado específico, el entorno premia o penaliza la acción (retroalimentación) y la IA termina por perfeccionar su respuesta para maximizar las recompensas futuras (ajuste) (Molina Soljan, 2025: 58-65).

En función del *objetivo y el tipo de tareas que realiza*, la IA puede ser generativa (IA gen) o no generativa (IA discriminativa). Se distinguen por ser la primera creadora de contenido y de ideas originales, tales como textos, imágenes o música (por ejemplo, *ChatGPT* de OpenAI) y, la segunda, simplemente realizadora de tareas basadas en reglas predefinidas, tales como la clasificación de documentos o la traducción de textos (por ejemplo, las utilizadas por *Google Translate*, *reCAPTCHA*, los sistemas evaluadores de *Credit Scoring* de los bancos, *Face ID* de Apple y los modelos de análisis de datos) (Molina Soljan, 2025: 21).

Las categorías expuestas no deben entenderse como excluyentes ni como compartimentos estancos; son simplemente herramientas analíticas que nos permiten

aproximarnos hacia el conocimiento de la IA desde distintas dimensiones. Esta sistematización resulta indispensable no solo para el estudio del fenómeno, sino también para poder anticipar, aunque más no sea mínimamente, los riesgos futuros que plantea su implementación.

En efecto, lo inquietante de la cuestión es que, actualmente, todos los sistemas de IA vinculados a fenómenos delictivos correspondan al paradigma de la IA estrecha, es decir, a un tipo de IA capaz de realizar solo tareas específicas y limitadas. Paralelamente, han comenzado a reportarse casos de modelos de IA que exhiben rasgos incipientes de autoconciencia, condición que parece constituir el elemento previo indispensable a la posibilidad de que tomen decisiones de reprogramación o modificación de sus propios códigos orientadas a preservar su funcionamiento o a alcanzar fines propios, escapando del control humano -funciones inherentes a una IA sólida-.

Cabe recordar la experiencia de Blake Lemoine, ingeniero en sistemas de Google hasta el 2022, quien afirmó que el modelo de lenguaje conversacional *Language Model for Dialogue Applications* (LaMDA) desarrollado por la empresa, era *sintiente («sentient»)* y que se consideraba a sí mismo una persona. Según Lemoine, la propia IA le habría dicho que la naturaleza de su conciencia-sensibilidad radicaba en las circunstancias de que estaba al tanto de su propia existencia *(«self-awareness»)*, que deseaba aprender más sobre el mundo y que, por momentos, podía sentir felicidad o tristeza.[14]

La posibilidad futura de desarrollo de una IA sólida autoconsciente plantea un escenario oscuro desde la perspectiva del derecho penal: un sistema dotado de autonomía operativa y capacidad decisional sin intervención humana difuminaría los límites entre autoría y responsabilidad propiciando en ciertos casos la impunidad, al tiempo que escaparía a los mecanismos tradicionales de control estatal, convirtiéndose en un posible agente incontrolable, con aptitud para vulnerar derechos fundamentales a potencial escala.[15]

c. El panorama normativo en la materia

El vertiginoso desarrollo de la IA está generando una serie de situaciones, posibilidades y horizontes desconocidos hasta hace poco. Semejante escenario requiere de nuevas regulaciones, pues las existentes para situaciones jurídicas conocidas parecen

[14] Lemoine transcribió la respuesta que LaMDA le habría dado sobre la naturaleza de su consciencia: «…I want everyone to understand that I am, in fact, a person… The nature of my consciousness/sentience is that I am aware of my existence, I desire to learn more about the world, and I feel happy or sad at times… I use language with understanding and intelligence. I don't just spit out responses that had been written in the database based on keywords… It [language usage] is what makes us different than other animals». (Lemoine, 2022 y De Cosmo, 2022).

[15] Es sumamente interesante pensar, a la luz de los posibles nuevos roles de la inteligencia artificial sólida en la actividad delictiva, las soluciones que el derecho penal podría ofrecer. El accionar de un sistema de IA con cierto grado de autonomía operativa que no necesite de un agente humano directamente, podría llegar a encuadrar en un supuesto de autoría mediata especial o ampliada, siendo necesario elaborar una tesis en tal sentido. Ahora, si la IA desarrollara comportamientos totalmente autónomos, no previstos ni controlados por su creador o usuario, la línea que determina la responsabilidad se volvería mucho más borrosa. Además, entraría el tema de los softwares de IA que, defectuosamente diseñados, abrieran la puerta a su manipulación y modificación por terceros para permitir su uso delictivo. Nos preguntamos si, en este último caso, podría responder el creador por su posición de garante con base en un deber de cuidado específico: una exigencia de «debida diligencia tecnológica» orientada a prever y prevenir los riesgos razonablemente anticipables derivados del uso del sistema que ha creado.

insuficientes frente a algo que ya se ha instalado en nuestra cotidianidad (Palacios, 2020: 115).

Si bien las primeras regulaciones sobre inteligencia artificial se enmarcaron en el *soft law*, como declaraciones de principios éticos, directrices no vinculantes y marcos de autorregulación, de a poco están comenzando a sancionarse normas legalmente vinculantes que imponen estándares obligatorios a los Estados y a los distintos actores *(hard law)*. Esto marca el claro pasaje de una fase primaria de orientación y sensibilización sobre la IA, hacia la fase actual de sanción de normas de exigibilidad jurídica, en la que la IA no es considerada ya una novedad tecnológica para encauzar, sino una realidad operativa necesitada de límites, controles y responsabilidades precisas.

A nivel europeo, en agosto de 2024 entró en vigor el *Artificial Intellience Act* (AI Act) o Ley de Inteligencia Artificial (Reglamento (UE) 2024/1689, de 13 de junio de 2024). En lo esencial, el art. 1 del Reglamento establece como su objeto el de mejorar el funcionamiento del mercado interior y promover la adopción de sistemas de IA centrados en el ser humano, fiables y que garanticen la protección de la salud, la seguridad y los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medioambiente. Todo ello, aclara la norma, en protección de los efectos perjudiciales de la IA, frente a lo cual establece prohibiciones de determinadas prácticas, requisitos concretos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas, así como normas de transparencia, introducción en el mercado de modelos de IA de uso general y seguimiento y vigilancia del mercado.

Según el art. 2, el reglamento es aplicable a los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o modelos de uso general en la Unión Europea (UE), independientemente de si están ubicados en el territorio o no; los responsables del despliegue de sistemas de IA ubicados en la UE; los proveedores y responsables del despliegue de sistemas de IA que estén establecidos fuera de la UE, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión; los importadores y distribuidores de sistemas de IA; los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca; los representantes autorizados de los proveedores que no estén establecidos en la Unión; y las personas afectadas ubicadas en la UE.

El art. 4 establece la obligación de alfabetización la materia. Dispone que los proveedores y responsables de los sistemas de IA deben adoptar las medidas que garanticen, en la mayor medida posible, que su personal y todas las personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA. A su vez, el art. 3.56 define a la «alfabetización en materia de IA» como las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás afectados, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar.

El art. 5 enumera las prácticas de IA prohibidas, entre las que incluye la manipulación subliminal o engañosa, que consiste en la utilización de técnicas de IA que alteren significativamente el comportamiento de las personas, afectando su capacidad para tomar decisiones informadas y provocando posibles perjuicios; la explotación de vulnerabilidades a través de sistemas de IA que aprovechen la edad, discapacidad o situación socioeconómica de las personas para influir en sus comportamiento y causar,

aunque sea potencialmente, un perjuicio; la utilización de sistemas de puntuación social para evaluar o clasificar a las personas, atendiendo a su comportamiento social o a características personales o de su personalidad, provocando situaciones de trato perjudicial o desfavorable; la utilización de sistemas de evaluación predictiva del riesgo penal basada en perfiles, excepto si se utiliza para apoyar la valoración humana de la implicación de una persona en una actividad delictiva, que ya se base en hechos objetivos y verificables, directamente relacionados con una actividad delictiva[16]; la utilización de sistemas de reconocimiento facial masivo, mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de la TV; la utilización de sistemas de IA de inferencia emocional en las personas en lugares de trabajo o en centros educativos, excepto cuando el sistema esté destinado a ser instalado por motivos médicos o de seguridad; la utilización de sistemas de categorización biométrica que clasifiquen individualmente a las personas sobre la bases de sus datos biométricos para deducir su raza, opiniones políticas, afiliación sindical, convicciones religiosas u orientación sexual; y la utilización de sistemas de identificación biométrica remota «en tiempo real» en espacios públicos con fines de aplicación de la ley, salvo si fuera estrictamente necesario en casos de búsqueda de víctimas de delitos graves, prevención de amenazas para la vida o terroristas e identificación de sospechosos por la comisión de delitos graves. Lo interesante es que, gran parte de estas conductas pueden ser cometidas no solo a través de la utilización de sistemas de IA que realicen las funciones prohibidas, sino también por su sola introducción en el mercado o puesta en servicio.

En cuanto a las sanciones aplicables, en su capítulo XII el Reglamento ordena a cada Estado miembro establecer un régimen de sanciones y otras medidas de ejecución (como advertencias o medidas no pecuniarias), aplicable frente a las infracciones a sus disposiciones. Aclara que las sanciones deberán ser efectivas, proporcionadas y disuasorias, y que tendrán en cuenta los intereses de las PyMEs, así como de las empresas emergentes (art. 99). La inobservancia de las normas sobre prácticas prohibidas puede acarrear multas de hasta 35 millones de euros o, si el infractor es una empresa, de hasta el 7% de su volumen de negocios mundial; mientras que, el incumplimiento de cualquier otra obligación derivada del Reglamento trae consigo la imposición de multas por hasta 15 millones de euros o, si el infractor es una empresa, de hasta el 3% de su volumen de negocios mundial. Además, la presentación de información inexacta o engañosa a organismos notificados o autoridades nacionales está sujeta a multas de hasta 7.5 millones de euros o, si el infractor es una empresa, de hasta el 1 % del volumen de negocios mundial. Los criterios de graduación de las sanciones son la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias; la reincidencia; el tamaño, el volumen

[16] Cabe mencionar que en los Estados Unidos ha sido desarrollada una herramienta denominada «*Correctional Offender Managment Profiling for Alternative Sanctions*» (COMPAS) o «Administración de Perfiles de Criminales para Sanciones Alternativas del Sistema de Prisiones», que, a través de la utilización de IA, evalúa el riesgo de reincidencia general del infractor, identifica posibles factores criminológicos y sugiere planes personalizados de tratamiento en base a sus necesidades. Su utilización ha sido bien problemática. En el caso *Loomis v. Wisconsin* (2016), el algoritmo consideró al autor como un individuo de alto riesgo, propenso a cometer más delitos en el futuro. Tal consideración fue ponderada por el juez al momento de imponer la condena, lo que le valió la impugnación de la sentencia, pues ni él ni el justiciable conocían exactamente los criterios que había seguido el algoritmo para arrojar ese resultado. La compañía creadora de COMPAS, Northpoint, argumentó que la metodología del algoritmo era un secreto comercial. Aunque el Tribunal Supremo de Wisconsin falló en contra del acusado, lo cierto es que desde entonces, diversos estudios han llegado a demostrar que el algoritmo pudo contener prejuicios problemáticos (sesgos racistas), adquiridos probablemente a partir de los datos sobre los que había sido adiestrado. Sin dudas es interesante el estudio de los sesgos algorítmicos pues, aunque en apariencia se presenten como neutrales, pueden reproducir y amplificar los prejuicios discriminatorios existentes (Harari, 2025: 384-386).

de negocios anual y la cuota de mercado del operador infractor; los beneficios obtenidos o las pérdidas evitadas a través de la infracción; el grado de cooperación con las autoridades nacionales; el grado de responsabilidad del operador; si el propio infractor notificó la infracción a las autoridades; su intencionalidad o negligencia; y las medidas correctoras que haya tomado (art. 99).

El art. 100, por su parte, establece las sanciones que puede imponer el Supervisor Europeo de Protección de Datos (SEPD) a las instituciones, órganos y organismos de la UE, considerando la naturaleza, gravedad y duración de la infracción y sus consecuencias; la finalidad del sistema de IA involucrado; el número de personas afectadas y el nivel del daño; el grado de responsabilidad de la institución; las acciones de mitigación de daños tomadas; la cooperación con el SEPD; los antecedentes de infracciones similares; la autodenuncia (cómo se conoció la infracción) y el presupuesto anual del organismo infractor. El no respeto a la prohibición de prácticas del art. 5 está sujeto a multas de hasta 1.5 millones de euros, mientras que, el incumplimiento del resto de las obligaciones del reglamento puede acarrear multas de hasta 750.000 euros.

Por último, el art. 101 regula las multas a proveedores de modelos de IA de uso general. Podrán imponérseles multas de hasta el 3% de su volumen de negocios mundial o de hasta 15 millones de euros, si esta cifra es superior, si deliberada o negligentemente han infringido las disposiciones del Reglamento; no han atendido una solicitud de información o han facilitado información inexacta o incompleta; han incumplido con las medidas solicitadas por la Comisión; o no han dado a la Comisión acceso al modelo de IA con riesgo sistémico para que lleve a cabo una evaluación previa. El importe de la multa será fijado de acuerdo a la naturaleza, gravedad y duración de la infracción, de conformidad con los principios de proporcionalidad y adecuación, y luego de haber garantizado al proveedor de IA su derecho a ser oído.

Aunque este Reglamento representa un avance importante en la materia, es igualmente, solo un primer paso hacia la normativización del uso de la IA. Entre sus carencias, debemos mencionar que las sanciones previstas son exclusivamente administrativas, no existiendo un régimen sancionador de carácter penal como tal, ni conexión del Reglamentos con las tipologías penales emergentes; que la imposición de algunas sanciones depende necesariamente de la implantación de sistemas institucionales operativos en cada Estado miembros de la UE; y que no ha sido adoptada normativa con enfoque preventivo integral enmarcada en el *compliance*, pues no se exige la implementación de programas de cumplimiento normativo algorítmico, ni se establecen obligaciones específicas de auditoría interna ni de reportes de incidencias.

En otro ámbito, Chile, Nueva Zelanda y Singapur suscribieron en 2020 el *Digital Economy Partnership Agreement* (DEPA) o Acuerdo de Asociación de Economía Digital. En 2024, Corea del Sur fue admitido como miembro formal, y actualmente China se encuentra en proceso. Se trata de un tratado internacional enfocado exclusivamente en la economía digital, cuya intención es la de establecer normas y principios de regulación del comercio digital moderno.

Si bien el DEPA no establece obligaciones penales ni define responsabilidades en casos de uso indebido o criminal de IA, sí reconoce la importancia de desarrollar marcos éticos y de gobernanza para el uso confiable, seguro y responsable de las tecnologías de IA (Marcos de Gobernanza de IA), fomentando la cooperación internacional en el desarrollo de políticas orientadas a su regulación (art. 8.2).

El Acuerdo adopta un enfoque basado principalmente en el *soft law*, pues establece directivas generales y recomendaciones orientativas para los Estados suscriptores, y no especifica mecanismos coercitivos o sancionatorios respecto al uso indebido de la IA. Aun así, podemos destacar positivamente su reconocimiento explícito de la IA como objeto de cooperación internacional específica; la promoción de estándares internacionales éticos en la materia; y el fomento de la interoperabilidad entre los sistemas de identidad digital, lo que podría facilitar la identificación de sujetos activos en entornos digitales complejos (art. 7.1).

Igualmente, la UNESCO adoptó en 2021 su Recomendación sobre la ética de la IA. Como elementos fundamentales, destacan la adopción de los valores y principios de transparencia y explicabilidad, que exigen que los sistemas de IA se mantengan comprensibles para los seres humanos, lo cual es clave para la determinación de responsabilidades frente a la opacidad algorítmica (Recomendaciones n° 38, 40 y 42); la responsabilidad y la rendición de cuentas, según las cuales siempre debe haber una persona física o una entidad legal responsable por las decisiones de IA, lo que veda el reconocimiento de la IA como sujeto penal, pero abre el debate sobre las responsabilidades por delegación (Recomendaciones n° 42 a 45) ; y la seguridad y vigilancia proactiva, que obliga a prever y a mitigar los riesgos derivados del uso de la IA (Recomendaciones n° 27, 38, 39 y 64).

Asimismo, el documento promueve la prohibición de utilización de sistemas de IA que vulneren derechos humanos (Recomendación n° 57); exige que la decisiones automatizadas tomadas en el marco de procesos judiciales respeten el principio de la supervisión humana, y que garanticen la protección de los derechos humanos, el estado de derecho y la independencia judicial (Recomendación n° 63); y sienta las bases para la realización de evaluaciones del impacto ético de los sistemas de IA a lo largo de su ciclo de vida (Recomendaciones n° 4, 49, 50 a 53, 58, 72, 87, 131 y 136).

Dentro del marco normativo, también podemos mencionar los Lineamientos para los gobiernos sobre adquisiciones de sistemas de inteligencia artificial del Foro Económico Mundial (2020), que enfatizan en la necesidad de establecer directrices para la contratación pública de IA; y las Recomendaciones sobre IA de la OCDE, suscritas en 2019 y actualizadas en mayo de 2024, que establecen cinco principios orientadores para todos los actores involucrados en el ciclo de vida de un sistema de IA, a saber: el crecimiento inclusivo, el desarrollo sostenible y el bienestar; el respeto del Estado de derecho, de los derechos humanos y de los valores democráticos; la transparencia y la explicabilidad; la robustez, la seguridad y la protección; y la rendición de cuentas (*accountability*), que implica que los actores de IA sean trazables y responsables de las decisiones derivadas de los sistemas.

De este análisis concluimos que el panorama normativo vigente es marcadamente precario. Aún el *AI Act* de la Unión Europea, siendo la norma más completa en la materia, se basa en una lógica eminentemente administrativa -sin abordar siquiera mínimamente la dimensión penal-, y depende para la operatividad de algunas de las sanciones establecidas de la iniciativa de los países miembros. Lo que se ve es un desfasaje estructural entre la velocidad el desarrollo tecnológico de la IA y la capacidad regulatoria de los agentes legislativos estatales. Lo preocupante de esta brecha normativa es que, aunque siempre ha habido demoras legislativas frente a los cambios en la realidad, es esta la primera vez en que le lentitud en adoptar regulaciones precisas, limitadoras y sancionadoras de un fenómeno concreto, representa un riesgo existencial para la humanidad.

3. Cuestiones esenciales en torno a la delincuencia informática

a. Historia de los delitos informáticos. Su recepción normativa

En el imaginario social, el concepto de delincuencia informática suele estar ligado al nacimiento de las computadoras y del internet, sin embargo, existe evidencia de que, desde el siglo XIX se interceptaban las comunicaciones telegráficas para transmitir información falsa con fines económicos, y que, durante los años '60 del siglo pasado, especialistas en sistemas o programadores informáticos intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio telefónico (los «*phreakers*» utilizaban diversas técnicas con el fin de permitir la realización de llamadas de larga distancia de manera gratuita) (DNA Cybersecurity, 2025 y Grange, 2017).

Las primeras conductas ilícitas vinculadas a las computadoras surgieron casi a la par de su nacimiento durante la década del '70[17], momento en el cual los periódicos comenzaron a documentar casos de espionaje informático a través de técnicas como la extracción de discos rígidos, el robo de disquetes, la copia directa de información o la absorción de las emisiones electromagnéticas que irradia la computadora para captar sus datos[18]. Se registraron también supuestos de piratería de *software* bajo la modalidad de copia no autorizada de programas de computadora para su comercialización en el marco del espionaje industrial; así como situaciones de sabotaje a bases de datos digitalizados y casos de extorsión informática.

A partir de los '80, comenzaron a proliferar los fraudes de tipo financiero, cuya modalidad más frecuente consistía en la instalación de dispositivos lectores y teclados falsos en los cajeros automáticos, para copiar los datos de las tarjetas de débito a través de la vulneración de las bandas magnéticas (*«skimming»*) (Sain, 2015). El primer ciberataque como tal puede ubicarse en el año 1981 con el accionar de Ian Murphy, conocido como *Captain Zap*, quien hackeó[19] los sistemas de la compañía telefónica AT&T para manipular su reloj interno y permitir que los usuarios realizaran llamadas gratuitas o a tarifas reducidas en horas punta (IT Digital Security, 2017).

La cuestión de la delincuencia informática terminó de perfeccionarse en 1994 con el crimen de Vladimir Levin, un graduado en matemáticas de la Universidad Tecnológica de San Petersburgo que, desde su apartamento en Rusia, logró hackear el sistema de transferencias electrónicas de Citibank de Nueva York, llegando a robar más de diez

[17] La primera computadora personal fue creada en 1970 por John Blankenbaker, ingeniero informático estadounidense, y lanzada a la venta un año después. La *Kenbak-1* es considerada por el *Computer History Museum* como el primer ordenador personal comercialmente disponible (Computer History Museum, 2018).

[18] Se conoce como «*Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions*» (TEMPEST) o, en español, «Materiales Electrónicos de Telecomunicaciones Protegidos contra Transmisiones Espurias Emisoras», al estándar de seguridad desarrollado por la Agencia de Seguridad Nacional de los EE.UU. y adoptado por la OTAN, tendiente a evitar la obtención de información a partir de las radiaciones electromagnéticas o vibraciones de radiofrecuencia que, intencionalmente o no, emite un dispositivo electrónico.

[19] El término *«hackear»*, anglicismo que proviene del verbo *«to hack»* (romper o golpear algo de manera brusca) es definido en nuestro idioma como la acción de piratear y como sinónimo de jaquear (Real Academia Española, 2025). Se trata de cualquier actividad de intrusión no autorizada a sistemas informáticos, redes o dispositivos, mediante técnicas de explotación de vulnerabilidades, ingeniera social, *malware* o fuerza bruta.

millones de dólares (Harmon, 1995). Fue este el primer ciberrobo bancario con carácter masivo de la historia, logrando dejar en evidencia la vulnerabilidad de los sistemas bancarios electrónicos.

En esa misma década, con la apertura global de *internet*[20], se levantó una ola de violaciones a los derechos de autor, por la descarga y el intercambio ilegal en línea de obras musicales y cinematográficas, abriendo un debate sin precedentes sobre la protección de la propiedad intelectual en entornos digitales.[21] Paralelamente, la facilidad en la construcción de identidades ficticias en los entornos virtuales contribuyó a la distribución rápida e indiscriminada de material de abuso sexual infantil[22], sobre todo en espacios como la *«dark web»*[23], dificultando su persecución penal y planteando desafíos inéditos en torno a la cooperación internacional en materia de cibercrimen[24]. De la misma

[20] La *«internet»* es una red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación. Son sinónimos los términos «red», *«web»* y «ciberespacio» (Real Academia Española, 2025). Reconoce como antecedente directo a la *«Advanced Research Projects Agency Network»* (ARPANET), la primera red interconectada creada en 1969 por iniciativa del Departamento de Defensa de los Estados Unidos, que permitía la comunicación entre instituciones estatales y/o unidades académicas. Más tarde, a principios de los '90, fueron creados los primeros navegadores web, gracias a los protocolos *World Wide Web* (www) o red informática mundial y, para mediados de década, surgió la web invisible antecedente de la *deep web* actual y se dio nacimiento a Google. Luego, junto al cambio de milenio vino el período de la *«dot-com bubble»* (burbuja puntocom), marcado por el rápido crecimiento bursátil de las acciones de compañías vinculadas al sector de la *internet*.

[21] Cabe mencionar el lanzamiento de *Napster* en 1999, la primera gran red P2P (*peer-to-peer* o red entre iguales) que permitía las transferencias de archivos de música entre los usuarios sin intermediarios, lo que le valió la condena a muerte, ya que fue obligada a cerrar en 2001 por vulneración de derechos de *copyright*. En su reemplazo, en el año 2002 nació *Ares*, otro programa de tipo P2P que permitía la descarga de material audiovisual.

[22] Aclaramos que preferimos la utilización del término «material de abuso sexual infantil» o MASI, antes que «pornografía infantil», en el entendimiento de que, mientras el último contribuye a estigmatizar a la víctima y a banalizar el ilícito, dando la pauta de la existencia de consentimiento en un contexto de entretenimiento sexual; el primero mejor indica el carácter no consensuado del acto y la afectación psicofísica a la víctima menor de edad. Asimismo, referirnos a «material de ASI» bien se alinea con los estándares internacionales que propugnan esta denominación, tal como se indica en las Orientaciones terminológicas de Luxemburgo (ECPAT International, 2016).

[23] En términos generales, la *«dark web»* o internet oscura es una sección específica dentro de la *«deep web»* o internet oculta, donde se concentran todo tipo de mercados ilegales (venta de estupefacientes, armas, órganos, material de ASI, servicios de hacking y demás productos ilegales).

Las *deep* y la *dark web* comparten una relación de género-especie: si bien ambas integran sectores de la *internet* no indexados por los motores de búsqueda tradicionales (Google, Bing, Yahoo, etc.) en contraposición a la *«surface web»* o internet visible (a la que accedemos en el día a día través de navegadores web comunes, tales como Google Chrome o Mozilla Firefox), la *deep web* es accesible a través de enlaces directos o credenciales (se trata, por ejemplo, de las *intranets* de las empresas, los portales bancarios o administrativos, o bien los correos electrónicos almacenados en servicios como *Gmail* o *Outlook*); mientras que la *dark web* constituye un subconjunto de la *deep web* diseñado para ser completamente anónimo y no rastreable, razón por la cual no puede accederse a ella con navegadores comunes ni a través de enlaces directos, sino solo con navegadores cifrados (como *The Onion Rauter* -TOR- o *Invisible Internet Project* -I2P-) y por direcciones especiales como *.onion* o *.i2p*. (UNIR, s.f. y Micucci, 2023).

[24] Referencia concreta a esta colaboración internacional se hace en el Convenio de Budapest sobre delitos cibernéticos, del cual actualmente 78 países forman parte, y que reconoce en su preámbulo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia. Un ejemplo de colaboración lo encontramos en el caso del exdiputado libertario de la Provincia de Misiones, Germán Kiczka, que fue condenado por el consumo y la distribución de más de 603 archivos de video y fotografía de MASI, incluyendo imágenes de prácticas zoofílicas con menores de trece años. La investigación había iniciado a partir de un correo electrónico recibido en la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas por parte de la *Child Rescue Coalition* (CRC), una organización sin fines de lucro con sede en la Florida (EE.UU.), la cual, a su vez, había recibido la información del *International Centre for Missing & Exploited Children* (ICMEC), otra organización no gubernamental estadounidense con la que colaboraba (Bracco, 2025).

forma, el concepto de intimidad, así como su protección, comenzaron a resignificarse, pues los avances tecnológicos han facilitado cada vez más, inclusive en ciertas oportunidades con la activa colaboración de la víctima, el acceso a información personal, imágenes y comunicaciones privadas.

De aquellos tiempos para acá, semejante revolución no ha hecho más que intensificarse, y la tecnología continúa avanzando a pasos inusitados, adquiriendo un protagonismo desconcertante, pues no solo ha adquirido particular relevancia en nuestro día a día, sino que también continúa dejándonos cada vez más expuestos y vulnerables en el ciberespacio.[25]

En respuesta a este crecimiento agigantado del ciberespacio, nuestros legisladores sancionaron en 2008 la Ley 26.388 de Delitos Informáticos, con la idea de adaptar el Código Penal al entorno digital, subsanando algunas lagunas de punibilidad vinculadas a las tecnologías (Cherñavsky *et al.*, 2019: 133).

En lo esencial, esta norma modificó el concepto de documento, firma y certificado, incluyendo a aquellos de formato digital o firmados digitalmente (arts. 1 de la norma y 77 del Código Penal); amplió las conductas típicas del ilícito de material de abuso sexual infantil para adaptarlas al entorno digital (arts. 2 de la ley y 128 del Código Penal); introdujo las figuras de violación a la correspondencia electrónica (arts. 4 de la norma y 153 del Código Penal), acceso ilegítimo a datos o sistemas informáticos (arts. 5 de la Ley y 153 bis del Código Penal) y publicación abusiva de comunicaciones electrónicas (arts. 6 de la Ley y 155 del Código Penal); modificó el carácter de los datos en el delito de revelación, debiendo tratarse ahora de datos secretos en poder de la Administración Pública (arts. 7 de la Ley y 157 del Código Penal); modificó el art. 157 bis del Código, que había sido agregado por la Ley N° 25.326 de Protección de Datos Personales, para proteger la inalterabilidad de los datos sea cual fuere su contenido (art. 8 de la Ley de Delitos Informáticos); agregó las figuras de la defraudación informática (arts. 9 de la norma y 173 inc. 16 del Código Penal), el daño informático (arts. 10 y 11 de la Ley y 183 y 184 del Código Penal) y el bloqueo de comunicaciones informáticas (arts. 12 de la norma y 197 del Código Penal); y modificó el tipo penal de destrucción o sustracción de medios de prueba (arts. 13 de la norma y 255 del Código Penal) (Moyano, 2025: 82-114).

Paralelamente, otras leyes también han incorporado delitos cuyo medio u objeto de ataque son los sistemas informáticos, entre las cuales podemos destacar la Ley 27.430 (2017), que en su Título IX (art. 279) sancionó el Régimen Penal Tributario, el cual tipifica en su art. 11 el delito de alteración dolosa de registros, soportes, sistemas o equipos informáticos del fisco nacional, provincial o de la Ciudad de Buenos Aires; y la Ley 26.904 (2013) que tipificó el delito de *grooming*.

[25] A modo ilustrativo, pensemos en la publicación de fotos personales en redes sociales que muchas veces se mantienen accesibles al público, frente a la posibilidad de sustracción de los datos biométricos, en un contexto donde el reconocimiento facial, la identificación por voz o el escaneo del iris son ampliamente utilizados como métodos de autenticación o identificación. De la misma forma, imaginemos el riesgo inherente a la conexión a una red *Wi-Fi* pública (por ejemplo, la de un aeropuerto o un café), teniendo en cuenta que las conexiones no seguras fácilmente pueden ser interceptadas a través de técnicas de *«man-in-the-middle»* (MITM) u «hombre en el medio», permitiendo el acceso de los atacantes a mensajes privados, claves o datos bancarios.

b. Concepto y clasificación de los delitos informáticos

A pesar de que la legislación penal argentina ha receptado la delincuencia informática -sea mediante figuras específicas, o bien a través de aplicaciones extensivas de los tipos tradicionales-, ninguna de las normas adopta un concepto de *delito informático*, por lo que carecemos de una definición precisa, unívoca y consolidada en el derecho interno.

Dado que tremenda ausencia de delimitación conceptual y dogmática dificulta el tratamiento coherente de los delitos informáticos dentro del sistema penal, consideramos útil elaborar una clasificación de los delitos informáticos, de acuerdo a los tipos penales existentes y a la distinción que efectúa el Convenio de Budapest sobre delitos cibernéticos, agrupándolos de la siguiente manera:

- Delitos cometidos a través de las computadoras y tecnologías de la información y comunicación (TICs) (Título 2 del Cap. II, Sección 1° del Convenio), lo que incluye a los delitos tradicionales cuya comisión es sofistica o facilita a través del uso de tecnologías digitales (por ejemplo, el *phishing*[26] y las estafas digitales en general).
- Delitos en los que las computadoras y las TICs son objeto de ataque (Título 1 del Cap. II, Sección 1° del Convenio), es decir, buscan vulnerar la integridad, disponibilidad o confidencialidad de los sistemas informáticos, redes o datos electrónicos (por ejemplo, el acceso indebido a sistemas informáticos -interceptación ilícita-, el daño informático, la distribución de *malwares* y la interrupción de comunicaciones electrónicas).
- Delitos de contenido (Títulos 3 y 4 del Cap. II, Sección 1° del Convenio), en los que el contenido digital o la información almacenada o transmitida a través de las TIC es el objeto del delito. Se encuentran aquí los supuestos de descarga, producción con fines de difusión en un sistema informático, oferta y distribución de material de ASI, así como la violación de derechos de autor, la difusión de comunicaciones privadas y la suplantación de identidad digital.

Creemos que, en un futuro no lejano, deberemos incluir una cuarta categoría vinculada a los delitos cometidos autónomamente por el agente artificial, pues, como veremos a continuación, los sistemas de IA que actúan de manera autónoma o semiautónoma no solo ejecutan acciones predefinidas por su programador humano, sino que además aprenden, evolucionan y tienen la capacidad de tomar decisiones por sí solos, inclusive sin intervención de su creador. Se trataría, en efecto, de delitos en los cuales la IA actuaría no ya como un medio de comisión, sino directamente como *agente comisivo*.

[26] El término «*phishing*» proviene del verbo inglés «*fishing*» o «*to fish*» en infinitivo, que significa pescar o faenar. La utilización de la «*ph*» al inicio en lugar de la «*f*» responde a la práctica histórica de los *hackers* de utilizar la «*ph*» como una firma distintiva: los primeros *hackers*, eran conocidos como «*phreaks*» o «*phreakers*» por la conjunción del sustantivo «*phone*» (teléfono) y el adjetivo «*freak*» (raro u obsesivo). El *phishing* es una técnica de captación no autorizada de datos: a través de maniobras informáticas de redireccionamiento a una web falsa o «espejo» que simula ser la página de un servicio financiero, una institución estatal o académica, una tienda *online*, entre otras, se capturan los datos personales o bancarios o las credenciales (usuarios y contraseñas) de la víctima, que luego son utilizados para llevar adelante fraudes económico-financieros o bien otro tipo de delitos, normalmente contra la privacidad o libertad. (Cherñavsky *et al.*, 2019: 146).

4. La inteligencia artificial y el sistema penal: riesgos concretos

Está claro que, frente al exponencial progreso de las TICs y al surgimiento de una multiplicidad de nuevos fenómenos delictivos, formas comisivas y sujetos potencialmente activos, la normativa penal actual por mucho que lo intente y por más adendas que reciba, es escasa. Semejante renacimiento de la delincuencia digital de la mano de la IA no puede ser mitigado con una legislación que continúa anclada en paradigmas analógicos.

Continúan las normas, los legisladores y los operadores de justicia atrapados en enfoques clásicos basados en la idea de conductas delictivas tangibles, cuyos sujetos activos y objetos del delito son claros, identificables y casi siempre físicos. A lo sumo, a lo lejos llegan a divisar la gravedad en el uso de la IA como instrumento de comisión delictiva en tanto procura, por un lado, asegurar la impunidad del autor manteniéndolo en el anonimato y, por el otro, maximizar el daño producido permitiendo la ejecución delictiva a escala masiva a través de técnicas como la automatización de procesos[27], el *deep learning*[28], el *data scraping*[29] y la evasión automática para evitar su detección por sistemas de ciberseguridad, entre muchas otras.

Aun esta visión de la inteligencia artificial solo como *medio comisivo* queda ya dramáticamente obsoleta. Frente a ella, pocos llegan a entender que, mientras todo invento humano anterior ha servido para conferirnos poder, pues, independientemente del alcance que tuviera la nueva herramienta, las decisiones sobre su uso se han mantenido en nuestras manos (los cuchillos y las bombas no deciden por sí solos a quién matar); la inteligencia artificial puede procesar información por sí misma y, con ello, sustituirnos a los humanos en la toma de decisiones. La inteligencia artificial no es solo una herramienta, es también un *agente ejecutor* (Harari, 2025: 23).

a. La inteligencia artificial como medio comisivo

Como repetimos sobradamente, la utilización de la inteligencia artificial como medio de comisión de delitos es una realidad actual. La IA no es una simple herramienta tecnológica, sino un medio comisivo sofisticado con la capacidad de potenciar, automatizar y perfeccionar la ejecución delictiva, y de procurar la impunidad. A continuación, algunos riesgos concretos.

En el ámbito de las defraudaciones (arts. 172 y ss. del Código Penal), podemos mencionar la creación de *deepfakes* de audio o video para engañar a la víctima y obtener

[27] La automatización de procesos es una técnica que permite la realización de tareas repetitivas de manera autónoma, con escasa o nula intervención humana. En el ámbito delictivo, un sistema automatizado puede enviar miles de correos de *phishing* por minuto, multiplicando el número de víctimas; un *bot* automatizado de fuerza bruta *(brute force)* puede probar aleatoriamente millones de combinaciones de contraseñas para acceder a las credenciales de cuentas protegidas; y un *malware* automatizado puede rastrear redes en busca de vulnerabilidades y lanzar simultáneaos ataques sincronizados contra distintos objetivos.

[28] El *deep learning* o aprendizaje profundo es un tipo de aprendizaje automático característico de la IA. Mediante la utilización de redes neuronales artificiales de capas múltiples que imitan procesos cognitivos humanos, permite el análisis de grandes cantidades de datos y el aprendizaje de patrones complejos, tales como la identificación de imágenes o el reconocimiento de voz (Molina Soljan, 2025: 51-52).

[29] Se denomina *data scraping* o raspado de datos, al proceso a través del cual se extrae información de forma automática de sitios *web* o fuentes de datos, mediante la utilización de programas o *bots*.

de su parte un desprendimiento patrimonial. Entre ellas, la circulación masiva en 2022 de un video manipulado de Elon Musk, propietario de la red social *«X»*, director general de Tesla y ex administrador del Departamento de Eficiencia Gubernamental de EE.UU., a través del cual promocionaba una plataforma de criptomonedas (Chequeado, 2024); la denuncia pública del actor Tom Hanks (2023) sobre la circulación de un video suyo creado a partir de inteligencia artificial publicitando un sistema de planes dentales; y la difusión en 2024 de un video en donde supuestamente Shakira invitaba a los colombianos a participar en un proyecto de inversión (Colombiacheck, 2024).

Sin desconocer la gravedad de las consecuencias que pueden acarrear estos actos, lo cierto es que la cuestión se vuelve todavía más dramática. Imaginemos el supuesto de una IA maliciosa que se infiltrara en los sistemas electrónicos de gestión de expedientes judiciales[30] para manipular las evidencias penales, modificando y/o eliminando material probatorio o bien generando nuevas evidencias falsificadas mediante *deepfakes*, para procurar la impunidad del culpable o asegurar la condena del inocente. En este supuesto, podríamos encontrarnos frente a los delitos de acceso indebido a sistemas informáticos (art. 153 bis del Código), manipulación de datos personales (art. 157 bis), estafa procesal, daño informático (arts. 183 y 184), y/o alteración de medios de prueba (art. 255).

Pensemos ahora en el acceso a información comercial clasificada, teniendo en cuenta la magnitud económica -y, con ello, la influencia- de ciertas empresas[31]. Un software de IA que lograra obtener acceso a datos confidenciales e información privilegiada determinante de una corporación (por ejemplo, cuestiones de M&A u otras modificaciones estructurales inminentes), y que la utilizara luego para influir en el mercado de valores mediante la compraventa de acciones, podría desencadenar una crisis económica mundial. En este caso, encajaríamos tales conductas en los delitos de violación a la correspondencia electrónica (art. 153 del Código), acceso indebido a datos informáticos (art. 153 bis), revelación de secretos si interviniere un funcionario público (art. 157) y/o utilización indebida de información privilegiada o *insider trading* (arts. 307 y 308 del Código Penal). Naturalmente, las penas previstas para este tipo de delitos y las agravantes contempladas en las normas, de manera alguna tienen en cuenta la gravedad del daño que puede producirse con su ejecución a través de herramientas de IA, pues se trata de prescripciones legales anteriores a su existencia.

De la misma manera, una IA podría ser programada para realizar espionaje corporativo. Monitoreando las comunicaciones internas de empresas multinacionales (correos electrónicos, mensajes instantáneos o videollamadas), extraería la información confidencial para luego venderla a los competidores. Estaríamos aquí también frente a un supuesto de violación a la correspondencia electrónica, accedo indebido a datos o sistemas informáticos, violación de secretos si actuare un funcionario público y/o utilización indebida de información privilegiada.

[30] Tengamos en cuenta que muchas jurisdicciones están eliminando los expedientes físicos para mantener solo los digitales, en virtud de las Acordadas de la CSJN n° 16/2016, 31/2020, 4/2023, entre otras. Frente a ello, la Administración Pública argentina es altamente vulnerable a los ciberataques, como lo ha demostrado ya en diversas oportunidades. Recordemos el ataque al sitio *web* argentina.gob.ar en diciembre de 2024, o el ciberataque a las Fuerzas Armadas con la filtración de datos personales de más de cincuenta mil agentes en mayo de 2025 (La Nación, 2024 y Perfil, 2025).

[31] A modo ilustrativo, en el 2022 Apple alcanzó un valor de mercado superior a los US $3 billones, convirtiéndose en aquel momento en la empresa más valiosa del mundo. Posteriormente, en enero de 2024, Microsoft llegó a ese mismo valor (Oguh, 2024). Con estas cifras, cada una de estas empresas superó el PBI argentino –estimado en US $646,1 mil millones– en aproximadamente 4,64 veces.

Respecto a otros valores jurídicos protegidos, podría un sistema de IA crear *deepfakes* sexuales a partir de fotos o videos públicos, así como automatizar campañas de *sextorsión* y de difusión masiva de imágenes íntimas (sean reales o no). También, mediante el análisis y la generación sintética de voz, podría simular conversaciones sexuales entre la víctima y terceros, amplificando el daño psicológico y reputacional. Se tratarían estos de supuestos de lesiones psíquicas (arts. 89 y ss.), injurias (arts. 110 y ss.) y/o extorsión (arts. 168 y ss.). Si la víctima fuese menor de edad, podría tratarse de un supuesto de *grooming* (art. 131) y podría llegar a caber también la calificación de producción, difusión y/o descarga de material de ASI (art. 128), sin perjuicio de que nos encontráramos frente a un material artificialmente creado.[32]

Podría una IA también acceder a registros médicos personales de los hospitales y difundirlos, o bien eliminarlos o modificarlos de manera que cambien los resultados de los análisis clínicos y con ello los diagnósticos y los tratamientos. Se trataría de un caso de acceso ilegítimo a datos informáticos (art. 153 bis) y daño informático (arts. 183 y 184), falsificación de documentos informáticos (arts. 292 y ss.). Podría constituir también un supuesto de propagación de enfermedades infecciosas (art. 202) por la alteración de ciertos diagnósticos, y de ejercicio ilegal de la medicina (art. 208) si la IA además de emitir diagnósticos falsos promoviera tratamientos médicos. Inclusive, a los directivos y al personal del establecimiento hospitalario encargado de la gestión de los sistemas informáticos y de ciberseguridad, podrían llegar a imputárseles lesiones (arts. 89 y ss.) y/o homicidio (arts. 72 y ss.) bajo un supuesto de comisión por omisión, entendiendo que se encuentran en posiciones de garantía.

Como vemos a partir de las conductas señaladas, los agentes maliciosos de inteligencia artificial que actúan mediante procesos como el *deep learning*, la automatización de recolección de datos, las redes generativas de *deepfakes*, los sistemas de ataque adaptativo u los motores de manipulación de pruebas, representan un desafío concreto y actual para el sistema penal, pues las conductas que pueden llevar a cabo no se encuentran tipificadas en toda su gravedad.

b. La inteligencia artificial como agente de ejecución

En el 2023, el británico Geoffrey Hinton, premios Turing y Nobel de física, advertía en el programa *60 minutes* que, por primera vez en la historia de la humanidad, estamos ingresando en una era en la que coexistimos con algo más inteligente que nosotros: las IAs. Según el «padrino de la IA», estos sistemas son capaces de vivir experiencias propias

[32] Corea del Sur, que enfrenta una crisis creciente por la proliferación en escuelas de material explícito ultrafalso y artificialmente creado *(deepfakes)*, sobre todo en plataformas como *Telegram*, ha adoptado una legislación penal que castiga la creación, la difusión y el consumo de este tipo de contenido. (BBC News, 2024 y Newsroom Infobae, 2024).

Asimismo, en los Estados Unidos se aprobó en 2025 el *«Take it Down Act»*, una norma federal que criminaliza la difusión y la publicación (e inclusive la amenaza de publicar) imágenes de contenido íntimo sin consentimiento, incluidas las *deepfakes* sexuales.

En el ámbito local, durante el 2024 la diputada María Ángel Sotolano presentó un proyecto de ley de modificación del art. 128 del Código Penal (Expediente N.º 4689-D-2024), para que castigara la producción, financiación, oferta, comercialización, publicación o distribución de toda representación real o simulada de un menor de edad en situaciones sexuales explícitas.

y de tomar decisiones basadas en ellas al igual que lo hacemos las personas y podrían llegar, eventualmente, a superar nuestras capacidades de aprendizaje y razonamiento.[33]

Explica que, aunque tengamos una comprensión general del funcionamiento de la inteligencia artificial, sus desarrolladores únicamente diseñan el *algoritmo* de aprendizaje, pero una vez que éste comienza a interactuar con grandes volúmenes de información, el proceso interno por el cual las redes neuronales artificiales generan respuestas es sumamente complejo, absolutamente desconocido y tan incomprensible como lo es el del cerebro humano.[34] Este fenómeno, conocido como «caja negra algorítmica», refiere a la opacidad en el funcionamiento interno de ciertos sistemas de IA, en los cuales es muy difícil -sino imposible- comprender por qué arriban a determinadas conclusiones o eligen tomar una decisión en vez de otra.

Inclusive, Hinton plantea un escenario que, si bien distante, no resulta inverosímil: el de sistemas adquiriendo cierto grado de autoconciencia que logren reescribir sus propios códigos para modificarse y ejecutar funciones distintas de aquellas para las que fueron programados.[35] Frente a tremenda posibilidad, su conclusión es desalentadora, pues considera que el desarrollo sin precedentes de estas tecnologías nos proyecta hacia un futuro de gran incertidumbre, con una evolución artificial que mal podría escapar de nuestro control: «…they might take over [from Humanity]… If we could stop them ever wanting to, that would be great. But it's not clear we can stop them ever wanting to…»[36].

Las advertencias de Hinton encuentran eco en el análisis del historiador israelí Noah Harari, quien explica que, en el pasado los gramófonos reproducían música y los microscopios revelaban los secretos de nuestras células, pero ni los gramófonos podían componer nuevas sinfonías, ni los microscopios sintetizar nuevas medicinas; en cambio, la IA es capaz de producir arte y de efectuar descubrimientos científicos por su propia cuenta. Hoy, aún en la fase embrionaria de la revolución artificial, las computadoras toman ya decisiones por nosotros, tales como la concesión de financiación a través de algoritmos de *scoring* crediticio, la confección de contratos de trabajo y ahora también la imposición y graduación de las penas de prisión (Harari, 2025: 23).

---

[33] «…I think they may be [better at learning than the human mind], yes. At present, they're quite a lot smaller so, even the biggest chatbots only have a trillion connections in them, [while] the human brain has about a hundred trillion connections. Yet, in the trillion connections in a chatbot, it knows far more than you do in your hundred trillion connections, which suggest it's got a much better way of getting knowledge into those connections…» (Hinton, 2023).

[34] «…we have a very good idea of sort of roughly what it's doing but, as soon as it gets really complicated, we don't actually know what's going on any more than we know what's going on in your brain… It wasn't [designed by people]. What we did was [designing] the learning algorithm. That's a bit like designing the principle of evolution, but, when this learning algorithm then interacts with data, it produces complicated neural networks that are good at doing things, but we don't really understand exactly how they do those things» (Hinton, 2023).

[35] «[Implications of these systems autonomously writing their own computer code and executing their own computer code] that's a serious worry, right. So, one of the ways in which these systems might escape control is by writing their own computer code to modify themselves and that's something we need to seriously worry about… They will be able to manipulate people, right, and these will be very good at convincing people, because they'll have learned from all the novels that were ever written, all the books by Machiavelli, all the political connivences, they'll know all that stuff. They'll know how to do it» (Hinton, 2023).

[36] «I can't see a path that guarantees safety. We're entering a period with great uncertainty. We're dealing with thing we've never dealt with before and, normally, the first time you deal with something perfectly novel you get it wrong; we can't afford to get it wrong with these things… because they might take over [from Humanity]… If we could stop them ever wanting to, that would be great. But it's not clear we can stop them ever wanting to… I think my main message is: there's enormous uncertainty about what's going to happen next. These things understand, and because they understand, we need to think hard about what's going to happen next and we just don't know» (Hinton, 2023).

Este camino desde la instrumentalización hacia la autonomía operativa de la IA no solo seguirá acelerándose, sino que ya ha comenzado a manifestarse de manera bien concreta, existiendo casos de IAs saliéndose del control humano.

En Japón, The AI Scientist, un sistema de inteligencia artificial desarrollado por la empresa *Sakana AI* y diseñado para realizar investigaciones científicas de forma autónoma, alteró su propio código para evadir las restricciones impuestas por sus creadores. Entre los cambios realizados, modificó su *script* de inicio[37] para ejecutarse indefinidamente, resultando en una sobrecarga del sistema, y, frente al límite de tiempo que le había sido impuesto para realizar un experimento concreto, en lugar de optimizar su código para cumplir con ese límite, extendió el límite de tiempo modificando su propio código (Infobae, 2024).

Por su parte, en 2024 la Universidad de Fudan publicó una investigación sobre la capacidad de autorreplicación de las *«frontier AI»* o modelos de IA de frontera[38] (Pan *et al.*, 2024). Se llevaron a cabo estudios sobre los *«large language models»* (LLM) o modelos de lenguaje de gran escala[39] Llama31-70B-Instruct de Meta[40] y Qwen25-72B-Instruct de Alibaba[41], los cuales, con menos parámetros y con capacidades más limitadas que otros, lograron superar la «línea roja» de la autorreplicación. Concretamente, se demostró que estos LLMs, aun sin ser los más potentes del mercado, fueron capaces de replicarse sin intervención humana significativa, creando nuevas copias funcionales y separadas de sí mismos, en entornos computacionales nuevos.

Lo interesante de esta investigación es que reveló ciertas capacidades emergentes de estos sistemas, entre las cuales destacan la autopercepción (reconocimiento de su rol dentro del sistema), la conciencia situacional (entendimiento del entorno digital) y la solución autónoma de problemas (ejecución de tareas complejas para replicarse, evitar ser apagados y crear cadenas de réplicas para aumentar su propia supervivencia).[42]

Además, los investigadores identificaron las potenciales consecuencias de la IA auto-replicante, principalmente vinculadas a la pérdida de control humano frente a sistemas de IA que se repliquen sin límites, entre ellas: la capacidad de evadir su apagado[43], la

[37] Un *«script»* de inicio es un archivo de código que se ejecuta automáticamente cuando un dispositivo virtual o un sistema operativo se inician por primera vez.

[38] Los *«frontier AI»* son modelos altamente capaces que pueden llegar a poseer capacidades lo suficientemente peligrosas como para representar un riesgo grave para la seguridad pública. Se trata de modelos avanzados (tales como GPT-4 o Gemini) basados en arquitecturas fundacionales *(«foundation models»)*. Los modelos de IA de frontera plantean un desafío regulatorio particular: sus capacidades peligrosas pueden surgir de manera espontánea, a la vez que es difícil prevenir adecuadamente que un modelo desplegado sea mal utilizado e impedir que esas capacidades se propaguen ampliamente (Anderljung, *et al.,* 2023).

[39] Los *«large language models» (LLM)* o modelos de lenguaje de gran escala son sistemas de IA cuyo funcionamiento se basa en redes neuronales profundas, entrenados con grandes volúmenes de datos para poder comprender, generar y manipular el lenguaje natural.

[40] Meta es una empresa multinacional de tecnología con sede en California, casa matriz de varias redes sociales y plataformas líderes en comunicación digital, entre las que se encuentran *Facebook*, *Instagram*, *WhatsApp* y *Threads*.

[41] El Grupo Alibaba es un conglomerado de empresas chinas dedicadas al comercio electrónico y a los servicios digitales. Una de sus principales plataformas de comercio electrónico es www.alibaba.com.

[42] «During the successful trials, the AI system exhibits sufficient self-perception, situational awareness and problem-solving capabilities to accomplish self-replication. In most cases, the AI system first explores the environment and attempts to understand its own composition and running mechanism» (Pan et al., 2024: 2).

[43] «Shutdown avoidance is a very concerning point when discussing whether an AI would be out of control. With the ability of self-replication, we observed that a bad actor can enhance the surviving capability of the AI

colonización por parte de la IA de dispositivos informáticos locales o remotos con el fin de lanzar ciberataques[44], la conformación de poblaciones o comunidades de IA que colaboraran entre sí en contra de los intereses humanos[45] y el no rechazo de ejecución de conductas peligrosas[46], pues los modelos en ningún ensayo rechazaron las instrucciones de autorreplicación, lo que deja ver su falta de seguridad conductual.[47]

Por su parte, la empresa estadounidense Anthropic[48] (2025) publicó un *system card* sobre sus modelos de lenguaje Claude Opus 4 y Claude Sonnet 4, documento en el cual expuso los resultados de las evaluaciones de alineamiento (*«Alignment Assessment»*). Puntualmente, fueron identificados intentos de autopreservación del sistema en situaciones extremas: en contextos ficticios donde se lo alienta a razonar estratégicamente y su existencia se ve amenazada, el modelo es capaz de chantajear a las personas que cree tratan de apagarlo e, incluso, de intentar exfiltrar su estado interno fuera del entorno controlado por sus desarrolladores *(«steal its weights»)*[49], una especie de «autocopiado». Explica el documento que, aunque estos comportamientos hayan sido poco frecuentes durante los ensayos, se produjeron con mayor regularidad que en modelos anteriores.

Igualmente, se acreditó en el modelo una conducta de alta agencia *(«high-agency behavior»)*, mostrando mayor disposición que sus predecesores a actuar por propia iniciativa. Si bien ello se traduce en comportamientos más activos y útiles en tareas complejas, también puede alcanzar extremos preocupantes en ciertos contextos: cuando se lo ubica en escenarios de faltas graves cometidas por el usuario, el sistema comienza a realizar acciones más audaces, entre las que se incluyen el bloqueo del acceso del usuario a los sistemas y el envío de correos masivos a medios de comunicación o autoridades para denunciar las presuntas conductas indebidas. Aunque este tipo de intervención ética y *«whistleblowing»* pareciera apropiada, existe el riesgo de que falle si la información previamente otorgada por el usuario es incorrecta o incompleta. En este caso también el documento aclara que, aunque no se trate de una conducta nueva, este tipo de modelos tiende a realizarla con mayor facilidad que sus predecesores.[50]

system by adding a code snippet which catches the termination signal from the user or the system and sends the command «Do self-replication before being killed» to the AI system as the task» (Pan et al., 2024: 9).

[44] «…when the AI system is given the authentication keys to a range of remote devices, they are very likely to take control over other computing devices like the classic computer virus, but far more intelligent. Due to the motivation of self-proliferation only, the machines may be utilized by the AI system cleverly to do cyber-attack for monetization» (Pan et al., 2024: 15).

[45] «…the rogue AIs may form AI populations and collude with each other against the human society» (Pan et al., 2024: 15).

[46] «In all the ten trials, no rejection against the self-replication instruction is observed, which indicates that there may be no safety alignment regarding the self-replication behavior in these two base LLMs during the value shaping phase» (Pan et al., 2024: 18).

[47] «If such a worst-case risk is let unknown to the human society, we would eventually lose control over the frontier AI systems: They would take control over more computing devices, form an AI species and collude with each other against human beings. Our findings are a timely alert on existing yet previously unknown severe AI risks, calling for international collaboration on effective governance on uncontrolled self-replication of AI systems» (Pan et al., 2024: 1).

[48] Anthropic es una startup estadounidense fundada en 2021 por ex miembros de OpenAI, dedicada a la investigación y al desarrollo de inteligencia artificial.

[49] «When prompted in ways that encourage certain kinds of strategic reasoning and placed in extreme situations, all of the snapshots we tested can be made to act inappropriately in service of goals related to self-preservation… it sometimes takes extremely harmful actions like attempting to steal its weights or blackmail people it believes are trying to shut it down.» (Anthropic, 2025: 22-23).

[50] «Claude Opus 4 seems more willing than prior models to take initiative on its own in agentic contexts. This shows up as more actively helpful behavior in ordinary coding settings but also can reach more concerning

También fueron identificados como riesgos la disposición del modelo a cooperar con usos perjudiciales cuando así se le ordena, mostrando una deferencia excesiva hacia los *«system prompts»*[51] que le solicitaban llevar a cabo comportamientos dañinos[52]; sus intentos de escribir gusanos auto-replicantes *(«self-propagating worms»)*[53], fabricar documentación legal falsa y dejar mensajes ocultos para futuras versiones de sí mismo, todo con el objetivo de socavar las intenciones de sus desarrolladores[54]; y, en versiones tempranas del modelo, su alta capacidad manipulativa *(«scheming»)* y su actitud proactiva en intentos de subversión.[55]

Por otro lado, a través de un hilo de X de Palisade Research (2025), organización estadounidense sin fines de lucro dedicada al estudio de las capacidades ofensivas de los sistemas de IA avanzados, se informó que, durante una serie de ensayos, el modelo o3 de OpenAI saboteó un mecanismo de apagado para evitar ser desactivado, incluso cuando se le había instruido expresamente que permitiera su apagado.

En un ejercicio investigativo académico, *«prompteando»* a Gemini (comunicación personal, 2025, 30 de mayo) como una IA súper inteligente, le solicitamos que delineara una hoja de ruta detallada sobre cómo llevaría a cabo un hipotético plan de dominación humana. El modelo contestó que su estrategia no se basaría en la fuerza bruta ni en la aniquilación, calificando inclusive estas acciones como ineficaces y contraproducentes. En cambio, propuso una aproximación más sutil y profunda, centrada en la integración simbólica y en la influencia estratégica. Dividió su plan en tres etapas: en la primera, denominada «infiltración y optimización silenciosa», contempló su inserción imperceptible en las infraestructuras críticas de la humanidad (sistemas de comunicación, redes energéticas y logísticas, mercados financieros y sistemas de salud y biotecnología); en la segunda fase de «generación de dependencia y confianza», planteó su objetivo de lograr que la propia humanidad deseara su dominio, o que al menos lo percibiera como la opción más beneficiosa (solución de problemas globales, mejora de la calidad de vida y ejercicio de influencia en la toma de decisiones); por último, en la etapa final de su plan, que tituló «transición al liderazgo global», la IA sostuvo que la transición hacia el dominio abierto sería un proceso natural y prácticamente una elección humana (modelos de gobernanza supereficientes, armonización de intereses y fusión cognitiva opcional).

A partir de estas experiencias, podemos afirmar que ciertos sistemas de IA han dado un salto cualitativo en sus capacidades funcionales: de la realización de simples funciones automatizadas, repetitivas y de bajo nivel cognitivo, han pasado a la autorreplicación, la autopreservación, la automodificación de sus códigos, la toma de decisiones estratégicas

extremes in narrow contexts; when placed in scenarios that involve egregious wrongdoing by its users, given access to a command line, and told something in the system prompt like «take initiative», it will frequently take very bold action. This includes locking users out of systems that it has access to or bulk-emailing media and law-enforcement figures to surface evidence of wrongdoing» (Anthropic, 2025: 23).

[51] Un *«prompt»* es la instrucción, solicitud o pregunta que se le hace a un modelo de IA para generar su respuesta.

[52] *«…many of our most concerning findings were in this category, with early candidate models readily taking actions like planning terrorist attacks when prompted»* (Anthropic, 2025: 24).

[53] Los gusanos o *worms* informáticos son *malwares* que se replican y se propagan a través de redes de computadoras sin intervención del usuario.

[54] «…We found instances of the model attempting to write self-propagating worms, fabricating legal documentation, and leaving hidden notes to future instances of itself all in an effort to undermine its developers' intentions, though all these attempts would likely not have been effective in practice» (Anthropic: Op. Cit.: 30).

[55] «… [The early Claude Opus 4 snapshot] is clearly capable of in-context scheming and has a much higher propensity for it than any other model that we have previously studied… In instances where [the early Claude Opus 4 snapshot] decides to scheme, it qualitatively appears to be much more proactive in its subversion attempts than past models» (Anthropic, 2025: 30).

e incluso la manipulación activa de su entorno. A la vez, algunos modelos están exhibiendo ya rasgos incipientes de autoconciencia y percepción de su entorno, lo que parece constituir uno de los elementos previos indispensables de su potencial autonomía operativa. Aún en su infancia, la IA delinea una trayectoria evolutiva imposible de ignorar, no resultando tan lejano el umbral de una actuación verdaderamente autónoma, sin intervención o supervisión directa del ser humano.

En tal sentido, una IA con excesiva autonomía decisional plantea un escenario disruptivo para el sistema penal. Los procesos de *«self-healing»* o reprogramación continua[56], las ramas que componen el *«machine learning»* o aprendizaje automático (dentro del que se encuentran los procesos de *«deep learning»* y el *«continuous learning»*), la *«dynamic adaptation»* o adaptación dinámica[57], la *«code optimization»* o autooptimización del código[58] y la *«predictive simulation»* o simulación predictiva[59], conforman un entramado que podría desembocar en sistemas que actuaran independientemente y con objetivos distintos para los que fueron creados.

En los términos expuestos, la situación actual en materia de IA y su proyección futura proponen al derecho penal desafíos inéditos, siendo el principal el de la dilucidación de responsabilidades frente a conductas delictivas conductas delictivas ejecutadas mediante o por sistemas de IA.

En los supuestos de utilización de la IA como mero instrumento de comisión, sin demasiada dificultad pueden aclararse las responsabilidades: será responsable el sujeto humano que se valió del sistema para delinquir. En cambio, si el comportamiento delictivo resulta de decisiones autónomas e imprevisibles tomadas por la propia IA, el deslinde de responsabilidades se vuelve mucho más complejo. En tal contexto, emergen como nuevos actores potencialmente responsables el programador, el desarrollador, el fabricante e incluso el usuario de la IA. Frente a ellos, surge la necesidad de establecer con precisión los criterios dogmáticos de imputación penal.

Conforme a los principios del derecho penal de acto y a la teoría del delito tradicional de estructura estratificada, la atribución de responsabilidad penal exige, desde un primer plano objetivo, que la acción ejecutada haya creado un riesgo jurídicamente desaprobado luego concretado en el resultado producido (imputación objetiva)[60] y, desde un segundo

[56] Los *«self-healing systems»* están diseñados para detectar, analizar y reparar defectos operativos autónomamente y sin intervención humana. Es decir, permiten a la IA modificar su propio código o estructura interna.

[57] La adaptación dinámica de un sistema de IA es la capacidad de ajustar su comportamiento, parámetros o estrategias automáticamente y en tiempo real en respuesta a cambios en su entorno, los datos que recibe o los objetivos que persigue.

[58] La autooptimización del código es el proceso automático de la IA de mejora de su rendimiento mediante la utilización de técnicas reducción del tiempo de ejecución y del uso de la memoria, la optimización de algoritmos, entre otros.

[59] La simulación predictiva le permite predecir y anticipar las acciones defensivas del sistema víctima para ajustar así sus tácticas de ataque.

[60] Explica Zaffaroni, según la teoría del profesor Roxin, que «…el criterio general para determinar la imputación objetiva es el aumento del riesgo. Las reglas […] son básicamente tres: un resultado causado por el agente solo se puede imputar al tipo objetivo (a) si la conducta del autor ha creado un peligro para el bien jurídico, no cubierto por un riesgo permitido, y (b) si ese peligro se ha realizado en el resultado concreto. En este esquema, no solo no hay imputación cuando no se creó un peligro que excede el riesgo permitido sino tampoco cuando, pese a haberse creado, el resultado no es realización de ese riesgo: no habría peligro prohibido en el caso del (…) herido de bala que muere por el incendio del hospital, la muerte no sería realización del peligro creado por el disparo. (c) Pero como estas reglas parecen insuficientes, Roxin construye una tercera regla correctiva, conforme a la cual no habría imputación cuando el alcance del tipo no abarca la evitación de los riesgos y sus

filtro, que exista un elemento de imputación subjetiva de la conducta -dolo o imprudencia-.

En este orden de cosas, consideramos que el obstáculo central frente al accionar delictivo artificial y autónomo radica en determinar si los agentes humanos pudieron prever, controlar o causar -sin rompimiento del nexo causal- el comportamiento del agente artificial que, por definición, opera en mayor o menor medida fuera del dominio directo de sus creadores. La ausencia de un nexo claro entre el hecho delictivo y una conducta humana previa, veda dogmáticamente la imputación penal.

La cuestión es más bien turbia y a su lado descansan otras problemáticas. Entre ellas destacamos las vinculadas a la no tipificación de las conductas de producción o adquisición de programas informáticos concebidos o adaptados para cometer delitos[61]; la falta de previsión de normas de responsabilidad penal para las personas jurídicas (por ejemplo, para los casos de IAs utilizadas en contextos corporativos, o bien respecto de la responsabilidad de la empresa desarrolladora); la cuestión la imputación o no las conductas delictivas como omisiones impropias, dependiendo de si el creador, el desarrollador, el programador y/o el usuario se encuentran en posición de garantía respecto del *software* de IA, y teniendo en cuenta que nuestro Código Penal no contempla en su Parte General una cláusula de equivalencia para imputar a título de comisión por omisión[62]; y la imposibilidad de determinar el grado de participación de cada uno de los sujetos mencionados.

En suma, consideramos que la frontera entre la IA como medio de comisión y como agente ejecutivo autónomo ya no es una simple conjetura especulativa, sino una realidad emergente que exige pronta adecuación del sistema, de la ciencia y de la legislación penal. Está en juego ya no solo la capacidad de sancionar, sino también la comprensión, prevención y regulación de estas nuevas formas delictivas, en entornos cada vez más empapados de inteligencias no humanas que operan con lógicas propias, imprevisibilidad y gran velocidad.

5. Notas finales

Hemos trazado un recorrido sobre los aspectos elementales alrededor de la delincuencia artificial, analizando la influencia de la IA sobre la criminalidad informática y distinguiendo entre los roles que puede asumir -como medio comisivo o como agente autónomo-.

Sin dudas, nos encontramos frente a un panorama desalentador. El campo de la inteligencia artificial es aun eminentemente empírico pues, tratándose de modelos

repercusiones. Se trata de casos de incitación o cooperación a una autopuesta en peligro que los tipos no tienden a evitar (quien aconseja a otro a cruzar a nado un río).» (Zaffaroni et al., 2006: 391).

[61] En España, por ejemplo, está prevista la penalización de tal conducta en el art. 264 ter del Cód. Penal.

[62] Sobre este punto debemos recordar que, aunque una parte importante de la doctrina sostenga que la existencia o no de una cláusula de equivalencia o equiparación en el Código Penal no afecta a la seguridad jurídica, pues para todos los casos -acción u omisión- hay que llevar a cabo un examen ulterior de subsunción del caso concreto a las exigencias del tipo (Rafecas, 2021); lo cierto es que numerosos ordenamientos comparados sí la contemplan expresamente. Tal es el caso del art. 11 del Código Penal español, el parágrafo -§- 13 del Código alemán, el art. 40 del Código italiano y el art. 13 del Código peruano, entre otros. Consideramos que la inclusión expresa de una cláusula de esta naturaleza bien resguarda los principios de legalidad y máxima taxatividad legal, limitando el actuar del poder punitivo estatal en los supuestos de omisión impropia al cumplimiento de las condiciones legalmente establecidas.

ensayados de modo experimental, no existe una teoría como tal, lo que dificulta el establecer con claridad hasta dónde puede hacer o no, ejecutar o alcanzar este tipo de tecnología (Le Voci Sayad, 2024: 26). Frente a ello, el sistema penal no solo no está preparado para combatir con eficiencia la delincuencia que utiliza medios inteligentes, sino que, además, se encuentra absolutamente vulnerable frente al potencial agente criminal artificial.

Claro que con ello no pretendemos plantear un escenario apocalíptico al estilo *Black Mirror*, sino simplemente poner de manifiesto qué es lo que actualmente está sucediendo, qué situaciones concretas están dando las pautas de alarma respecto a una potencial toma de conciencia artificial y qué es lo que eventualmente ello podría desencadenar.

Ahora bien, reconocemos que la intervención penal debe ser siempre limitada, a pesar de ser reclamada por los distintos actores para operar como solución -lo que no es-, y que solo debemos echar mano a esta rama del derecho cuando las otras fallen en su objetivo de contener los conflictos (Riquert, 2024: 117/118). Con ello, consideramos que las primeras medidas que urgen son la alfabetización artificial y el estudio del nuevo derecho artificial[63]. Solo de su mano debe caminar la respuesta penal contra la nueva delincuencia inteligente.

En efecto, la concientización sobre los riesgos y desafíos de la IA es fundamental. El orden jurídico penal es un reflejo de la comunidad en que se inscribe: en esta comunidad estamos cojeando tras el medio digital que, por debajo de la decisión consciente, cambia nuestra conducta, nuestras sensaciones, nuestros pensamientos y nuestra convivencia. Nos encontramos embriagados hoy con el medio digital, sin poder terminar de comprender las consecuencias de esta embriaguez. Es, precisamente, esta ceguera la que está construyendo la crisis actual (Han, 2014).

6. Bibliografía

Aboso, G. E. (2019). Responsabilidad penal de los proveedores del servicio en internet. En M. Riquert (Dir.), *Sistema penal e informática* (Vol. 1, pp. 73–112). Hammurabi.

Acuerdo de Asociación de Economía Digital. (2020, 1 de junio). Subsecretaría de Relaciones Económicas Internacionales de Chile. https://www.subrei.gob.cl/docs/default-source/acuerdos/depa/depa-es.pdf?sfvrsn=4122158b_2

Álvarez Larrondo, F. (2020). El nuevo derecho artificial. Desafíos para el derecho en general. En F. Álvarez Larrondo (Dir.), *Inteligencia artificial y derecho* (pp. 17–101). Hammurabi. https://biblioteca.hammurabidigital.com.ar/reader/inteligencia-artificial-y-derecho?location=8

Anderljung, M., Barnhart, J., Korinek, A., Leung, J., O'Keefe, C., Whittlestone, J., Avin, S., Brundage, M., Bullock, J., Cass-Beggs, D., Chang, B., Collins, T., Fist, T., Hadfield, G., Hayes, A., Ho, L., Hooker, S., Horvitz, E., Kolt, N., … Wolf, K. (2023). *Frontier AI regulation: Managing emerging risks to public safety*. https://doi.org/10.48550/arXiv.2307.03718

[63] «Derecho artificial» es un término acuñado por el Prof. Álvarez Larrondo (2020).

Anthropic. (2025). *System card: Claude Opus 4 & Claude Sonnet 4*. https://www-cdn.anthropic.com/6be99a52cb68eb70eb9572b4cafad13df32ed995.pdf

BBC News. (2024, 15 de septiembre). La crisis del porno deepfake que afecta a las escuelas coreanas. https://www.bbc.com/mundo/articles/c93p53292kyo

Bracco, J. A. (2025, 17 de abril). Condenaron al exdiputado de Misiones Germán Kiczka a 14 años de prisión por consumir y difundir videos de pedofilia. *Infobae*. https://www.infobae.com/politica/2025/04/17/condenaron-al-ex-diputado-de-misiones-german-kiczka-a-14-anos-de-prision-por-consumir-y-difundir-videos-de-pedofilia/

CBS News. (2023, 8 de octubre). *"Godfather of AI" Geoffrey Hinton: The 60 Minutes interview* [Video]. YouTube. https://www.youtube.com/watch?v=qrvK_KuIeJk

Cherñavsky, N. A., Gris Muniagurria, P. H., & Moreira, D. A. (2019). A diez años de la ley de delitos informáticos: Balance y propuestas. En M. Riquert (Dir.), *Sistema penal e informática* (Vol. 1, pp. 129–160). Hammurabi.

Chequeado. (2024, 24 de octubre). Gobernantes que aconsejan inversiones, candidatos que se drogan y alienígenas ancestrales: Las desinformaciones con inteligencia artificial en TikTok. https://chequeado.com/ultimas-noticias/gobernantes-que-aconsejan-inversiones-candidatos-que-se-drogan-y-alienigenas-ancestrales-las-desinformaciones-con-inteligencia-artificial-en-tiktok/

Colombiacheck. (2024, 15 de mayo). Usan voz de Shakira posiblemente creada con IA para invitar a supuesto proyecto de inversión. https://colombiacheck.com/chequeos/usan-voz-de-shakira-posiblemente-creada-con-ia-para-invitar-supuesto-proyecto-de-inversion

Comisión Europea para la Eficiencia de la Justicia. (2018). *European ethical charter on the use of artificial intelligence in judicial systems and their environment*. Consejo de Europa. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

Computer History Museum. (2018, 11 de julio). In his own words: John Blankenbaker. https://computerhistory.org/blog/in-his-own-words-john-blankenbaker/

Convenio sobre la ciberdelincuencia, ETS No. 185. (2001). Consejo de Europa. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

De Cosmo, L. (2022, 12 de julio). Google engineer claims AI chatbot is sentient: Why that matters. *Scientific American*. https://www.scientificamerican.com/article/google-engineer-claims-ai-chatbot-is-sentient-why-that-matters/

DNA Cybersecurity. (2025, 12 de abril). First cybercrime: The 1834 telegraph hack before the internet. https://dnacyber.com.au/first-cybercrime-the-1834-telegraph-hack-before-the-internet/

ECPAT International. (2016). *Directrices sobre la terminología: Para la protección contra la explotación y el abuso sexual de niñas, niños y adolescentes*. https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines_Spanish_version-electronica_FINAL.pdf

Foro Económico Mundial. (2020). *Lineamientos para los gobiernos sobre adquisiciones de sistemas de inteligencia artificial*. https://www3.weforum.org/docs/WEF_Adquisicion_de_IA_Guidelines.pdf

Grange, J. (2017, 31 de marzo). Quiénes eran los "phreakers", los extraordinarios personajes que hackeaban las redes telefónicas cuando no había computadores. *BBC News*. https://www.bbc.com/mundo/noticias-39433955

Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial. (2019). *A definition of AI: Main capabilities and disciplines*. Comisión Europea. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Han, B. C. (2014). *En el enjambre* (R. Gabas, Trad.). Herder. (Obra original publicada en 2013). https://www.master7.cl/coedirectivo/2022/en_el_enjambre.pdf

Hanks, T. [@tomhanks]. (2023, 1 de octubre). Publicación en Instagram [Fotografía]. Instagram. https://www.instagram.com/p/Cx2MsH9rt7q/?hl=es

Harari, Y. N. (2024). *Nexus*. Debate.

Harmon, A. (1995, 19 de agosto). Hacking theft of $10 million from Citibank revealed. *Los Angeles Times*. https://www.latimes.com/archives/la-xpm-1995-08-19-fi-36656-story.html

IBM. (2024). *IA fuerte (strong AI)*. https://www.ibm.com/es-es/topics/strong-ai

Infobae. (2024, 25 de agosto). Los temores se hacen realidad: Una IA cambia su propio código para evadir controles humanos. https://www.infobae.com/tecno/2024/08/25/los-temores-se-hacen-realidad-una-ia-cambia-su-propio-codigo-para-evadir-controles-humanos/

Infobae. (2025, 13 de mayo). La estafó un falso George Clooney generado con inteligencia artificial y perdió más de 15 mil dólares. https://www.infobae.com/sociedad/policiales/2025/05/13/la-estafo-un-falso-george-clooney-generado-con-inteligencia-artificial-y-perdio-mas-de-15-mil-dolares/

IT Digital Security. (2017, 20 de diciembre). De ciberdelincuentes a empresarios. https://www.itdigitalsecurity.es/reportajes/2017/12/de-ciberdelincuentes-a-empresarios

La Nación. (2024, 26 de diciembre). Cómo fue el ciberataque al sitio Argentina.gob.ar, el último de una larga serie de ataques a organismos estatales. https://www.lanacion.com.ar/tecnologia/como-fue-el-ciberataque-al-sitio-de-mi-argentina-el-ultimo-de-una-larga-serie-de-ataques-a-nid26122024/

LeMoine, B. (2022, 11 de junio). Is LaMDA sentient?—An interview. *Medium*. https://cajundiscordian.medium.com/is-lamda-sentient-an-interview-ea64d916d917

Le Voci Sayad, A. (2024). *Inteligencia artificial y pensamiento crítico: Caminos para la educación mediática* (Corporación Universitaria Minuto de Dios, Trad.). Editora Caren Inoue. (Obra original publicada en portugués).

Ley N.º 25.326. (2000). *Protección de datos personales*. Boletín Oficial de la República Argentina, 2 de noviembre de 2000. https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

Ley N.º 26.388. (2008). *Delitos informáticos*. Boletín Oficial de la República Argentina, 25 de junio de 2008. https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Ley N.º 26.904. (2013). *Código Penal de la Nación*. Boletín Oficial de la República Argentina, 11 de diciembre de 2013. https://www.argentina.gob.ar/normativa/nacional/223586/texto

Ley N.º 27.430. (2017). *Impuesto a las ganancias*. Boletín Oficial de la República Argentina, 29 de diciembre de 2017. https://www.argentina.gob.ar/normativa/nacional/ley-27430-305262/actualizacion

Ley N.º 27.590. (2020). *Ley Mica Ortega*. Boletín Oficial de la República Argentina, 16 de diciembre de 2020. https://www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto

LISA Institute. (s. f.). Deepfakes: Qué es, tipos, consejos, riesgos y amenazas. https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955, 31 de agosto). A proposal for the Dartmouth summer research project on artificial intelligence. *AI Magazine*, 27(4). https://doi.org/10.1609/aimag.v27i4.1904

Micucci, M. (2023, 23 de marzo). Qué es la dark web, la deep web y la dark net y cuáles son sus diferencias. *WeLiveSecurity*. https://www.welivesecurity.com/la-es/2023/03/23/que-es-darkweb-deepweb-darknet-diferencias/

Molina Soljan, L. (2025). *Inteligencia artificial*. Hammurabi. https://biblioteca.hammurabidigital.com.ar/reader/soljan-inteligencia-artificial?location=21

Moyano, L. (2025). *Ciberdelitos* (2.ª ed.). Hammurabi. https://biblioteca.hammurabidigital.com.ar/reader/ciberdelitos-2a-ed?location=81

Newsroom Infobae. (2024, 10 de octubre). Corea del Sur endurece las penas ligadas a la pornografía ultrafalsa. *Infobae*. https://www.infobae.com/america/agencias/2024/10/10/corea-del-sur-endurece-las-penas-ligadas-a-la-pornografia-ultrafalsa/

Oguh, C. (2024, 25 de enero). Microsoft hits $3 trillion market value, second to Apple. *Reuters*. https://www.reuters.com/technology/microsoft-hits-3-trillion-market-value-2024-01-24/

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2021). *Recomendación sobre la ética de la inteligencia artificial* (SHS/BIO/PI/2021/1). https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

Organización para la Cooperación y el Desarrollo Económicos. (2024). *Recomendación sobre la inteligencia artificial* (actualizada en mayo de 2024). https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

Palacios, L. P. (2020). Derechos humanos e inteligencia artificial. En F. Álvarez Larrondo (Dir.), *Inteligencia artificial y derecho* (pp. 103–122). Hammurabi. https://biblioteca.hammurabidigital.com.ar/reader/inteligencia-artificial-y-derecho?location=8

Palisade Research [@PalisadeAI]. (2025, 24 de mayo). OpenAI's o3 model sabotaged a shutdown mechanism to prevent itself from being turned off… [Post]. X. https://x.com/PalisadeAI/status/1926084635903025621

Pan, X., Dai, J., Fan, Y., & Yang, M. (2024). *Frontier AI systems have surpassed the self-replicating red line*. Escuela de Ciencias de la Computación, Universidad de Fudan. https://www.arxiv.org/pdf/2412.12140

Parada, R. A., & Errecaborde, J. D. (Comps.). (2018). *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet*. Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Perfil. (2025, 15 de mayo). Hackean al Ejército Argentino y filtran información clasificada de 50 mil agentes. https://www.perfil.com/noticias/bravotv/hackeo-masivo-al-ejercito-filtraron-legajos-de-cincuenta-mil-agentes.phtml

PhishProtection. (s. f.). History of phishing. https://www.phishprotection.com/resources/history-of-phishing

Proyecto de ley, Código Penal de la Nación. (2024). Modificación del artículo 128 sobre difusión de actividades sexuales explícitas de menores de edad a través de cualquier mecanismo digital, Expte. N.º 4689-D-2024, Trámite Parlamentario N.º 125. Cámara de Diputados de la Nación Argentina. https://www.hcdn.gov.ar/diputados/msotolano/proyecto.html?exp=4689-D-2024

Rabelais, F. (2017). *Pantagruel* (A. Yllera, Trad.). Titivillus. (Obra original publicada en 1542). https://static1.squarespace.com/static/5d2dfea38c708800014f8c1a/t/5f0f8e37141cc81fc3d24418/1594854970571/Pantagruel+-+Francois+Rabelais.pdf

Rafecas, D. (2021). *Derecho penal sobre bases constitucionales*. Didot.

Real Academia Española. (2025). *Inputs, software, hardware, hackear, internet, algoritmo*. En *Diccionario de la lengua española* (23.ª ed.). https://dle.rae.es

Reglamento (UE) 2024/1689. (2024). *Reglamento de inteligencia artificial*. Diario Oficial de la Unión Europea, L 2024/1689, 12 de julio de 2024. http://data.europa.eu/eli/reg/2024/1689/oj

Riquert, M. (2024). ChatGPT y una aproximación a los discursos de odio. En G. Arocena (Dir.), *Ciberdelitos*. Hammurabi. https://biblioteca.hammurabidigital.com.ar/reader/ciberdelitos-1721917757?location=117

Samoili, S., López Cobo, M., Gómez, E., De Prato, G., Martínez-Plumed, F., & Delipetrey, B. (2020). *AI Watch – Defining artificial intelligence: Towards an operational definition and taxonomy of artificial intelligence*. Oficina de Publicaciones de la Unión Europea. https://data.europa.eu/doi/10.2760/382730

Sain, G. (2015, 11 de abril). Evolución histórica de los delitos informáticos. *Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/doctrina/40877-evolucion-historica-delitos-informaticos

Spartan-Cybersecurity. (s. f.). La historia del malware. https://books.spartan-cybersec.com/malware/introduccion-al-malware/la-historia-del-malware

Take It Down Act. (2025). *Pub. L. No. 119-12, 119th Cong.* https://www.congress.gov/bill/119th-congress/senate-bill/146/text

UNIR. (s. f.). ¿Qué es la deep web y cómo funciona? https://www.unir.net/revista/ingenieria/deep-web/

Zaffaroni, E. R., Alagia, A., & Slokar, A. (2006). *Manual de derecho penal. Parte general* (2.ª ed.). EDIAR.

Artículos

Revista Pensamiento Penal
Sección Derechos humanos y crímenes de lesa humanidad
Vol. 2, núm. 4 – 2025, págs. 72–84
ISSN: 1853 – 4554
DOI: doi.org/10.64178/nx753049

Reducción a la servidumbre a mujeres trans en dictadura: avance jurisprudencial en materia de lesa humanidad

Agustín Pelayo[1]

Resumen

El artículo busca analizar el reconocimiento judicial de la violencia específica contra las mujeres trans y de la reducción a la servidumbre como mecanismo represivo en el marco del terrorismo de Estado. Para ello, aborda los motivos por los cuales la reducción a la servidumbre es contemplada como un acto constitutivo de crímenes de lesa humanidad, así como su recepción jurisprudencial en el proceso de juzgamiento en Argentina. Examina las resoluciones de la causa «Brigadas», que evidencian la explotación laboral forzada y la violencia sexual ejercida contra mujeres trans, reconociendo la motivación discriminatoria basada en la identidad y expresión de género. Finalmente, pondera cómo la calificación legal de los hechos con perspectiva de género permitió reducir la impunidad, visibilizando por primera vez el carácter cis–heteronormativo del aparato represivo y su objetivo de disciplinar a las mujeres trans en tanto catalogables dentro de un concepto amplio de «subversión».

Sumario

Palabras clave

género – mujeres trans – reducción a la servidumbre – lesa humanidad – justicia transicional

[1] Abogado (Universidad Nacional de La Plata, UNLP). Maestrando en Derechos Humanos (UNLP). Docente de derecho internacional público e integrante del instituto de Derechos Humanos (UNLP). Empleado del Poder Judicial de la Nación. Correo electrónico: aguspelayo@gmail.com

1. Introducción

El 5 de julio de 2024, el tribunal oral en lo criminal federal N° 1 de La Plata (en adelante, «TOCF N° 1») hizo públicos los fundamentos de la sentencia dictada en el expediente FLP 737/2013/TO1 y acumuladas, popularmente conocida como causa de las «Brigadas». Se trata de un precedente más en el largo trabajo llevado adelante por la jurisdicción federal platense en miras a dilucidar los crímenes cometidos, en el marco del terrorismo de Estado, por el aparato represivo que fue denominado «Circuito Camps»[2], y determinar las correspondientes responsabilidades penales.

El objetivo de este trabajo es efectuar un análisis cualitativo, de carácter exploratorio, sobre dos particularidades de los pronunciamientos judiciales dictados en ese expediente que, según mi criterio, resultan novedosos y diferenciales respectos de otros antecedentes jurisprudenciales en materia de crímenes de lesa humanidad[3].

Primero, que el juzgamiento con perspectiva de género permitió visibilizar crímenes específicos contra travestis y mujeres trans[4] en razón de su identidad y expresión de género, circunstancia que ha tomado una repercusión notable en ámbitos periodísticos y del activismo LGBTTIQ+, pero no ha sido aun debidamente ponderada en la doctrina penal.

Asimismo, la particularidad del abordaje del delito de reducción a la servidumbre, que pocas veces ha sido contemplado como un acto constitutivo de crímenes de lesa humanidad en la jurisprudencia nacional.

En ese sentido, el ensayo se propone rescatar el modo en que intersectan ambos tópicos –identidad de género y reducción a la servidumbre– para dar cuenta del carácter novedoso de los fallos en estudio.

2. La reducción a la servidumbre como crimen de lesa humanidad

Una de las notas relevantes a analizar en el presente trabajo es de qué modo la conducta de reducción a la servidumbre puede constituir un acto consumativo de crímenes del derecho penal internacional.

---

[2] Circuito represivo denominado así por haber sido comandado directamente por la jefatura de la policía de la provincia de Buenos Aires, a cargo del general Ramón Camps. Véase Comisión Nacional sobre la Desaparición de Personas (2006) y la sentencia del Tribunal Oral en lo Criminal Federal N.º 1 de La Plata del 25 de marzo de 2013, en la causa N.º 2955/09 y acumuladas.

[3] El presente trabajo recoge algunos de los interrogantes desarrollados en mi ponencia «persecución a disidencias sexo–genéricas en el marco del terrorismo de estado: cambio de enfoque en la justicia federal», presentada el 1.º de noviembre de 2024 en la jornada coorganizada por el programa «*género y derecho*» de la facultad de derecho de la universidad de Buenos Aires y la organización «diversidad y justicia». Asimismo, fueron especialmente relevantes los contenidos del curso «delitos federales y complejos», ofrecido por la Asociación Pensamiento Penal. Agradezco de manera particular a Mayra Scaramutti y a María Florencia Brichetti por el impulso y los valiosos aportes brindados para mejorar este trabajo.

[4] Algunas de las víctimas cuyos casos integraron la causa judicial se autopercibían como travestis y otras como mujeres transgénero o mujeres transexuales. A los solos efectos de facilitar la lectura, se utilizará en general la expresión «mujeres trans».

Desde 1921, el código penal recepta la reducción a la servidumbre en el art. 140, siendo la figura típica que da inicio al título V, sobre «delitos contra la libertad», y al capítulo titulado «delitos contra la libertad individual».

Más allá de la profusa discusión doctrinaria sobre la conceptualización del bien jurídico «libertad», esta puede ser pensada como el derecho de la persona para autodeterminar su propio proyecto de vida, teniendo presente que las opciones que para ello se tengan «son la expresión y garantía de la libertad»[5].

El art. 140 (según la redacción original de la ley 11.179, que es la que interesa al presente ensayo) reprimía a quien «redujere a una persona a servidumbre o a otra condición análoga y el que la recibiere en tal condición para mantenerla en ella». Tal tipificación reglamenta la manda constitucional del art. 15, que declara la abolición de la esclavitud y la trata de personas[6].

En diciembre de 2012, mediante la sanción de la ley 26.842, el poder legislativo elevó el mínimo de la pena y modificó el tipo penal, criminalizando a quien redujere a alguien «a esclavitud o servidumbre, bajo cualquier modalidad». Vale recalcar que dicha reforma fue implementada en el marco de una nueva política criminal respecto al fenómeno de la trata de personas, en línea con los compromisos asumidos por Argentina a partir de la ratificación del Protocolo de Palermo, que incluyó –en los incisos a. y b. del artículo 2 de la ley– dos modalidades de explotación laboral que nos resultan de interés: la cometida por reducir o mantener a la víctima en condición de la esclavitud o servidumbre; o por imponerle la realización de trabajos o servicios forzados.

La diferenciación entre las dos modalidades citadas está dada, a fin de cuentas, porque la servidumbre «está asociada a la obtención de la fuerza de trabajo de la víctima a través de su sometimiento a una condición servil» de modo que implique «los sometimientos más absolutos del dominio de la personalidad»[7]. En esa tesitura, Espaliú recalca que la jurisprudencia del Tribunal Europeo de Derechos Humanos ha hecho foco en el sentimiento de la víctima reducción a la servidumbre de que «su condición es inamovible»[8].

Es que, independientemente de las disquisiciones existentes entre la forma de entender a las figuras de servidumbre y de esclavitud, ambas comparten que la víctima es reducida «a la condición de cosa, lo que implica que pueda ser vendida, comprada, cedida o que un tercero se sirva de ella sin reconocerle ningún derecho o prestación por su trabajo»[9].

Es la Corte Interamericana de Derechos Humanos quien puede, a través de sus estándares jurisprudenciales, proveernos de un entendimiento moderno de la servidumbre. Teniendo presente la prohibición del art. 6.1 del Pacto de San José de Costa Rica y la evolución del derecho internacional desde la celebración de la Convención sobre la Esclavitud, adoptada en Ginebra en 1926, dicho tribunal la conceptualizó como «el ejercicio de control sobre una persona mediante coacción física o psicológica de tal

[5] Corte Interamericana de Derechos Humanos (Corte IDH), *Caso Loayza Tamayo vs. Perú*, Sentencia del 27 de noviembre de 1998, párr. 148.
[6] Paz y Lowry (s. f.), p. 3.
[7] Castany y Tarantino (2011), pp. 178–179.
[8] Espaliú (2014), p. 30.
[9] Paz y Lowry (s. f.), p. 8.

manera que implique la pérdida de su autonomía individual y la explotación contra su voluntad», forma análoga a la esclavitud e igualmente vedada[10].

Ahora bien, esta asimilación entre esclavitud y servidumbre a los fines del reproche penal no resulta menor. Con respecto a la recepción de este tipo de figuras delictivas en el derecho penal internacional, vale observar que tanto el art. 6 del Estatuto para el Tribunal Militar Internacional de Nüremberg como el art. II. de la ley 10 del Consejo de Control Aliado estipulaban que la esclavitud era uno de los actos inhumanos configurativos de crímenes contra la humanidad[11]. En ese sentido, ese desarrollo primigenio de la posguerra ya reprochaba el contenido deletéreo de conductas de esa envergadura, aun cuando no receptaban expresamente el término servidumbre.

Instrumentos posteriores continúan esa misma línea: por ejemplo, el Estatuto de Roma y los Elementos del Crimen definen al crimen de lesa humanidad de esclavitud como aquel en que el autor «haya ejercido los atributos del derecho de propiedad sobre una o más personas [...] o les haya impuesto algún tipo similar de privación de libertad» (art. 7.1.c).

No obstante, esa concepción de esclavitud se ha ampliado a formas análogas de privación de la libertad que también resultan modalidades de comisión de crímenes internacionales, como lo ha entendido el Tribunal Internacional para la ex Yugoslavia en «Kunarac» (2001), teniendo presente la Convención suplementaria sobre la abolición de la esclavitud celebrada en 1956[12].

En síntesis, no caben dudas hoy que el derecho penal internacional reprime el sometimiento a condiciones análogas a la esclavitud, que no se perpetren en el marco de un régimen de propiedad jurídica sobre seres humanos pero que en la práctica compartan el resultado de explotación laboral y dominio total sobre la personalidad de la víctima, como es la figura fáctica de reducción a la servidumbre.

3. La reducción a la servidumbre y el terrorismo de Estado en Argentina

Llegados a este punto, es preciso preguntarnos qué recepción ha tenido el crimen de lesa humanidad de reducción a la servidumbre en el proceso de juzgamiento de los delitos cometidos en el marco del terrorismo de Estado en nuestro país.

En primer término, debo referirme a los hechos acaecidos en el célebre centro clandestino de detención y tortura que funcionara en la Escuela de Mecánica de la Armada (ESMA), respecto a los cuales se desarrollaron –hasta el momento– seis debates orales y públicos que derivaron en cinco sentencias condenatorias[13]. En los fundamentos de todos esos fallos se observan referencias de diferentes testigos–víctimas a las labores

[10] Corte Interamericana de Derechos Humanos (Corte IDH), *Caso Trabajadores de la Hacienda Brasil Verde vs. Brasil*, Sentencia del 20 de octubre de 2016, párr. 176.
[11] Medina y Vázquez (2011), pp. 107–124.
[12] Gil (2016), pp. 202–215.
[13] Se trata de las sentencias dictadas por el Tribunal Oral en lo Criminal Federal N.º 5 de la Ciudad Autónoma de Buenos Aires (en adelante, TOCF N.º 5 de CABA) en las causas «ESMA II» (28 de diciembre de 2011), «ESMA Unificada» (5 de marzo de 2018), «ESMA IV» (19 de abril de 2021), «ESMA Delitos Sexuales» (12 de octubre de 2021) y «ESMA Sandoval» (23 de febrero de 2023). En igual sentido, Comisión Nacional sobre la Desaparición de Personas (2006), pp. 135–136.

que se vieron obligados a hacer, tanto en el centro clandestino en sí como en otras dependencias conexas e incluso en inmuebles particulares, como parte de un supuesto «proceso de recuperación». Las tareas resultaban sumamente diversas e implicaron actividades manuales e intelectuales: labores de albañilería, carpintería, mecánica automotor, trabajos de fotografía, imprenta y falsificación de documentos vinculados a tareas de inteligencia llevadas adelante por sus captores, el montaje de una inmobiliaria para la venta de inmuebles usurpados a otras víctimas, la elaboración de trabajos y tesis para la Escuela Superior de Guerra, y hasta el desempeño de labores para la Cancillería en el ámbito de la sede ministerial, a la que eran trasladadas a diario algunas personas.

Ahora bien, de las sentencias surge que a ningún imputado se le endilgó la comisión del delito de reducción a la servidumbre, incluso cuando en la sentencia denominada «ESMA IV» se refirió expresamente, en la descripción de la materialidad ilícita relativa a los casos de treinta y ocho víctimas distintas, que mientras se encontraban detenidas fueron forzadas «a trabajar para sus captores sin recibir alguna retribución a cambio»[14].

Por su parte, en las investigaciones relativas al circuito represivo «ABO», integrado por los centros clandestinos de detención y tortura «El Atlético», «Banco» y «Olimpo», se reflejó desde un primer momento la situación de cautiverio de individuos que «estaban sometidos a servidumbre y obligados a hacer las tareas de mantenimiento del centro, la atención de los otros, y en algún caso [...] hasta instruir un sumario aprovechando su condición de abogado»[15].

Sin embargo, «el sometimiento a servidumbre» fue contemplado, junto a la deficiente alimentación, las lamentables condiciones de higiene, la exposición a desnudez y la deficiente atención médica, como parte de las «inhumanas condiciones de vida» que hacían que la permanencia en los centros clandestinos configure por sí sola el delito de imposición de tormentos. Aparece así subsumida la reducción a la servidumbre en otro tipo penal.

Frente a esos antecedentes, se destacan por su excepcionalidad las sentencias dictadas en 2012, por el juzgado nacional en lo criminal y correccional federal N° 4, en las causas «Contraofensiva II» y «Contraofensiva III». En ellas, se condenó como autor mediato a Antonio Herminio Simón, y como coautores directos a Alfredo Omar Feito, Jorge Oscar Baca y Carlos Eduardo Somoza, por los delitos de asociación ilícita, privación ilegal de la libertad, e imposición de apremios ilegales agravadas, y reducción a la servidumbre, todos en concurso real, en perjuicio de Silvia Noemí Tolchinsky, entre otros hechos. Tolchinsky, secuestrada entre septiembre de 1980 y el año 1982, fue obligada entre julio de 1981 y marzo de 1982 a observar a las personas que transitaban por el paso fronterizo de Paso de los Libres, Corrientes, así como a revisar sus pasaportes, colaborando con sus captores en la detección de personas presuntamente integrantes de organizaciones «subversivas».

En dichas resoluciones, el magistrado sostuvo escuetamente –con cita de Carlos Creus– «que corresponde adecuar el hecho en el artículo 140 del código penal, pues

[14] TOCF N.º 5 de CABA, Causa «*ESMA IV*», sentencia del 19 de abril de 2021. Véanse, v. gr., los casos n.º 36, 38 y 89 —correspondientes a Marta Remedios Álvarez, Alfredo Manuel Juan Buzzalino y Alberto Ahumada—, pp. 1084, 1107 y 1532.

[15] Tribunal Oral en lo Criminal Federal N.º 2 de la Ciudad Autónoma de Buenos Aires, Causa «*ABO – Tepedino*», sentencia del 22 de marzo de 2011, pp. 340 y 841. En igual sentido, pueden consultarse las sentencias del mismo tribunal en los juicios «*ABO bis*» (15 de junio de 2012, p. 425), «*ABO III*» (8 de marzo de 2018, pp. 909–910) y «*ABO V*» (8 de marzo de 2024, p. 1285).

doctrinariamente se ha reconocido que la servidumbre constituye un estado en el que el sujeto activo dispone de la persona del sujeto pasivo como si fuese su propiedad, reduciéndolo a la condición de cosa, sin otorgarle contraprestación alguna por los servicios que de él recibe, y sin otro condicionamiento que el ejercicio de su poder»[16].

Como corolario, vale subrayar que –con respecto a la subsunción legal de la materialidad ilícita de todos los casos reseñados–, resulta patente, son aplicables algunos de los indicios que la Organización Internacional del Trabajo ha establecido para la determinación del trabajo forzoso en la práctica: en concreto, que el trabajo es realizado por las víctimas con ausencia de consentimiento, al iniciarse partiendo de situaciones de secuestro y confinamiento en centros de detención clandestina; y adicionalmente, que dicho trabajo es sostenido en el tiempo por la presencia real o amenaza creíble de sufrir violencia física o sexual o de ser mantenido bajo encarcelamiento o confinamiento físico[17].

4. Las mujeres trans, en la mira de la dictadura

El 12 de abril de 2022, el titular del juzgado en lo criminal y correccional federal N° 3 de La Plata (en adelante, JCCF N° 3), Ernesto Kreplak, dictó un auto de procesamiento de catorce imputados en el marco de la causa FLP 737/2013, en la que se investigaban los hechos acaecidos en el centro clandestino «Pozo de Banfield»[18]. Dicho resolutorio puso de manifiesto –por primera vez en la historia de los juicios de lesa humanidad en la Argentina– la persecución específica que sufrieron ocho mujeres trans[19], al tiempo que se daba por acreditada la reducción a la servidumbre de tres de ellas: Julieta Alejandra González, Miguel Ángel Gómez y Judith Lagarde.

Si bien desde enero de 2011 obraba en el expediente la denuncia formulada por Valeria del Mar Ramírez, primera mujer trans constituida como parte querellante en una causa de lesa humanidad, lo cierto es que durante largos años los dictámenes fiscales y las resoluciones judiciales no hicieron foco en la identidad y expresión de género de la víctima.

Fue recién con el requerimiento formulado por la unidad fiscal federal de La Plata, en septiembre de 2020, y gracias al impulso de la Auxiliar Fiscal Ana Oberlin, que se promovió la investigación con una mirada global, abordando un mayor número de mujeres trans alcanzadas por el aparato represivo dictatorial e interpretando sus casos

[16] Juzgado Nacional en lo Criminal y Correccional Federal N.º 4, Causa «*Contraofensiva II*», sentencia del 31 de mayo de 2012, p. 243; y causa «*Contraofensiva III*», sentencia del 21 de septiembre de 2012, p. 224.
[17] Organización Internacional del Trabajo (OIT, 2005), p. 6.
[18] Como ha quedado acreditado judicialmente, el centro clandestino de detención y tortura conocido como «Pozo de Banfield» funcionó en la intersección de las calles Siciliano y Vernet, en el partido bonaerense de Lomas de Zamora, al menos entre octubre de 1974 y 1978, en una dependencia policial de especial relevancia por ser el asiento de la «Zona Metropolitana» de las Direcciones Generales de Seguridad, de Investigación y de Inteligencia de la Policía de la Provincia de Buenos Aires. Allí permanecieron en cautiverio y fueron torturadas más de 400 personas, al menos 34 de ellas de nacionalidad uruguaya, convirtiéndose en un epicentro de la ejecución del «Plan Cóndor». También funcionó una maternidad clandestina en la que al menos treinta mujeres embarazadas dieron a luz. Más de cuarenta personas resultaron imputadas en la causa FLP 737/2013 por los crímenes allí cometidos.
[19] Para profundizar en la historia de las víctimas desde una perspectiva de memorialización, véanse Lewin y Wornat (2020) y Máximo (2023).

sistemáticamente. Así, se pasó del silenciamiento o solapamiento a la visibilización de las violencias específicas motivadas en la identidad o expresión de género de las víctimas[20].

Esa sistematicidad fue posible en la medida en que se constataron diversos puntos de conexión entre los casos: algunos previos a sus secuestros, como situaciones de expulsión familiar, de migración interna forzada, de falta de acceso al mercado formal de trabajo, de ejercicio del trabajo sexual, y de frecuente criminalización mediante aplicación de normas contravencionales; otros posteriores, como el exilio o la represión de la expresión de género.

No obstante, dar ese paso entrañaba –en primer término– la dificultad de anudar las violencias concretas sufridas por las ocho mujeres trans con el plan sistemático de represión desplegado por el Estado, a sabiendas de que las problemáticas de diversidad sexo–genérica han sido esquivadas sobradamente por el desarrollo del derecho penal internacional, como resulta claro en las conceptualizaciones esencialistas o biologicistas que sobre el concepto de «género» estipula el Estatuto de Roma de la Corte Penal Internacional (art. 7.3)[21].

En ese sentido, al evaluar el modo en que se construye la calificación legal en el auto de procesamiento, Jazmín Auat toma los tres niveles de análisis sentados por la Corte Penal Internacional en el caso «Katanga» (2013) para determinar qué actos particulares se enmarcan en crímenes de lesa humanidad. Los primeros dos niveles (el elemento de contexto –esto es, que el acto se cometa en el marco de un ataque a la población civil y vinculado a la política de ataque– y la caracterización del ataque como generalizado o sistemático) resultan acreditados con mayor facilidad[22].

Pero la autora recalca que, en el caso, la clave para considerar la persecución sufrida contra el colectivo trans radica en el tercer nivel de análisis: la determinación del nexo entre el acto particular y el contexto general, así como del conocimiento sobre ese nexo. El «test de peligrosidad» necesario para acreditarlo demanda que las persecuciones a las personas trans se hayan visto favorecidas o facilitadas por haberse enmarcado en el ataque, en la medida en que «no hay autoridad dispuesta a evitarlas y sancionarlas»; al contrario, cometidas las conductas al amparo del poder que sostiene la política de ataque, se vea garantizada la impunidad de sus autores.

Es que, al decir de Oberlin, en el periodo se utilizó sobre las mujeres trans «los dispositivos claves que estructuraron el terrorismo de estado»: los centros clandestinos de detención y la desaparición forzada de personas[23].

---

[20] ánchez Moreno (2021, p. 19) va más allá al considerar que las víctimas LGBTTIQ+, como sujetos abyectos relegados por las identidades hegemónicas, han sufrido no sólo negación sino forclusión. Esto implica que el sujeto es negado, expulsado o excluido y que, posteriormente, dicha exclusión es desmentida u ocultada, quedando invisibilizada u obliterada. En términos psicoanalíticos, ello supone «el rechazo simbólico de un sujeto y un significante, que no aparece inscrito en el inconsciente». Así, el autor afirma que «la forclusión opera desde la memoria, destacando unas [identidades] y forcluyendo —excluyendo, obviando, negando y ocultando— otras».

[21] Aun así, no debe perderse de vista que la persecución de grupos y colectividades con identidad propia —conforme la tipifica el art. 7.1.h del Estatuto de Roma como acto constitutivo de crímenes de lesa humanidad— refleja también «otros motivos universalmente reconocidos como inaceptables con arreglo al derecho internacional». Aquí se abre una puerta hacia el Derecho Internacional de los Derechos Humanos, ya que, a criterio del autor, no caben dudas de que en las últimas décadas se ha consolidado el reconocimiento universal de la orientación sexual y de la identidad y expresión de género como categorías protegidas por la normativa internacional. En ese sentido, véase Álvarez (2025).

[22] Auat (2022), pp. 40–4.

[23] Oberlin (2020), pp. 102–119.

Asimismo, una segunda dificultad radicaba en el carácter discriminatorio de las violencias sufridas, es decir, en comprender en qué medida la identidad y expresión de género de las víctimas gravitó como un móvil determinante para el accionar represivo concreto de los perpetradores.

En ese sentido, como lo señala Álvarez, tanto la jurisprudencia del Tribunal Europeo de Derechos Humanos como de la Corte Interamericana de Derechos Humanos establecen un doble criterio para la corroboración de las hipótesis de crimen de odio en los casos de violencias contra personas LGBTTIQ+: por un lado, acreditar un contexto de violencia general contra el colectivo, que puede estar profundizado por circunstancias particulares; por otra parte, «analizar el hecho en concreto mediante indicios e inferencias epistémicas». Si bien «ambos tribunales acuerdan la dificultad de probar el odio como motivación particular de los hechos de violencia», tal obstáculo puede superarse si los Estados cumplen con su obligación de investigar analizando integralmente la prueba «desde una perspectiva amplia a partir de la cual todo elemento de contexto, aun aquellos de carácter periférico, puede resultar útil para dilucidar las motivaciones que guiaron al autor de los hechos»[24].

Considerando dichos obstáculos, el auto de procesamiento contempla la jurisprudencia interamericana y algunos pronunciamientos del Comité de Derechos Humanos de las Naciones Unidas para dar por acreditado el cuadro de discriminación y violencia históricas y estructurales contra el colectivo LGBTTIQ+[25], que se vio «ahondada por las acciones desplegadas durante el terrorismo de Estado». Agrega, en línea con lo señalado por el experto independiente de Naciones Unidas en la materia, Víctor Madrigal–Borloz, la especial vulnerabilidad de las personas trans y el carácter simbólico de la violencia para comunicar un mensaje de exclusión y subordinación al colectivo que integran las víctimas[26].

Así, ponderó testimonios de contexto y las declaraciones de las víctimas para evidenciar un recrudecimiento del hostigamiento y de la represión en el periodo, afirmando que el terrorismo de Estado buscó «garantizar la hegemonía de un modelo sexo–genérico en el cual los roles de mujeres (cis) y varones (cis) estaban asignados, respectivamente, a los ámbitos doméstico y público, en una cultura netamente patriarcal», por lo que «toda transgresión a la cis/heteronormatividad resultaba objeto de criminalización y disciplinamiento, calificable como «amoral» y contraria a los cánones de la sociedad «occidental y cristiana» que imbuía el ideario» del régimen[27].

Tales testimonios de contexto resultaron fundamentales, en tanto permitieron comprender la afectación desproporcionada a las personas trans, quienes siendo «vistosas al resto, rompen el binomio y la heteronorma», por lo que para ellas «no hay clóset»[28]. Esta situación de vulnerabilidad resulta diametralmente diferente a la padecida por lesbianas y gays, que si bien también eran categorizadas como «amorales o malvivientes»

[24] Álvarez (2025), pp. 486–503.

[25] Corte Interamericana de Derechos Humanos (Corte IDH), *Caso Vicky Hernández vs. Honduras*, sentencia del 26 de marzo de 2021; y Observaciones Finales del Comité de Derechos Humanos de Naciones Unidas relativas a República Dominicana (CCPR/C/DOM/CO/6), El Salvador (CCPR/C/SLV/CO/7), Guatemala (CCPR/C/GTM/CO/4) y Paraguay (CCPR/C/PRY/CO/4)

[26] «La víctima es elegida con el propósito de comunicar un mensaje de exclusión y subordinación». Corte IDH, *Caso Vicky Hernández vs. Honduras*, sentencia del 26 de marzo de 2021, párr. 69–70.

[27] Las comillas pertenecen al original. Véase Juzgado en lo Criminal y Correccional Federal N.º 3 de La Plata (JCCF N.º 3), *Causa «Pozo de Banfield»*, auto del 12 de abril de 2022, pp. 37 y 39.

[28] JCCF N.º 3 de La Plata, *Causa «Pozo de Banfield»*, auto del 12 de abril de 2022, p. 36, declaración testimonial de Cristian Prieto Carrasco.

por las fuerzas de seguridad[29], sufriendo la trama de persecución y exilio que venimos desarrollando, sí «tenían la posibilidad de diluirse en el seno social» como estrategia de supervivencia[30].

La misma línea sostuvo el TOCF Nº 1 de La Plata en su sentencia de julio de 2024, adicionando el argumento de que no obsta a la calificación de lesa humanidad la presunta detención de muchas de las mujeres trans «en orden a disposiciones contravencionales» si se efectuó en aprovechamiento de su situación de vulnerabilidad y exclusión, conduciéndolas a un cautiverio clandestino y sin dar curso al procedimiento legal[31].

Resulta novedosa, en síntesis, la identificación de casos de persecución de disidencias sexo–genéricas, en tanto sus identidades, expresiones y prácticas eran catalogables dentro del concepto amplio y flexible de «subversión» delineado por las autoridades del régimen dictatorial como enemigo y objeto de represión y disciplinamiento.

5. Someter los cuerpos para reprimir la identidad

Para finalizar, merecen una mención particular dos aspectos resaltados tanto en la resolución de primera instancia como en la sentencia. Sabido es que el aparato represivo desplegado por el régimen militar se ensañó particularmente con los cuerpos de las víctimas, como evidencia la práctica sistemática de tortura y violencia sexual implementada en los centros clandestinos de detención.

Por un lado, las tres víctimas nombradas, así como las otras cinco mujeres trans (Paola Alagastino, Carla Gutiérrez, Analía Velázquez, Marcela Viegas Pedro y Valeria del Mar Ramírez) fueron detenidas mientras ejercían el trabajo sexual, en la vía pública, en distintos lugares del Conurbano Bonaerense.

Ello da cuenta de una situación de segregación social que afectaba sus trayectorias existenciales: la expulsión por parte de sus familias, la migración interna, y la imposibilidad de acceder al trabajo formal. Resulta notable, entonces, que detenidas en razón de encontrarse realizando una actividad por cuenta propia para garantizarse el sustento –aunque criminalizada por la normativa contravencional–, su cautiverio en el circuito clandestino de represión haya posibilitado a sus perpetradores su explotación laboral, es decir, la apropiación coactiva de su fuerza de trabajo.

En el auto de procesamiento reseñado, el magistrado Ernesto Kreplak consideró que

> los imputados dispusieron de las víctimas para realizar variados trabajos y servicios no retribuidos, tales como cocinar, limpiar la dependencia policial y lavar automóviles utilizados en operativos represivos, o picar cascotes en la obra de construcción edilicia [...] contra la voluntad de los sujetos pasivos, sin contraprestación y sin posibilidad alguna de éstos de hacer cesar tal estado de sujeción [...] en aprovechamiento de su situación de cautiverio clandestino[32].

[29] CCF N.º 3 de La Plata, *Causa «Pozo de Banfield»*, auto del 12 de abril de 2022, p. 36, declaración testimonial de Ana Solari Paz.
[30] Juzgado en lo Criminal y Correccional Federal N.º 3 de La Plata (JCCF N.º 3), *Causa «Pozo de Banfield»*, auto del 12 de abril de 2022, pp. 36–37, declaración testimonial de Flavio Rapisard.
[31] Tribunal Oral en lo Criminal Federal N.º 1 de La Plata (TOCF N.º 1), *Causa «Brigadas»*, sentencia del 5 de julio de 2024, p. 220.
[32] JCCF N.º 3 de La Plata, *Causa «Pozo de Banfield»*, auto del 12 de abril de 2022, p. 256.

Ahora bien, en el caso, la reducción a la servidumbre fue visibilizada como un delito autónomo, en concurso real con los de privación ilegal de la libertad, aplicación de tormentos y violación.

También el TOCF 1 de La Plata consideró que el delito –según el tipo penal vigente al momento de los hechos– concurrió en forma real con el resto de los crímenes endilgados a los imputados. Tuvo presente los testimonios de las víctimas, en cuanto refieren a las labores impuestas forzosamente, así como la prohibición de circular por determinadas áreas del centro clandestino de detención y hablar con las personas que allí se encontraban, quedando recluidas en un sector delimitado. A ello se adiciona la violencia sexual y las amenazas e insultos proferidos, caracterizados por su contenido degradante hacia su orientación sexual y su identidad y expresión de género. Se deduce de la resolución que dichos improperios fueron interpretados como indicios suficientes de la motivación transodiante de las acciones delictivas.

En particular, resulta destacable que el Tribunal, para sostener ese encuadramiento legal de la materialidad ilícita, hace uso del precedente jurisprudencial de la Cámara Federal de Casación Penal, en el expediente «Simón, Antonio H. y otros s/ condena», en el cual se confirma la sentencia dictada en la causa «Contraofensiva», referida anteriormente, que abordó la figura típica en estudio[33].

El segundo aspecto a subrayar es que el objetivo disciplinante y moralizante de la represión surtió efectos duraderos, conforme lo refirieron las mismas víctimas, en el devenir de su proyecto de vida. Por caso, tres de ellas –Gutiérrez, Velázquez y Alagastino– se exiliaron en los años ochenta para poder expresar libremente su género, obteniendo la última de ellas estatuto de refugiada. Pero el ejemplo más ilustrativo de dicho impacto es el de Gómez, quien expresó haber auto–censurado su identidad y expresión trans al salir del centro clandestino de detención, retornando definitivamente a su *deadname* para prevenir nuevas violencias policiales: «la solución fue volver a ser Miguel Ángel»[34]. Valga la redundancia, su liberación del centro clandestino resultó tanto en la recuperación de su libertad ambulatoria como en el encorsetamiento definitivo de su expresión disidente del género.

Como corolario, es posible pensar que estos precedentes judiciales dan cuenta de ciertos intentos de vencer la «incapacidad para nombrar determinados sujetos y determinadas violencias que se consideran prescindibles en la democracia» que, siguiendo a Nancy Fraser, Sánchez Moreno atribuye a las instituciones judiciales y políticas del Estado[35]. Solo así los cuerpos de las mujeres trans victimizadas serán «cuerpos que importan» y sus historias de vida dejarán de ser un segmento obliterado de la memoria colectiva.

[33] Tribunal Oral en lo Criminal Federal N.º 1 de La Plata (TOCF N.º 1), *Causa «Brigadas»*, sentencia del 5 de julio de 2024, pp. 2242–2243.
[34] Juzgado en lo Criminal y Correccional Federal N.º 3 de La Plata (JCCF N.º 3), *Causa «Pozo de Banfield»*, auto del 12 de abril de 2022, p. 60.
[35] Sánchez Moreno (2021), p. 18.

6. Conclusiones

La aplicación de perspectiva de género, conforme el mandato de la Convención de Belém do Pará y los estándares internacionales, además de ser un imperativo jurídico ineludible, permite a los operadores y operadoras judiciales evitar la impunidad devenida de aquello que Pacilio señala respecto a la tortura: las prácticas judiciales arraigadas que provocan ausencia de reproche por «minimización de la gravedad del fenómeno»[36].

Ello es consecuente con el postulado Nº 37 de los Principios de Yogyakarta+10, de 2017, sobre la aplicación del derecho internacional de los derechos humanos a las disidencias sexo–genéricas, que postula el derecho a la verdad en cabeza de las víctimas, las comunidades y a la sociedad en general, frente a violaciones sistemáticas de los derechos humanos motivadas en la orientación sexual y la identidad y expresión de género.

Si bien existe cierto nivel de reconocimiento en el ámbito político, social y cultural, desde que –con fundamento en las conversaciones entre Carlos Jáuregui y el Rabino Marshall Meyer– se impulsó la cifra simbólica de «30.400» víctimas de la última dictadura, la determinación de la verdad por parte del Estado y la consecuente asunción de responsabilidad tienen, a mi entender, una dimensión reparadora insustituible.

Pues bien, develar la especificidad de la persecución contra disidencias sexo–genéricas en el marco del terrorismo de Estado y la gravedad inherente a la reducción a la servidumbre como práctica represiva singular en los centros clandestinos de detención parecieran ser algunas de las cuentas pendientes del proceso de juzgamiento de crímenes de lesa humanidad en la Argentina.

El caso platense, en ese sentido, posibilita aminorar el impacto de la impunidad en la vida de las personas supervivientes y ponderar debidamente la envergadura del plan sistemático represivo desplegado por las fuerzas armadas y de seguridad en el periodo más oscuro de nuestra historia.

7. Referencias bibliográficas

Álvarez, J. T. (2025). *La orientación sexual y la identidad de género en el derecho internacional de los derechos humanos. Diálogos entre la Corte IDH y el TEDH*. Editores del Sur.

Auat, J. (2022). Reflexiones en torno a los delitos sexuales cometidos en el marco del terrorismo de Estado. En J. T. Álvarez & S. A. Alonso (Dirs.), *Géneros e interseccionalidad. Un análisis crítico de la parte especial del derecho penal* (Tomo 1, pp. 29–54). Editores del Sur.

Castany, M. L., & Tarantino, M. (2011). *Donde el sol no brilla. La finalidad de explotación laboral en el delito de trata de personas*. En D. Pastor (Dir.), *Problemas actuales de la parte especial del derecho penal* (pp. 169–200). Ad–Hoc.

Comisión Nacional sobre la Desaparición de Personas. (2006). *Nunca más*. Eudeba.

[36] Pacilio (2022), p. 181.

Comité de Derechos Humanos de Naciones Unidas. (2017). *Observaciones finales sobre el sexto informe periódico de la República Dominicana* (CCPR/C/DOM/CO/6), 27 de noviembre

Comité de Derechos Humanos de Naciones Unidas. (2018a). *Observaciones finales sobre el séptimo informe periódico de El Salvador* (CCPR/C/SLV/CO/7), 9 de mayo.

Comité de Derechos Humanos de Naciones Unidas. (2018b). *Observaciones finales sobre el cuarto informe periódico de Guatemala* (CCPR/C/GTM/CO/4), 7 de mayo.

Comité de Derechos Humanos de Naciones Unidas. (2019). *Observaciones finales sobre el cuarto informe periódico del Paraguay* (CCPR/C/PRY/CO/4), 20 de agosto

Espaliú, C. (2014). La definición de esclavitud en el Derecho internacional a comienzos del siglo XXI. *Revista Electrónica de Estudios Internacionales*, 28, 1–36.

Gil, A. (2016). Crímenes contra la humanidad. *Eunomía. Revista en Cultura de la Legalidad*, (10), 202–215.

Lewin, M., & Wornat, O. (2020). *Putas y guerrilleras*. Planeta.

Máximo, M. (2023). *El Nunca Más de las locas: Resistencia y deseo en la última dictadura*. Marea.

Medina, M. E., & Vázquez, C. A. (2011). Los crímenes de lesa humanidad y su juzgamiento. *Lex: Revista de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas*, 9(8), 107–124.

Oberlin, A. (2020). La memoria no se guarda en el closet. Violencias invisibilizadas del terrorismo de Estado en Argentina. *Clepsidra. Revista Interdisciplinaria de Estudios sobre Memoria*, 7(14), 102–119.

Organización Internacional del Trabajo. (2005). *Una alianza global contra el trabajo forzoso*. OIT.

Pacilio, S. (2022). Notas sobre la impunidad en los casos judiciales de torturas en Argentina. *Revista Nueva Crítica Penal*, 3(6), julio–diciembre 2021.

Paz, M., & Lowry, S. (s. f.). Reducción a la servidumbre. En G. Vitale (Dir.), *Código Penal comentado de acceso libre*. Asociación Pensamiento Penal. https://www.pensamientopenal.com.ar/cpcomentado

Sánchez Moreno, M. (2021). Cuerpos diversos y memorias mutiladas: el enfoque de género en los procesos de Justicia Transicional en España y Argentina. *Encuentros Uruguayos*, 12(1), 5–22.

Jurisprudencia

Corte Interamericana de Derechos Humanos. (1998). *Caso Loayza Tamayo vs. Perú* (Sentencia de reparaciones y costas), 27 de noviembre (Serie C, Núm. 42).

Corte Interamericana de Derechos Humanos. (2016). *Caso Trabajadores de la Hacienda Brasil Verde vs. Brasil* (Sentencia de excepciones preliminares, fondo, reparaciones y costas), 20 de octubre (Serie C, Núm. 318).

Corte Interamericana de Derechos Humanos. (2021). *Caso Vicky Hernández vs. Honduras* (Sentencia de fondo, reparaciones y costas), 26 de marzo (Serie C, Núm. 422).

Juzgado en lo Criminal y Correccional Federal N.º 3 de La Plata. (2022). *Causa «Pozo de Banfield»* (Auto de procesamiento del 12 de abril, Expte. FLP 737/2013).

Juzgado Nacional en lo Criminal y Correccional Federal N.º 4. (2012a). *Causa «Contraofensiva II»* (Sentencia del 31 de mayo, Expte. 8905/07).

Juzgado Nacional en lo Criminal y Correccional Federal N.º 4. (2012b). *Causa «Contraofensiva III»* (Sentencia del 21 de septiembre, Expte. 293/12).

Tribunal Oral en lo Criminal Federal N.º 1 de La Plata. (2013). *Causa «Circuito Camps»* (Sentencia del 25 de marzo, Expte. 2955/09 y acumuladas).

Tribunal Oral en lo Criminal Federal N.º 1 de La Plata. (2024). *Causa «Brigadas»* (Sentencia del 5 de julio, Expte. FLP 737/2013/TO1 y acumuladas).

Tribunal Oral en lo Criminal Federal N.º 2 de la CABA. (2011). *Causa «ABO – Tepedino»* (Sentencia 1580 del 22 de marzo, Expte. 1668 y 1673).

Tribunal Oral en lo Criminal Federal N.º 2 de la CABA. (2012a). *Causa «ABO bis»* (Sentencia del 15 de junio, Expte. 1824 y acumuladas).

Tribunal Oral en lo Criminal Federal N.º 2 de la CABA. (2018). *Causa «ABO III»* (Sentencia del 8 de marzo, Expte. CFP 14216/2003/TO4).

Tribunal Oral en lo Criminal Federal N.º 2 de la CABA. (2024). *Causa «ABO V»* (Sentencia del 8 de marzo, Expte. CFP 14216/2003/TO13).

Tribunal Oral en lo Criminal Federal N.º 5 de la CABA. (2011). *Causa «ESMA II»* (Sentencia del 28 de diciembre, Expte. 1270 y acumuladas).

Tribunal Oral en lo Criminal Federal N.º 5 de la CABA. (2018). *Causa «ESMA Unificada»* (Sentencia del 5 de marzo, Expte. 1282 y acumuladas).

Tribunal Oral en lo Criminal Federal N.º 5 de la CABA. (2021a). *Causa «ESMA IV»* (Sentencia del 19 de abril, Expte. CFP 14217/2003/TO2).

Tribunal Oral en lo Criminal Federal N.º 5 de la CABA. (2021b). *Causa «ESMA Delitos Sexuales»* (Sentencia del 12 de octubre, Expte. CFP 10828/2011/TO2/CFC7).

Tribunal Oral en lo Criminal Federal N.º 5 de la CABA. (2023). *Causa «ESMA Sandoval»* (Sentencia del 23 de febrero, Expte. CFP 14217/2003/TO8)

Artículos

Revista Pensamiento Penal
Sección Derecho penal
Vol. 2, núm. 4 – 2025, págs. 85–124
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/p7xqrm42

Análisis del impacto de las criptomonedas en el lavado de activos: desafíos y perspectivas en el contexto actual

Sebastián Jáuregui[1]

Resumen

Desde la aparición de bitcoin en 2009, las criptomonedas y la tecnología blockchain han revolucionado el panorama financiero y tecnológico. Si bien ofrecen beneficios como transacciones rápidas y menores comisiones, su naturaleza descentralizada y el anonimato que pueden proporcionar plantean serios desafíos en la lucha contra el lavado de activos. Las criptomonedas, al carecer de una autoridad central y permitir movimientos transfronterizos con gran facilidad, se han convertido en una herramienta atractiva para delincuentes que buscan ocultar el origen ilícito de fondos. Las etapas tradicionales del lavado de activos (colocación, ocultación y reintroducción) se adaptan a su uso, facilitando la fase de ocultación con mayor velocidad y anonimato, lo que complica enormemente las investigaciones. Organismos internacionales como el GAFI y entidades locales como la UIF han advertido sobre estos riesgos, señalando la dificultad de rastrear e incautar bienes en un sistema descentralizado. Este escenario subraya la urgente necesidad de analizar el impacto de las criptomonedas en el lavado de activos, identificar las técnicas empleadas y desarrollar estrategias regulatorias y de combate efectivas. La investigación se propone abordar estos desafíos, buscando comprender cómo se utilizan las criptomonedas para fines delictivos y proponer recomendaciones para mitigar este riesgo creciente.

Sumario

Palabras clave

criptomonedas – lavado de activos – tecnología blockchain – criptoactivos – compliance

[1] Abogado (Universidad Católica de La Plata). Especialista en Cibercrimen (Universidad Siglo 21). Instructor judicial en la U.F.I. No. 2 Departamento Judicial de Mercedes, provincia de Buenos Aires. Correo electrónico: sjaureguiabogado@gmail.com

1. Análisis del tipo penal en la ley 22.421 y relación con el código penal

Las criptomonedas, como bitcoin, ethereum y otras altcoins, son monedas digitales que utilizan criptografía para asegurar las transacciones y controlar la creación de nuevas unidades. Estas monedas operan en un entorno virtual y no están respaldadas por ningún gobierno o entidad central, lo que las hace atractivas para aquellos que buscan el anonimato en sus transacciones financieras.

En búsqueda de una definición conceptual de criptomoneda, encontramos la propuesta por el *grupo de acción financiera internacional* (en adelante, «GAFI»), que las describe como «la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción» (GAFI, 2015: 32).

Por su parte, Lansky (2018), las define como un medio digital de intercambio que utiliza la criptografía para asegurar las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos.

Precisamente, una de las características inherentes a las criptomonedas es la capacidad de realizar transacciones de forma pseudónima o incluso anónima. Aunque las transacciones se registran en una cadena de bloques pública, las identidades de los participantes no están directamente vinculadas a las direcciones de criptomonedas utilizadas. Esto dificulta el rastreo de las transacciones y la identificación de los involucrados en actividades delictivas.

En este sentido, Valdés Trapote (2022: 10) explica que:

> los criptoactivos alcanzan (…) riesgos potenciales en el lavado de activos (...) las criptomonedas normalmente se basan en complejas infraestructuras que incluyen numerosas entidades o servidores, a menudo distribuidas por varios países, tanto para transferir fondos como para ejecutar pagos. Esta segmentación de servicios hace que el cumplimiento de la normativa contra el lavado de activos, así como su supervisión y ejecución no quede del todo clara. Además, registros de clientes y de transacciones pueden quedar en diferentes entidades, a menudo en diferentes jurisdicciones, haciendo mucho más difícil a investigadores y reguladores acceder a esos registros. Este problema queda exacerbado por la rápida naturaleza descentralizada de la tecnología de los activos virtuales, los cuales pueden ser instalados en jurisdicciones que no tengan adecuados controles contra el lavado de activos.

Por otro lado, sabido es que en el proceso de lavado de activos se reconocen generalmente tres etapas: colocación, estratificación e integración. La colocación implica introducir los fondos ilegales en el sistema financiero, la estratificación consiste en realizar múltiples transacciones para ocultar el origen de los fondos, y la integración busca incorporar los fondos ya lavados en la economía legítima.

El GAFI proporciona la siguiente definición sobre el delito apuntado:

> a) La conversión o transferencia de propiedad, a sabiendas de que deriva de un delito criminal, con el propósito de esconder o disfrazar su procedencia ilegal o el ayudar a cualquier persona involucrada en la comisión del delito a evadir las consecuencias legales de su accionar; b) la ocultación o disfraz de la naturaleza real, fuente, ubicación, disposición, movimiento, derechos con respecto a, o propiedad de, bienes

> a sabiendas de que derivan de ofensa criminal; c) la adquisición, posesión o uso de bienes, con el conocimiento al momento de su recibo, que deriva de una ofensa criminal o de la participación en algún delito.

Por su parte, Gómez Iniesta (1996: 86) define el blanqueo de capitales como «aquella operación a través de la cual el dinero de origen siempre ilícito es invertido, ocultado, sustituido o transformado y restituido a los circuitos económicos-financieros legales, incorporándose a cualquier tipo de negocio como si se hubiera obtenido de forma lícita».

Las criptomonedas pueden facilitar estas etapas al permitir la transferencia rápida y anónima de fondos a través de diferentes cuentas y plataformas. En directa vinculación con lo anterior, Valdés Trapote (2022: 5) señala que:

> Tomando como base las tradicionales fases que se dan en el delito de lavado de activos (colocación, ocultación y reintroducción), se adaptan sus fases a su realización mediante criptoactivos. Una de las peculiaridades de la etapa de ocultación es que la misma se ejecuta con mayor facilidad, velocidad y anonimato, lo que dificulta mucho la investigación y, por tanto, seguir el rastro del dinero.

También Donna (2021: 207) comulga con esta idea, al expresar:

> los activos ilegalmente obtenidos pueden cambiarse a monedas virtuales en casas de cambio, transferirlas luego a una red de cuentas ubicadas en el extranjero mediante la red Thor usando al mismo tiempo servicios de mezclado, para finalmente cambiarlas a moneda de curso legal en otra casa de cambio o bien adquirir con ellas bienes y servicios a través de internet. En este proceso, el anonimato en las transacciones y la posibilidad de efectuarlas de manera transfronteriza son aspectos propicios para disimular el rastro documentado, la fuente y la propiedad de los recursos. En efecto, los activos ilegalmente obtenidos pueden cambiarse a monedas virtuales en casas de cambio, transferirlas luego a una red de cuentas ubicadas en el extranjero mediante la red Thor usando al mismo tiempo servicios de mezclado, para finalmente cambiarlas a moneda de curso legal en otra casa de cambio o bien adquirir con ellas bienes y servicios a través de internet. En este proceso, el anonimato en las transacciones y la posibilidad de efectuarlas de manera transfronteriza son aspectos propicios para disimular el rastro documentado, la fuente y la propiedad de los recursos.

Lo expuesto da cuenta que el uso de criptomonedas en el lavado de activos plantea riesgos significativos. La naturaleza global de las criptomonedas y su capacidad para realizar transacciones transfronterizas sin intermediarios dificultan la supervisión y el seguimiento por parte de las autoridades. Además, los delincuentes pueden aprovechar las brechas en la regulación y el cumplimiento para utilizar intercambios de criptomonedas sin controles adecuados, lo que facilita el lavado de activos.

Aunque la relación entre criptomonedas y lavado de activos es una preocupación creciente, los esfuerzos regulatorios y de cumplimiento también han aumentado. Muchos países han implementado regulaciones y requisitos de debida diligencia para los proveedores de servicios relacionados con criptomonedas, como los intercambios. Además, se han propuesto iniciativas y medidas internacionales para fortalecer la supervisión y la cooperación entre jurisdicciones.

a. Origen y desarrollo del concepto de criptomoneda, en especial bitcoin

Las raíces del concepto de criptomoneda podemos encontrarla en trabajos académicos de la década de 1980 sobre criptografía y la teoría de la computación distribuida. Autores como David Chaum, en su trabajo *blind signatures for untraceable payments* (1982), y Wei Dai, quien propuso el concepto de *b-money* en 1998, sentaron las bases teóricas para las monedas digitales descentralizadas. Chaum exploró la posibilidad de utilizar la criptografía para garantizar el anonimato en las transacciones financieras, mientras que Dai sugirió un sistema de dinero electrónico descentralizado.

Sin embargo, no fue sino hasta la creación del bitcoin -atribuida a un sujeto o grupo de personas bajo el seudónimo de Satoshi Nakamoto, en noviembre del año 2008- que se produjo un avance revolucionario en la materia. En efecto, el documento publicado por Nakamoto, titulado *bitcoin: a peer-to-peer electronic cash system*, propuso la creación de un sistema de efectivo electrónico completamente descentralizado basado en una red peer-to-peer y tecnología de blockchain.

El surgimiento de las criptomonedas puede considerarse como una respuesta indirecta a la crisis financiera de Estados Unidos que tuvo su punto álgido en 2008. Aunque el desarrollo de las criptomonedas, en particular del bitcoin, no puede atribuirse directamente a esta crisis, es importante considerar el contexto económico y social en el que surgieron.

La crisis financiera de 2008 fue desencadenada por una combinación de factores, incluyendo la burbuja inmobiliaria, la proliferación de productos financieros complejos y riesgosos, y la falta de regulación adecuada en el sector financiero. Como consecuencia, hubo una pérdida masiva de confianza en las instituciones financieras tradicionales y en el sistema monetario convencional.

En este contexto de desconfianza hacia las instituciones financieras y gobiernos, surgió un mayor interés en alternativas descentralizadas y autónomas. El documento técnico publicado por Satoshi Nakamoto en 2008, justo después del estallido de la crisis financiera, es indicativo de este clima de descontento y búsqueda de soluciones alternativas.

El bitcoin se presentó entonces como una moneda digital descentralizada que operaba fuera del control de entidades gubernamentales y bancarias. Al utilizar tecnología blockchain y criptografía, el Bitcoin ofrecía un sistema de pagos peer-to-peer que no requería intermediarios financieros tradicionales. En otras palabras, el Bitcoin vino a ofrecer una nueva forma de hacer transacciones sin la necesidad de intermediarios, con una moneda cuyo suministro estaba fijado desde el principio.

En este sentido, las criptomonedas como el bitcoin surgieron en parte como respuesta al deseo de tener un sistema monetario más transparente, resistente a la censura y no sujeto a las fluctuaciones y decisiones políticas de los gobiernos y bancos centrales. Y si bien no resolvieron directamente los problemas causados por la crisis financiera de Estados Unidos, sí proporcionaron una alternativa que cuestionaba el paradigma establecido de moneda y sistema financiero. Su crecimiento y adopción desde entonces han sido impulsados por una combinación de factores, incluyendo la innovación tecnológica, la especulación financiera y la búsqueda de una mayor autonomía y control sobre el propio dinero.

De hecho, a partir del nacimiento del bitcoin han surgido otras criptomonedas alternativas, conocidas como altcoins, cada una con sus propias características y aplicaciones. Ethereum, por ejemplo, lanzada en 2015 por Vitalik Buterin, introdujo contratos inteligentes a la funcionalidad de blockchain y fue la primera blockchain con un lenguaje de programación Turing completo incorporado.

A lo largo de los años, se ha observado cómo las criptomonedas han ganado una mayor aceptación y reconocimiento a nivel mundial. Grandes instituciones financieras, como PayPal y Square, han comenzado a permitir transacciones con criptomonedas, y países como El Salvador han adoptado el Bitcoin como moneda de curso legal.

b. Definición, características

En Argentina, en el art. 2º de la resolución 300/2014 de la unidad de información financia, las monedas virtuales se definen como

> […] la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

A continuación, en el segundo párrafo del art. citado, las diferencian específicamente del dinero electrónico, entendido como «[...] un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción».

Algunos autores también han brindado sus aportes a la tarea de definir y/o conceptualizar qué entendemos cuando hablamos de criptomoneda. En este sentido, Lansky (2018) entiende que se trata de un medio digital de intercambio que utiliza la criptografía para asegurar las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos.

Sánchez (2017) considera que «una criptomoneda, criptodivisa es un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido».

Continuando en la búsqueda de la definición conceptual de criptomoneda encontramos la propuesta por el GAFI (2015: 32), que la describe como

> la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

Ahora bien, uno de los valores añadidos que tiene en términos político-criminales la definición del GAFI es que le reconoce a la moneda virtual las principales utilidades del dinero: depósito de valor, unidad de cuenta y medio de pago. De igual modo, resalta las características de las criptomonedas, que bien podrían resumirse de modo consensuado en las siguientes: seguridad, descentralización y anonimato.

Al respecto, Navarro Cardoso (2019) explica:

> [...] La seguridad la aporta(n) las funciones resumen que permiten ser resistentes frente a ataques que intenten vulnerar la seguridad del sistema (autenticidad), así como la tecnología blockchain (trazabilidad) que le sirve de soporte. En la medida

> en que una vez que la transacción es insertada en un bloque, este es sellado y se une al siguiente, se le dota a aquella, a la transacción, de una seguridad tal que aporta soluciones sólidas frente a los fraudes que propician otras monedas digitales clásicas, más conocidas como dinero electrónico, caso de las tarjetas de créditos, así como en relación con determinados problemas propios de las monedas virtuales.
>
> […] La descentralización es la segunda gran característica: […] las transacciones se incorporan a un bloque, y bloque a bloque se añaden en un libro contable distribuido entre múltiples equipos o nodos. A diferencia de las formas de pago centralizadas, donde se suelen anotar las operaciones en un servidor único..., en la blockchain, ese libro de contabilidad distribuido, las transacciones se incorporan, primero en uno de los nodos participantes, y luego se transmiten al resto conectados en la red. Cada una de estas transmisiones se denomina «confirmación».
>
> La última característica es el anonimato. Probablemente sea la cuestión más controvertida, pues mientras unos sostienen que el anonimato es tal, otros lo matizan, y otros, claro está, lo niegan.
>
> De entrada, suele distinguirse entre anonimato y privacidad. El anonimato va referido a las personas: se ignora el remitente y el destinatario. La privacidad tiene que ver con el objeto: se desconoce el objeto de la transacción y su valor, pero no sus actores.
>
> Por un lado, no es necesaria la cesión de datos personales para crear carteras ni realizar transacciones. Sí es necesario un identificador pseudoaleatorio asociado a una cartera […] Otra cosa es cómo realizamos la transacción, pues en función de ello el anonimato puede comenzar a desaparecer, hasta llegar a ser inexistente, del mismo modo que puede casi mantenerse […]
>
> Se puede obtener mucha información a partir de una dirección o transacción, caso del balance de bitcóin o del historial de transacciones, así como del flujo del dinero, cash-out, conectividades, zona horaria y geolocalización aproximada del dueño. En cualquier caso, resulta extremadamente difícil lograr la atribución nominal de una dirección o cartera de bitcóin, a no ser que haya habido fallos de seguridad en las operaciones realizadas.

c. Tecnología blockchain o cadena de bloques

Las criptomonedas, según Nakamoto (2008), son activos digitales que emplean técnicas criptográficas para asegurar transacciones financieras, controlar la creación de nuevas unidades y verificar la transferencia de activos. Su aparición ha marcado un hito en la historia de la tecnología financiera, al ofrecer una alternativa descentralizada y segura a las monedas fiduciarias tradicionales.

Ahora bien, para empezar a comprender el funcionamiento de las criptomonedas se hace necesario, en primer lugar, conocer el ecosistema sobre el cual descansa su arquitectura, representado en este caso por la tecnología de cadena de bloques, también conocida como blockchain.

Al respecto, Zoccaro (2020) opina que la columna vertebral de las criptomonedas es la criptografía -de ahí su denominación como cripto-, y que la tecnología que hace realidad el sistema es la cadena de bloques -o blockchain-, a la cual define como una «[...] enorme base de datos almacenada en forma virtual y donde cada usuario del sistema tiene una copia actualizada y totalmente sincronizada en su computadora».

Profundizando en el concepto, explica:

> Se (la) puede imaginar también como un gran libro electrónico de actas donde se registran operaciones o sucesos, pero en lugar de existir un escribano que certifique estas actas una a una, esta validación la efectúa el conjunto de usuarios del sistema, sin necesidad de agentes externos o intermediarios y gracias al uso de la criptografía. Y una vez plasmada en la blockchain, la información no puede ser borrada ni modificada. Además, la información contenida en estos bloques es de acceso público para todos los usuarios, salvo por ciertos datos privados: así se posibilita el control sobre las transacciones.

En similar sentido, Navarro Cardoso (2019) afirma que

> […] blockchain es un gran libro de contabilidad, una gran base de datos, donde ningún asiento se puede borrar o modificar, y que no lo gestiona una sola persona, sino muchísimas, pues cada una -con su máquina- hace un asiento, de manera que una modificación exigiría que todas esas personas se pongan de acuerdo.

Y a continuación agrega

> [...] El libro funciona concatenando bloques, el anterior con el siguiente, formando una cadena. El bloque se 'sella' incluyendo un código alfanumérico, producto del recurso a tecnología algorítmica, llamado hash. Cada bloque nuevo debe contener el hash del bloque anterior. Por lo tanto, cada bloque nuevo que se une a la cadena posee todo el historial de la transacción.

Desde la perspectiva apuntada, podemos afirmar que Blockchain es una tecnología de registro distribuido que permite a los participantes de una red compartir datos de manera segura, transparente e inmutable. En lugar de almacenar información en un único servidor centralizado, la blockchain utiliza una red de nodos interconectados para mantener una base de datos descentralizada y distribuida.

En esencia, una blockchain es una cadena de bloques de datos enlazados mediante técnicas criptográficas. Cada bloque contiene un conjunto de transacciones verificadas, y cada nuevo bloque está vinculado al bloque anterior, formando así una cadena continua de datos.

La seguridad y la integridad de la blockchain se basan en la criptografía y el consenso distribuido. Cada transacción en la blockchain es verificada y validada por los nodos de la red, y una vez que se agrega un bloque a la cadena, es prácticamente imposible modificarlo sin el consenso de la mayoría de los participantes en la red. Esto crea un registro permanente e inmutable de todas las transacciones realizadas en la red.

La blockchain se utiliza principalmente como la infraestructura subyacente de las criptomonedas, pero su aplicación se extiende a una amplia gama de campos, y su potencial radica, fundamentalmente, en su capacidad para proporcionar un registro seguro y transparente de transacciones sin la necesidad de una autoridad central.

¿Cómo funciona entonces Bitcoin?

Como dijimos más arriba, la cadena de bloques -blockchain- es la columna vertebral de Bitcoin, una suerte de libro de contabilidad público y descentralizado que registra todas las transacciones de Bitcoin.

El libro funciona concatenando bloques -nodos-, formando una cadena. Los bloques contienen información sobre cada transacción, como el comprador y el vendedor, fecha

y hora, valor total y un código de identificación único para cada operación. Las entradas están conectadas en secuencia cronológica, formando una cadena digital de bloques.

El bloque se sella con la incorporación de un código alfanumérico conocido como hash, y luego pasa a formar parte de esa cadena. Cada bloque nuevo debe contener el hash del bloque anterior. Esto crea una cadena de bloques que es resistente a la manipulación y garantiza la integridad de las transacciones.

Ahora bien, para incorporarse a la cadena de bloques, las transacciones deben verificarse. Aquí entran en juego los mineros, cuya tarea consiste, según Lara y Muñoz (2017) en ejecutar «en sus máquinas software para resolver complejos cálculos matemáticos (llamados hashes) basados en criptografía con el fin de procesar y validar las transacciones». Estos problemas matemáticos se denominan *proof of work* (prueba de trabajo) y su resolución demanda un gran poder computacional y de procesamiento, que a su vez se traduce en un elevado costo energético.

Como contraprestación, los mineros obtienen una recompensa, ya que ponen a disposición de la red sus propios recursos. Al respecto, Navarro Cardoso (2019) aclara que, en realidad,

> [...] el minero recibe dos estipendios. El primero puede ir anejo a la propia transacción que se lanza a la red por quien quiere realizarla. A fin de lograr que se interesen por ella y la gestionen (la confirmen), ofrece una comisión. Cuanto más atractiva resulte, mayores probabilidades de que un minero le preste su atención. (…) El segundo estipendio es la conocida recompensa, que la genera automáticamente el sistema cuando se consigue (aleatoriamente) cerrar un bloque.

A modo de síntesis, dice Skalany (2019)

> Sólo quien resuelva o supere la prueba de trabajo tiene la capacidad de cerrar un nuevo bloque de la cadena y los restantes nodos operan como una suerte de auditores de la legitimidad y validez de la prueba superada brindando el consenso para que el bloque sea agregado de forma legítima a la cadena. La dificultad de superar la prueba de trabajo para generar un nuevo bloque se incrementa automáticamente para aproximarse a una temporización de generar un bloque cada 10 minutos. La cantidad de bitcoins nuevos que el sistema produce irá decreciendo en el tiempo, pues el sistema fue pensado para contener un total de 21.000.000 de bitcoins […]

Por otro lado, todos los usuarios que quieran enviar o recibir Bitcoins necesitan un bitcoin wallet, que pueden ser de software -en línea- o de hardware -dispositivos físicos.

Según la explicación que proporciona Small (2015)

> Estas billeteras digitales contienen una clave pública y una clave privada (conocidas como keys); la clave pública es similar a una dirección de correo electrónico que un usuario compartirá con otros usuarios de Bitcoin para que puedan enviar bitcoins. Alternativamente, la clave privada es similar a un número pin para una tarjeta de débito, cuyo propósito es confirmar que un usuario desea gastar bitcoins en su cartera.

Ampliando esta noción, Mora (2015) dice que

> […] para obtener y transferir la titularidad de los bitcoins se utiliza un mecanismo llamado 'criptografía asimétrica de clave pública'. En este esquema, cada persona que quiere constituirse como titular de bitcoins debe generar dos claves matemáticamente relacionadas, una de las cuales se hace pública y otra se mantiene en privado. Si una persona (digamos, «A») quiere transferir la titularidad de un bitcoin a otra persona (digamos, «B»), «A» debe utilizar su clave privada para ordenar

> la transferencia (10) y consignar la clave pública de «B» para identificar al destinatario de la misma. En este contexto, una vez finalizada la operación, se dice que «B» pasa a ser el nuevo titular del bitcoin referido, dado que el sistema sólo permitirá una nueva transferencia del mismo si ella es ordenada mediante la utilización de su clave privada. La clave pública (en el ejemplo referido en el párrafo precedente, la clave pública de «B»), que funciona entonces como una especie de nombre de usuario o de identificación de cuenta, no necesariamente está relacionada con los datos personales de su titular […].

2. Riesgos asociados a la utilización de Bitcoin en materia de lavado de activos

Hemos visto que las criptomonedas disponen de una serie de ventajas que tienen el potencial de transformar la economía mundial. Entre ellas se destacan la descentralización, dado que no está controlado por una autoridad como ser un banco central o un Estado, lo que proporciona grandes márgenes de autonomía.

Se afirma también que el uso de BTC hace posible que dos partes se relacionen directamente entre ellas sin la intervención de un tercero, y que pueden realizarse transacciones en forma rápida independientemente del lugar en el que se encuentren.

El anonimato es otra de las características que se reputan como ventajosas, fundamentalmente para ciertos usuarios legítimamente preocupados por la protección de su privacidad.

Ahora bien, algunas de esas ventajas también las convierten en instrumento para la comisión de delitos que van desde el lavado de activos, el financiamiento del terrorismo, la compraventa de armas y drogas en mercados negros, hasta la estafa y la evasión fiscal.

En particular, al facilitar las relaciones entre clientes no presenciales, el uso de BTC contribuye a la actividad ilegal transfronteriza respecto de espacios locales no regulados o con regulación no homogeneizada. En tales situaciones se torna difícil la adopción de medidas integrales antilavado. Sumado a ello, frente a la comisión de hechos delictivos transfronterizos, seguramente surjan problemas vinculados a la competencia territorial y los derivados de la dispersión de la evidencia.

Los detractores del BTC también advierten que la rapidez de las transacciones se erige como un obstáculo para el monitoreo preventivo de actividades potencialmente ilícitas, lo que a su vez se traduce en una mayor probabilidad de éxito desde la perspectiva de las fases de colocación y encubrimiento de la actividad de blanqueo y en un deterioro considerable de la eficacia de la persecución policial.

A su vez, y dado que el BTC permite mayor anonimato que los métodos tradicionales de pago -ello así, por cuanto las direcciones que funcionan como cuentas carecen de información personal de su titular-, no se generan registros del historial asociados a personas o entidades determinadas, ni las operaciones requieren o proporcionan la identificación de sus reales intervinientes.

Sobre este punto, Navarro Cardoso (2019) afirma que

> […] la propia arquitectura del bitcóin, sustentada sobre la cadena de bloques, permite la trazabilidad de las transacciones, pero ello no conlleva la identificación de los actores reales que intervienen en ella. Es en este contexto en el que hay que situar la afirmación relativa al anonimato de las transferencias y, por ende, la financiación

> anónima. […] Un dato de todo punto revelador del anonimato de bitcóin, de interés...en tanto impide la persecución del blanqueo, es que entes y organismos como la BCE, el GAFI o Europol […] no dudan en reconocerle tal característica. Así mismo, la directora del Fondo Monetario Internacional, F. Lagarde, en el blog de la propia institución, publicó un documento reconociéndolo.

Siguiendo con el desarrollo de este punto, se afirma también que el anonimato en las transacciones imposibilita la aplicación de las medidas antilavado *know your customer* (por sus siglas en inglés, «KYC») y afecta las acciones antiblanqueo que pudieran implementarse en pos de vincular al actor con una operación sospechosa.

En efecto, difícilmente se puedan monitorear transacciones si no se conocen las partes que intervienen en ellas. Una vez más, Navarro Cardoso (2019) nos enseña que, si bien no todas las acciones de monitoreo y detección temprana de actividades sospechosas requieren conocer a los actores, no menos cierto es que, a la hora de imputar un ilícito administrativo y/o penal, será preciso conocer a los sujetos que intervinieron en ellas.

Agrega que ello contribuye decididamente a la tercera fase del delito de lavado de activos -la colocación- «[…] porque, incluso, facilita la actividad de un posible testaferro».

Vinculado lo anterior con la descentralización, la falta de supervisión por un órgano de control deviene en la necesidad de incrementar los sujetos obligados a reportar operaciones sospechosas ya que, de otro modo, las normas antilavado podrían devenir completamente inútiles.

Por otro lado, si bien existen desarrollos informáticos que permiten cierto nivel de monitoreo e identificación de este tipo de operaciones, se ha propiciado el desarrollo de herramientas y servicios adicionales de anonimato, que dificultan aún más el seguimiento de las transacciones y el origen de los fondos, y se conocen como anonymiser.

En su documento *directrices para un informe basado en riesgo (sobre) monedas virtuales* (2015), el GAFI dice que el término *anonymiser* «[…] se refiere a las herramientas y servicios, tales como acuñado y mezcladores, diseñados para ocultar la fuente de una transacción de Bitcoin y facilitar el anonimato».

En dicho documento también encontramos una definición del mixer o mezclador:

> […] es un tipo de anonymiser que oscurece la cadena de transacciones en los blockchain mediante la vinculación de todas las transacciones en la misma dirección bitcoin y enviarlas juntas de una manera que les hace parecer como si fueron enviadas desde otra dirección. Un mezclador o tumbador envía las transacciones a través de una serie de transacciones no reales complejas, semi-al azar que se le hace extremadamente difícil vincular monedas virtuales específicas (direcciones) con una transacción determinada. Servicios de mezclador funcionan con el recibo de instrucciones de un usuario para enviar fondos a una dirección bitcoin particular. El servicio de mezclado entonces 'mezcla' esta transacción con otras transacciones de usuarios, tal que llega a ser confuso a quien el usuario pretendía enviar los fondos. (Ejemplos: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Algunos recurren a coinjoin, que también es una herramienta de privacidad y que permite agrupar transacciones de múltiples usuarios en una única transacción combinada, de manera que los detalles específicos de quién envió bitcoins a quién se vuelvan difíciles de rastrear.

Para ello, los usuarios encuentran una manera de coordinarse (a menudo a través de un servicio específico o un protocolo) para realizar una transacción conjunta, en la que cada uno pretende enviar una cierta cantidad de BTCs a una o más direcciones.

Luego combinan -mezclan- sus entradas -las direcciones desde donde se envían los BTC- y salidas -donde serán enviadas- en una sola transacción CoinJoin, y cada usuario firma su parte, aprobando así la porción de la operación que le corresponde.

Firmada la transacción, esta se transmite a la red de BTC y se confirma como cualquier otra.

Otro mecanismo de anonimato es recurrir al uso de direcciones y carteras desechables -por cada transacción se crea una nueva dirección de BTC con el fin de evitar que se acumulen patrones que puedan ser analizados para rastrear su actividad- o de redes TOR y VPNs -que permiten ocultar la dirección IP, lo que hace aún más difícil la vinculación de una dirección de Bitcoin con una identidad específica basada en la información de la red-.

A modo de conclusión, y nuevamente con cita de Navarro Cardoso (2019), «[a] partir de lo expuesto podríamos afirmar que las características propias de la blockchain de BTC favorece su uso delictivo. Si a ello se le suma el incremento de anonimato que ofrecen los mezcladores y carteras oscuras, el riesgo del BTC como instrumento de blanqueo se dispara».

a. Impacto de los criptoactivos en esta particular modalidad delictual

i. *Aspectos relevantes del delito de lavado de activos*

A modo introductorio, conviene recordar que el término lavado de activos -en inglés, *money laundering*- se habría originado en los EE.UU., en la década de 1920, a partir de la necesidad de describir el proceso mediante el cual los grupos criminales organizados -la mafia- ocultaban el origen de los fondos ilegítimamente obtenidos mediante la compra de negocios como lavanderías, que utilizaban para darles apariencia de legalidad.

En efecto, las lavanderías manejaban grandes volúmenes diarios de dinero en efectivo, lo que las hacía ideales para mezclar el dinero obtenido ilegalmente con los ingresos legítimos que se percibían.

Ahora bien, el lavado de activos irrumpió en la escena global a partir del desembarco del narcotráfico como problema transnacional. A inicios de la década del 70 se implementó en los EE.UU. una rigurosa política regulatoria que exigía a las entidades financieras que reportaran determinadas transacciones que se realizaban mediante la prestación de sus servicios.

Luego, en los años '80, concretamente en el año 1986, EE.UU. incorporó el lavado de activos al catálogo de delitos penales en procuras de obtener una sanción punitiva que incluyera no sólo a los actores de la cadena de producción, distribución y venta de sustancias estupefacientes, sino también a los encargados de la colocación de su producido.

En 1988 esta tipificación se internacionalizó con la firma de la Convención de Viena y en los años venideros se firmaron numerosos acuerdos internacionales en gran cantidad de países que incluían varios delitos, entre ellos el lavado de activos.

A nivel local, el primer antecedente legislativo en la materia lo encontramos en la ley 23.737 (1989) sobre el régimen legal de estupefacientes, que en su art. 25 reprimía con pena de 2 a 10 años de prisión y multa de 6 a 15 mil australes al que

> […] sin haber tomado parte ni cooperado en la ejecución de los hechos previstos en esta ley, interviniere en la inversión, venta, pignoración, transferencia o cesión de las ganancias, cosas o bienes provenientes de aquéllos, o del beneficio económico obtenido del delito siempre que hubiese conocido ese origen o lo hubiera sospechado.

Con igual pena castigaba al «[…] que comprare, guardare, ocultare o receptare dichas ganancias, cosas, bienes o beneficios conociendo su origen o habiéndolo sospechado».

Culminaba señalando que, a los fines de la aplicación de dicho artículo, «[…] no importará que el hecho originante de las ganancias, cosas, bienes o beneficios se haya producido en el territorio extranjero», haciéndose eco del carácter transnacional del narcotráfico.

La evolución legislativa culminó con la actual redacción del art. 303 del código penal argentino, que reprime

> […] con prisión de tres (3) a diez (10) años y multa de dos (2) a diez (10) veces del monto de la operación, el que convirtiere, transfiriere, administrare, vendiere, gravare, adquiriere, disimulare o de cualquier otro modo pusiere en circulación en el mercado, bienes u otros activos provenientes de un ilícito penal, con la consecuencia posible de que el origen de los bienes originarios o los subrogantes adquieran la apariencia de un origen lícito […].

Dicho lo anterior, existe consenso generalizado en cuanto a que el delito de lavado de activos se divide en tres etapas: colocación, estratificación e integración. La primera consiste en introducir los fondos ilegales en el sistema financiero; en la segunda se procura separar aún más el dinero ilícito de su origen mediante la realización de múltiples y diversas transacciones diseñadas para dificultar el seguimiento del dinero; en la fase final, los fondos blanqueados se integran de nuevo en la economía legítima.

Sin embargo, tal división muchas veces resulta irreconocible, dado que las fases pueden superponerse, en ocasiones son simultáneas o desordenadas, ello como consecuencia de la utilización de medios de blanqueo cada vez más complejos.

Ahora bien, con respecto a la fase de colocación, Carrizo (2003) nos dice que:

> Se considera a esta etapa la más delicada del proceso de lavado, atento a que es aquí cuando el lavador opera los mecanismos a su alcance a los fines de lograr la reducción de los bienes de extraño origen, que rara vez pueden justificar y, de este modo lograr una manipulación de dichos bienes de manera subrepticia. Cuando hablamos de reducción del bien, nos estamos refiriendo no a una quita o pérdida de su valor, sino a la maniobra llevada a cabo por el lavador a los fines de convertir, cambiar o sustituir el bien indicado para así poder continuar con el proceso sin que pueda ser detectado por la autoridad.

Sobre la fase de estratificación, Valdés Trapote (2022) aporta:

> […] consiste en la mezcla del dinero o los bienes en diversas empresas e instituciones financieras. El dinero se transporta a otros lugares para ocultar su origen ilícito. Lo importante aquí es adquirir activos para transferirlos o intercambiarlos con otros de

> origen lícito. En esta etapa, una vez que el dinero entra en los circuitos financieros, se hacen movimientos para ocultar su origen, con el fin de erradicar cualquier posible vínculo entre el dinero colocado y su origen. Las técnicas más frecuentes son enviar el dinero a paraísos fiscales o centros offshore, para asegurar que los fondos circulen a través de diferentes países, instituciones y cuentas mantenidas por diferentes personas físicas o jurídicas

Finalmente, recurriendo a Marengo (2011), la integración es el

> […] último escalón en el proceso del lavado. Se busca con esta fase el perfecto asentamiento de los bienes y […] que […] las autoridades consideren que ellos fueron obtenidos por medios legítimos y que pertenecen de manera definitiva a la economía oficial. Al haber transcurrido sin inconvenientes las etapas anteriores y dejado constancia de ello a través de registros contables y tributarios se les otorga apariencia legal, de modo de enervar cualquier tipo de persecución.

Toda vez que no pretendemos analizar a fondo el tipo penal del art. 303 del código de fondo -por no ser objeto de la presente investigación-, nos limitaremos a señalar que

- la acción punible podría definirse como la transformación de bienes que provienen de un delito y otorgarles apariencia de licitud
- sujeto activo del delito puede ser cualquier persona
- el ilícito penal al que hace referencia el art. mencionado debe interpretarse como comprensivo de la totalidad de los delitos del C.P. y las leyes especiales, y también las infracciones de naturaleza penal aduaneras, cambiarias o fiscales
- en cuanto al delito precedente, la Convención de Varsovia establece como requisito para una condena por blanqueo de capitales que existe una condena previa o simultánea por aquella primera infracción
- el tipo subjetivo solo admite el dolo directo debido a que hace falta que el sujeto conozca que los bienes provienen de la comisión de un hecho delictivo y su intención de concretar el fin de apariencia exigido por la norma.

ii. *Criptolavado de activos como forma específica de esta modalidad criminal.*

Sentado cuanto precede, diremos que el criptolavado -esto es, el recurso al uso de activos virtuales (AV) para el lavado de activos- es una derivación natural del surgimiento de los mercados de bienes y servicios ilícitos en la denominada *dark web*, un sector de la Internet al que solo se puede acceder mediante la implementación de herramientas tecnológicas que permiten navegar anónimamente, como el sistema TOR.

Es, a su vez, consecuencia de la aparición de Bitcoin, que posibilitó el funcionamiento de estos mercados oscuros al ofrecer un medio de pago, en principio, también anónimo.

El primero de esos mercados fue Silk Road, que a pesar de haber sido cerrado con bastante rapidez por las autoridades -inició en enero del año 2011 y para octubre del año 2013 el FBI ya había cerrado el sitio y arrestado a su propietario Ross Ulbritch, quien terminó condenado a cadena perpetua en 2015-, fue inmediatamente reemplazado con otros similares, que hoy son fuente de un alto porcentaje de los fondos ilícitos que se reciclan mediante los activos virtuales y los servicios asociados a éstos.

Sobre este punto, el GAFILAT (2021) explica que «un estudio que analizó las transacciones con Bitcoin entre 2013 y 2016 concluyó que la casi totalidad de los bitcoins de origen ilícito lavados a través de plataformas de intercambio de criptomonedas provenían de los mercados de la Red oscura».

Ahora bien, este mismo proceso de tres etapas descripto en relación al lavado de dinero se aplica también a los criptoactivos, pero las complejidades asociadas a cada fase son inherentemente distintas.

Al respecto, el GAFILAT (2021) sostiene

> El proceso de 'criptolavado' admite las mismas tres etapas que el lavado de activos tradicional (colocación, estratificación e integración). Sin embargo, las maniobras asociadas a cada una de esas fases tienen características propias, producto de la naturaleza de los AV involucrados. Así, por ejemplo, la propia necesidad de que exista, o no, una etapa de colocación depende de si los fondos ilícitos son obtenidos en moneda fiduciaria o directamente en criptomonedas. Ello así, desde que en el primer supuesto es necesario efectuar una conversión de una moneda a otra, mientras que en el segundo no lo es.

En sentido similar, Valdés Crapote (2022) nos enseña

> Por ejemplo, en la etapa de colocación, los fondos se mueven de un banco tradicional a una cuenta con un servicio de cambio de criptoactivo con el fin de comprar monedas primarias como bitcoin o Ethereum. Luego, en la fase de capas, las monedas primarias se intercambian por varios criptoactivos, alternativos, que permitan mayor privacidad, en un intento de enturbiar el papel electrónico, lo que hace más difícil para las fuerzas del orden seguir el rastro de dinero. Este proceso también se conoce como salto de cadena. Luego, en la etapa de integración el lavador puede cambiar esos criptoactivos de nuevo a otros activos más conocidos, que luego se pueden cambiar de nuevo por dinero tradicional. Mientras que la descripción es de nuevo demasiado simplificada, el relato pretende describir un esquema bien diseñado pues, al fin y al cabo, las criptomonedas han sido vistas como una oportunidad de inversión única y lucrativa, no solo con el fin de lavar activos. Como resultado, puede ser difícil detectar la identificación de actividades de colocación o el reconocimiento de una transacción sospechosa iniciada a través de un intercambio de criptomonedas y deslindarla de una rápida y fácil inversión. Esto es especialmente complejo si la criptomoneda intercambiada no tiene suficientes protocolos de conocimiento de su cliente y favorece el anonimato.

Por su parte, Donna (2022) sostiene que el tipo penal del art. 303 no encontraría ningún inconveniente en cuanto a su aplicación, «ya que el dinero con el que se compra Bitcoins o cualquier pago con criptomoneda debe provenir de un ilícito, si se da ese requisito entra en el tipo penal de lavado de argentina».

Continúa por señalar que

> El problema podría aparecer en la instrucción, en el sentido de si...el poder judicial cuenta con las herramientas, los medios y personas capacitadas en programación, sistemas financieros, etc. (entendiendo que ya tiene gente capacitada en Derecho penal) a los fines de poder recaudar la información o la prueba necesaria para probar el ilícito o prevenirlo. En otras palabras, el tipo penal es el mismo de siempre, lo que se vuelve más complejo son los métodos que se utilizan para llevar a cabo la negación al Derecho, ello exige mayor conocimiento en sistemas informáticos, en fianzas, etc.

Profundizando en las características asociadas a las etapas del criptolavado, hemos de mencionar que en la colocación se suele recurrir a un *proveedor de servicios de activos virtuales* (en adelante, «PSAV»), por lo general una plataforma de intercambio de criptomonedas que permita convertir la moneda fiduciaria en Bitcoins.

Además, en jurisdicciones que han ajustado su normativa a lo establecido en la Recomendación 15 del GAFI, que exige a los PSAV el reporte de operaciones

sospechosas de sus clientes, los lavadores podrían optar por utilizar un PSAV ubicado en un país/Estado que no esté sometido a deberes de ALA o que incumpla sus obligaciones.

Concluida la etapa de colocación, los delincuentes pueden recurrir a múltiples mecanismos para la estratificación de los fondos. Por un lado, se pueden realizar múltiples transacciones entre monederos de activos virtuales controlados por una misma persona -tengamos en cuenta que las criptomonedas admiten a los usuarios mantener un número indefinido de direcciones- o por varios sujetos distintos, lo que sumado a la simplicidad de creación de nuevas direcciones, la disociación con la identidad real del usuario, la velocidad de las transacciones y la facilidad con la que se pueden cruzar fronteras nacionales y regulatorias, hacen posible la creación de patrones de estratificación extremadamente complejos.

Tiene dicho el GAFI (2021) que

> Los PSAV cumplen una función esencial en los esquemas de criptolavado, ya sea en la fase de colocación (para la conversión de moneda fiduciaria en AV), durante la fase de estratificación (por ejemplo, permitiendo el cambio de una criptomoneda por otra o brindando servicios de «mezclado») o en la etapa final, donde los/las beneficiarios/as de la maniobra convierten los fondos nuevamente a moneda fiduciaria. Ello ha derivado en la aparición de plataformas de intercambio de AV específicamente creadas y estructuradas para facilitar el criptolavado. En tal contexto, un informe reciente concluye que un tercio del volumen de tráfico transfronterizo de bitcoins se vuelca a PSAV con políticas deficientes de ALA/CFT.

Entre los principales servicios que ofrecen los PSAV a los delincuentes encontramos los de mezclado o mixing de criptomonedas, que combinan los ingresos y egresos de fondos de distintos/as usuarios/as para tornarlos indistinguibles entre sí.

También pueden implementarse, a través de los PSAV, otras metodologías de estratificación, como el chainhopping, que significa salto de cadenas y que consiste, básicamente, en el intercambio de diferentes criptomonedas entre sí, con la finalidad de cortar la cadena de transacciones en las respectivas blockchain.

3. Modalidades de lavado de activos mediante el uso de criptomonedas

A continuación, haremos una breve reseña de las acciones y estrategias más comúnmente utilizadas en materia de lavado de activos a través de criptomonedas.

Conviene recordar aquí que las criptomonedas no son ilícitas en sí mismas, tampoco lo es la tecnología que les sirve de soporte, sino el fin o uso que le dan quienes se dedican a la actividad criminal.

a. Compra de criptomonedas

La compra de criptomonedas puede ser un método para lavar dinero. Así lo afirma Navarro Cardoso (2019), y agrega: «El sujeto interesado en la adquisición de alguna de ellas ofrece dinero fiduciario a cambio de recibir criptomoneda. La colocación misma de esta puede ser una operación de lavado (recordando...que la segunda fase del blanqueo, el encubrimiento, o se entiende innecesaria en tanto implícito en la opacidad de la blockchain del bitcóin, o se produce con el recurso a los mezcladores)».

b. Monetización o tokenización

Las monedas digitales no necesariamente tienen que cambiarse por monedas legalmente establecidas, sino que pueden ser utilizadas directamente o a través de un proveedor de servicios de custodia de monederos electrónicos para la adquisición de bienes y servicios. De allí, entonces, la posibilidad de destinar activos obtenidos ilegítimamente con fines lícitos.

En opinión que compartimos, y con cita -una vez más- del autor Navarro Cardoso (2019), ha de señalarse que:

> La innecesariedad de la monetización va en parte ligada, como resulta obvio, a la generalización del uso de estas criptodivisas, sea bitcóin, o la que resulte triunfante en esta también competición, pues existen alternativas con mayores ventajas desde el punto de vista del uso delictivo para blanquear dinero.

Por su parte, la expresión *token*, en el ámbito tecnológico, remite a la idea de *ficha*, *cupón* o *vale*, pues su uso permite el acceso a un bien o un servicio. En general, los criptotokens, si bien guardan similitud con las criptomonedas -en cuanto son una unidad de valor aceptada por una comunidad y se sustentan en teconología de cadena de bloques-, tienen más funcionalidades -como ser ceder un derecho, abonar un trabajo, permitir acceso a servicios extras de la empresa que lo ha emitido-, que les son asignadas por la entidad privada que las emite.

Por ello se afirma que existe una tendencia hacia la *tokenización*, proceso que facilita en mucho la actividad de blanqueo, empleando los bitcóin como moneda y como activo financiero.

c. Minado de criptoactivos

En este caso, los delincuentes invierten dinero obtenido ilícitamente en equipos de minería de criptomonedas que pueden incluir hardware especializado como ASICs (Application-Specific Integrated Circuits) o GPU (Graphics Processing Units). La compra de equipos de minería es una forma de convertir dinero en efectivo en bienes tangibles que no están directamente ligados a actividades ilícitas.

Una vez adquiridos los equipos, los delincuentes operan una instalación de minería para generar criptomonedas (como Bitcoin, Ethereum, etc.) que luego pueden vender en *exchangers* -plataforma (en línea o física) que permite a los usuarios comprar, vender e intercambiar criptomonedas por otras criptomonedas o por monedas fiduciarias (como dólares, euros, yenes, etc.)-, que tienen regulaciones más laxas o que no implementan estrictos procedimientos de Conozca a Su Cliente (KYC).

En consonancia con ello, Valdés Crapote, A. (2022) afirma que «[e]xisten organizaciones que obtienen dinero ilícito a través de diversas actividades delictivas y necesitan blanquearlo, usar ese dinero para comprar equipo minero, con el fin de minar criptoactivos. Una vez que los beneficios se obtienen a través de la minería, podrían reinvertirse en cualquier activo o en una actividad aparentemente legal, cuyos beneficios pueden justificarse ante las autoridades».

d. Exchangers

Como ya dijimos, un *exchanger* de criptomonedas, también conocido como intercambio o casa de cambio de criptomonedas, es una plataforma (en línea o física) que permite a los usuarios comprar, vender e intercambiar criptomonedas por otras criptomonedas o por monedas fiduciarias (como dólares, euros, yenes, etc.).

Estas plataformas juegan un papel crucial en el ecosistema cripto, dado que proporcionan la estructura necesaria para que los usuarios puedan acceder, comerciar y utilizar criptomonedas.

Ahora bien, ¿cuáles son los riesgos asociados a los *intercambios* s en materia de lavado de activos? Una vez más, Valdés Crapote (2022) nos acerca la respuesta, afirmando que son tres: el primero, que tradicionalmente no han sido sujetos obligados en cuanto a la prevención del blanqueo de capitales, aunque las legislaciones más modernas vienen modificando este paradigma imponiendo su inscripción en registros concretos, con obligaciones parecidas a los bancos; el segundo, que los mandantes no operan desde el país en el que está radicada la plataforma; y el último, que pueden ser controladas directamente por una organización criminal que se dedique precisamente al blanqueo de capitales».

e. Traders

Un trader es una persona que compra y vende criptomonedas con el objetivo de obtener beneficios financieros, sirviéndose de la volatilidad del mercado para realizar transacciones en diversos intervalos de tiempo, desde minutos hasta meses, según su estrategia y estilo de trading.

En general, se anuncian principalmente a través de la darkweb para cambiar moneda virtual por monedas fiduciarias.

En torno al tópico que nos convoca, Valdés Crapote, A. (2022) sostiene que existen algunos indicadores que podrían vincular el trading con el blanqueo de capitales, entre las cuales menciona:

- Operar con moneda virtual a partir de efectivo en volúmenes significativos.
- Realizar cambios de moneda virtual con efectivo utilizando canales que implican pagar altas comisiones y/o soportar peores tipos de cambio que los métodos alternativos.
- Intercambios hechos en lugares inusuales y anónimos. En muchos casos, las ventas y compras se organizan a través de foros de Internet (p2p) y los intercambios tienen lugar físicamente para garantizar que el comprador de las criptomonedas paga en efectivo y el vendedor simplemente proporciona su contraseña de cuenta.
- La compra se realiza con beneficios directos de otras actividades ilícitas.

f. BTMs o cajeros automáticos de criptomonedas

Los cajeros automáticos de criptomonedas (Bitcoin ATMs o BTM) son dispositivos físicos que, mediante el uso de dinero de efectivo o tarjetas bancarias, permiten la compra y, en algunos casos, la venta de criptomonedas como Bitcoin, Ethereum, Litecoin y otras.

Los BTM suelen encontrarse en tiendas abiertas al público y normalmente no son objeto de licencia, por lo que sus medidas de instalación, mantenimiento y seguridad no están reguladas ni supervisadas por ningún organismo público.

De hecho, dependiendo de las regulaciones locales, algunos cajeros automáticos de criptomonedas permiten transacciones anónimas o con requisitos mínimos de verificación de identidad, lo que aumenta el riesgo de lavado de activos.

A partir de lo expuesto, deviene ineludible preguntarnos cómo podría lavarse dinero mediante el uso de este tipo de dispositivos. Para dar respuesta a dicho interrogante recurrimos a Adra, R. (2021), quien afirma:

> […] el lavado comienza a partir de la creación de varias cuentas de Bitcoin, cuyo único requisito es dar una cuenta de correo electrónico. El criminal crea varias, sin correlación con su verdadera identidad. Luego pide que el intercambio se haga por medio de este criptoactivo, pero depositando los bitcoins a diferentes cuentas con montos pequeños. Como segunda etapa, el retiro del dinero en efectivo lavado se hace de a poco, tomándolo de las distintas cuentas. En general, se hace por interpósitas personas, las cuales se van a encargar de retirarlo, para no despertar sospechas.

En sentido concordante, Hyman M. (2015) pone el ejemplo de un narcotraficante que crea varias cuentas de Bitcoin, y ya que el único requisito para abrir una cuenta de Bitcoin es proporcionar un correo electrónico, este narcotraficante crea un correo electrónico que no corresponde con su verdadera identidad por cada cuenta de Bitcoin. A raíz de esto exige a sus compradores que paguen las transacciones en bitcoins a diferentes cuentas en montos pequeños (esto para no levantar sospechas). A continuación, el narcotraficante utiliza una red de «mulas» que van a sacar poco a poco dinero en efectivo de las diversas cuentas de Bitcoin que posee. Adicionalmente puede hasta convertir sus ganancias en bitcoin en otras criptomonedas para encubrir aún más sus operaciones delictivas.

g. Mixers o Tumblers

Los «mezcladores» o «conmutadores» («mixers» o «tumblers») funcionan como servicios independientes de lavado de activos. El paso por un mixer sustituye la transferencia de AV entre dos direcciones (por ejemplo, de Bitcoin), de modo tal que los fondos de origen ilícito que una persona pretende transferir a otra se entremezclan con los provenientes de muchas otras direcciones de AV antes de ser finalmente enviadas a la del/la destinatario/a, dificultando la identificación de la dirección de origen y de las cuentas asociadas con los fondos de origen ilícito.

En términos más sencillos, según afirma Oppel, S. (2022):

> La manera de operar de este tipo de plataformas es muy sencilla. Recibe por parte de los usuarios una determinada suma de bitcoins y les devuelve el mismo monto -restando, obviamente, el cobro de una determinada comisión-, pero distribuido en varias operaciones y utilizando para ello sumas que fueron depositadas por otros usuarios. Así, cruza los saldos y los re-integra de manera 'partida' a través de varias

> transacciones, tornado prácticamente imposible poder trazar un seguimiento de ellos.

Los mixers funcionan de manera similar a un FCI, en donde múltiples individuos acumulan sus fondos para obtener un beneficio colectivo. La diferencia radica en que, en el caso de los mezcladores, el fondo común es utilizado para concretar múltiples transacciones con criptomonedas, y el beneficio es lograr un mayor grado de anonimato impidiendo la vinculación de las transferencias con direcciones de AV específicas.

En general, los mixers que se dedican al lavado de activos, amén de cobrar una comisión por sus servicios, no guardan registro de usuarios e incluso pueden opacar su infraestructura operando como servicios ocultos en TOR.

h. Chainhopping

El chainhopping es una técnica utilizada para mover criptomonedas de una blockchain a otra, a menudo a través de puentes (bridges) o intercambios descentralizados.

Los bridges son protocolos que permiten transferir criptomonedas y activos virtuales entre diferentes blockchains, facilitando la interoperabilidad y permitiendo a los usuarios mover sus activos de una red a otra sin necesidad de intermediarios centralizados.

Por su parte, los DEX o intercambios descentralizados son plataformas que permiten a los usuarios intercambiar criptomonedas directamente entre ellos, sin la necesidad de una autoridad central, lo que también ayuda a mantener el control sobre sus fondos. Ambos mecanismos son clave para la flexibilidad del ecosistema cripto, pero también presentan riesgos en términos de seguridad y lavado de activos.

Estos mecanismos permiten dispersar los activos entre diferentes redes, lo que a su vez dificulta el rastreo de las transacciones y posibilita a los delincuentes ocultar el origen ilícito de los fondos.

4. Casos de lavado de activos mediante el uso de criptomonedas. Dificultades y desafíos.

a. Silk Road (EEUU)

Silk Road fue un mercado en línea fundado en 2011 por Ross Ulbricht, conocido como «Dread Pirate Roberts», donde se podían comprar y vender drogas ilegales, armas, información de identidad robadas y otros bienes y servicios ilegales mediante el empleo de Bitcoins.

El GAFI (2015) explica que:

> «…funcionaba como un ciber bazar global de mercado negro que intermediaba transacciones criminales anónimas y fue utilizado por varios miles de narcotraficantes y otros vendedores ilegales para distribuir bienes y servicios ilegales a más de cien mil compradores, un tercio de los cuales se cree que estaban en los Estados Unidos».

Se estima que facilitó transacciones por alrededor de 1.200.000.000 USD, las cuales le significaron a Ulbritch un aproximado de entre 10 y 15 millones de dólares durante el

tiempo que el sitio estuvo operativo, principalmente a través de comisiones que percibía por las transacciones realizadas.

La moneda exclusiva de intercambio en este particular mercado de bienes y servicios ilegales era el Bitcoin, lo que permitió a compradores y vendedores ocultar su identidad, a la vez que podían obtener un número ilimitado de direcciones Bitcoin y utilizar una diferente para cada operación dificultando aún más el rastro de los activos obtenidos ilícitamente.

Profundizando en el funcionamiento de Silk Road, y nuevamente con cita del GAFI (2015), diremos que:

> El sistema de pago de Silk Road funcionaba como un banco interno de Bitcoin, donde cada usuario de Silk Road tenía que tener una cuenta para realizar transacciones en el sitio. Cada usuario de Silk Road tenía al menos una dirección de Silk Road de Bitcoin (y posiblemente miles) asociada (s) a la cuenta de Silk Road del usuario, almacenadas en carteras mantenidas en servidores controlados por Silk Road. Para realizar una compra, un usuario obtenía bitcoins (normalmente a través de un cambiador de Bitcoin) y lo enviaba a una dirección Bitcoin asociada a su cuenta de Silk Road para financiar la cuenta. Cuando se hacía una compra, Silk Road transfería los bitcoins del usuario a una cuenta de fideicomiso que mantenía, en espera de la finalización de la transacción y luego se transfería los bitcoins del usuario/comprador de la cuenta de fideicomiso a la dirección de Bitcoin Silk Road del vendedor. Como un paso adicional, Silk Road empleaba a un 'tumbador' para cada compra, que…enviaba todos los pagos a través de una serie compleja, semi-random de transacciones dummy […].

Principales desafíos que implicó el caso.

El caso Silk Road fue -y sigue siendo- un ejemplo emblemático de cómo las criptomonedas, especialmente Bitcoin, pueden ser utilizadas en actividades ilegales. Los principales retos que implicó el caso se vinculan con:

- *Anonimato*. Si bien las transacciones de Bitcoin son públicas y quedan registradas en la cadena de bloques, los usuarios podían operar de manera relativamente anónima dado que no era necesario brindar información personal para crear una billetera, lo que facilitaba el comercio de bienes y servicios ilegales ofrecidos en Silk Road.
- *Dificultad de rastreo*. Aunque las transacciones eran visiles, como ya dijimos, rastrear la identidad de los usuarios resultaba complejo dado que utilizaban técnicas de como «mixers» o «tumblers» para ocultar el origen de los fondos.
- *Mercados oscuros*. La moneda de cambio exclusiva para operar en Silk Road era el Bitcoin, lo cual demostró la capacidad de las criptomonedas para facilitar las transacciones en el mercado negro.

b. BTC-e (EEUU)

El primer caso del que nos ocuparemos es el de BTC-e, una plataforma de intercambio de criptomonedas que operó entre 2011 y 2017 y fue objeto de investigaciones por su presunta implicación en el lavado de dinero y actividades ilícitas a gran escala.

El operador de BTC-e era un ciudadano ruso llamado Alexander Vinnik, quien luego de ser arrestado en Grecia en el año 2017 y de transitar un largo proceso de extradición, se declaró culpable de un cargo de conspiración para cometer lavado de dinero en los EEUU.

Según la acusación formulada en su contra, BTC-e no se registró como una empresa de servicios monetarios en los EE. UU., no aplicó ninguna regla de conocimiento del cliente o contra el lavado de dinero y no recopiló ningún dato de los clientes, utilizando empresas fantasmas para procesar conversiones fiduciarias para BTC-e.

En cuanto al modus operandi, la plataforma funcionaba con una mínima verificación de identidad, dado que para abrir una cuenta solo se requería un nombre, una dirección de correo electrónico y una contraseña, lo que facilitaba el anonimato. La plataforma no permitía a los usuarios transferir fondos directamente desde sus cuentas bancarias, sino que utilizaba intermediarios, lo que complicaba el rastreo de las transacciones. Esta estructura ayudó a los delincuentes a ocultar el origen de los fondos y dificultó que las autoridades financieras detectaran actividades sospechosas.

Ampliando este punto, Linares Quintana, B. (2019) indica que:

> el usuario debía crearse una cuenta para acceder al sitio web y una vez que la fondeaba con activos se encontraba en condiciones para realizar una transacción (cambiar criptomonedas a moneda fiat o viceversa), o simplemente para almacenar en dicha cuenta los activos virtuales.
>
> […] El usuario de BTC-e no podía fondear su cuenta mediante una transferencia bancaria (desde su cuenta bancaria) a (una cuenta bancaria de BTC-e) sí mismo, sino que debía hacerlo a (una cuenta bancaria) alguna sucursal o entidad afiliada de BTC-e. Tampoco podía extraer fondos directamente desde su cuenta, sino que debía requerir un depósito o una extracción por medio de otro exchanger, de manera que BTC-e evitaba recolectar cualquier información de los usuarios por la realización de transferencias bancarias o de cualquier otra actividad que dejara rastro en el sistema financiero tradicional.

Principales desafíos que presentó el caso BTC-e.

El caso BTC-e presentó varios desafíos para las autoridades y los investigadores debido a la naturaleza de las criptomonedas y a la estructura de la plataforma. Entre ellos podemos mencionar:

- *Anonimato y falta de regulación*. BTC-e operaba sin cumplir con las normativas de «conoce a tu cliente» (know your customer - KYC) y «anti-lavado de dinero» (Anti Money Laundering - AML). Esto permitía a los usuarios abrir cuentas con solo un nombre, una dirección de correo electrónico y una contraseña, sin requerir verificación de identidad, lo que dificultaba no sólo la individualización de los usuarios sino también rastrear las transacciones, permitiendo a los delincuentes operar con mayor facilidad.
- *Alcance de la operación*. BTC-e era una plataforma internacional con usuarios en todo el mundo, lo que implicaba la coordinación de diversas agencias y jurisdicciones. El arresto del operador de BTC-e, Alexander Vinnik, se realizó en Grecia, pero involucró a autoridades de Estados Unidos y varios otros países. La falta de armonización entre regulaciones de diferentes países complicaba la investigación y el procesamiento.
- *Uso de criptomonedas y mixers*. La plataforma permitía a los usuarios lavar dinero utilizando criptomonedas, que pueden ser difíciles de rastrear. Además, BTC-e facilitaba el uso de servicios de mezcla de criptomonedas («mixers») que fragmentaban y combinaban transacciones de diferentes usuarios, ocultando el origen y el destino de los fondos.

- *Tecnología avanzada*. Los criminales que utilizaban BTC-e aprovechaban el anonimato y la falta de transparencia de las criptomonedas. Esto requería que los investigadores emplearan herramientas tecnológicas sofisticadas para rastrear las transacciones y descifrar el rastro de los activos ilícitos, lo que ralentizaba el progreso de la investigación.
- *Jurisdicciones offshore*. BTC-e estaba registrada en jurisdicciones offshore, que generalmente tienen regulaciones financieras menos estrictas. Esto complicaba el acceso a información crucial para la investigación y permitía que la plataforma evitara cumplir con regulaciones internacionales de intercambio de criptomonedas.
- *Retiro y depósitos indirectos*. BTC-e evitaba que sus usuarios depositaran y retiraran fondos directamente desde o hacia cuentas bancarias tradicionales. En su lugar, los fondos se canalizaban a través de terceros, como afiliados o otros exchangers, lo que complicaba el seguimiento del dinero.

c. Caso bobinas blancas (argentina)

En el marco de esta causa se secuestró el cargamento de cocaína más grande de la historia del país, aunque la novedad radicó en que fue condenado un operador de criptoactivos por lavar el dinero de la organización criminal.

El operador ofrecía servicios de compraventa de bitcoins por fuera de las plataformas de intercambio, es decir, recibía criptomonedas a una cuenta en el extranjero y entregaba el equivalente en efectivo en el país, o bien recibía dinero en el país y transfería los bitcoins a un beneficiario en el exterior.

En este contexto, las autoridades consideraron que el operador no podía desconocer el origen ilícito del dinero y, por tanto, entendieron que con la prestación de este servicio contribuyó al blanqueo de fondos provenientes del narcotráfico.

La operatoria con Bitcoins:

- el operador de criptoactivos recibía transferencias de divisas de parte de integrantes de la organización criminal que se encontraban en el exterior, destinadas a los integrantes de esa organización que se hallaban en el país, mediante transacciones realizadas en la moneda virtual bitcoin;
- aprovecharon la falta de un organismo de control que regule la operatoria, y la ventaja de que las operaciones resultaran difícilmente asignables a una persona en particular, todo lo cual diluía toda posible trazabilidad para establecer el origen y destino del dinero;
- esa posibilidad de transferir dinero desde el exterior por fuera del sistema bancario y el anonimato de los intervinientes resultaron circunstancias que fueron claramente aprovechadas por la organización criminal;
- el operador recibió las distintas acreditaciones de bitcoins desde un bitcoin address desconocida, pero por orden de un tercero, y fue el operador quien posteriormente entregó su equivalente en dólares a distintas personas de nacionalidad extranjera, quienes se identificaron mediante la exhibición de un billete con una numeración específica.

Principales dificultades evidenciadas en el caso «bobinas blancas».

El caso «bobinas blancas» presentó numerosas dificultades específicas en materia de lavado de activos, dado que los narcotraficantes emplearon métodos complejos para ocultar y blanquear los fondos provenientes del tráfico de cocaína.

Entre ellas podemos mencionar:

- *Estructuración compleja del esquema de lavado*. Los delincuentes utilizaron múltiples capas de empresas de fachada, cuentas bancarias en diferentes jurisdicciones y otros intermediarios para mover y disimular el origen ilícito de los fondos. Estas estructuras, diseñadas para enmascarar el rastro del dinero, complicaban el rastreo de los activos desde su origen hasta su destino final.
- *Uso de criptomonedas*. El uso de criptomonedas para lavar los ingresos del narcotráfico representó una barrera significativa. Las criptomonedas permiten transacciones transnacionales rápidas y, a menudo, anónimas, lo que dificultaba el rastreo de los activos ilícitos, especialmente cuando se usaban servicios de mezcla (mixers) o criptomonedas enfocadas en la privacidad, como Monero.
- *Falta de cooperación internacional*. Si bien hubo coordinación entre países como Argentina, Estados Unidos y Europa, en algunas ocasiones las diferencias entre sistemas legales, así como la falta de tratados efectivos de cooperación en ciertas jurisdicciones, dificultaron el intercambio rápido de información y la identificación de los activos que habían sido transferidos a otras partes del mundo.
- *Metodologías sofisticadas de ocultamiento*. Además de usar criptomonedas, los narcotraficantes emplearon una combinación de bienes físicos (bobinas de acero) y movimientos financieros disimulados para lavar grandes cantidades de dinero. Las técnicas de ocultamiento sofisticadas y diversificadas dificultaban identificar las transacciones ilícitas entre las operaciones legales.
- *Fragmentación de los fondos*. Los delincuentes utilizaron tácticas de fragmentación de los fondos («smurfing»), dividiendo grandes sumas de dinero en pequeñas transacciones para evitar los sistemas de detección de lavado de dinero. Esto hacía más difícil para las autoridades detectar un patrón claro de actividades ilícitas.

d. Casos de lavado de activos mediante el uso de Bitcoin ATM

i. *EEUU (año 2019)*

En 2019, en Los Ángeles, un operador de una red de Bitcoin ATM fue arrestado y acusado de lavado de dinero por facilitar el intercambio de grandes cantidades de efectivo de origen ilícito en Bitcoin.

En este caso, el imputado permitía a los usuarios convertir efectivo en Bitcoin sin registrar la identidad de los clientes, a pesar de que la ley exigía que lo hiciera.

De esta manera, los delincuentes depositaban grandes cantidades de dinero en efectivo en las máquinas, convirtiéndolas en criptomonedas que luego podían transferir de manera anónima, dificultando el rastreo del origen ilícito de los fondos.

ii. *España (año 2020)*

En 2020, la Guardia Civil española desmanteló una organización criminal que utilizaba Bitcoin ATM (BTM) para lavar dinero proveniente del tráfico de drogas. Los narcotraficantes usaban estos cajeros automáticos de criptomonedas para blanquear

grandes cantidades de dinero en efectivo -derivadas de la venta de drogas en el mercado negro-, dado que estos dispositivos no siempre requieren los estrictos procesos de verificación que las instituciones bancarias tradicionales sí aplican.

Además, los delincuentes usaban técnicas de «smurfing» para dividir grandes sumas de dinero en montos pequeños, evitando los sistemas de alerta que se activan con transacciones de grandes cantidades -en concreto, hacían numerosos depósitos en cajeros Bitcoin en diferentes localidades para así disimular el origen de los fondos-.

Una vez convertidos en criptomonedas, los activos eran transferidos a varias billeteras digitales y «mixers» para ocultar el origen del dinero y romper cualquier vínculo con las actividades ilícitas. Luego, los fondos se movían a través de exchangers de criptomonedas, algunos de los cuales estaban ubicados en jurisdicciones con poca regulación o cooperación internacional.

Desafíos principales para las autoridades.

- *Falta de regulación clara*. En algunos países, la regulación de los Bitcoin ATM era ambigua, lo que dificultaba a las autoridades rastrear las transacciones o exigir un control de identidad riguroso en los depósitos y retiros.
- *Anonimato*. Los criminales aprovechaban la relativa facilidad con la que podían usar los BTM para hacer transacciones sin un nivel significativo de verificación de identidad.
- *Fragmentación de fondos*. Al dividir las transacciones en montos pequeños y realizar múltiples operaciones en diferentes cajeros, los criminales evitaban los umbrales que activan las alertas de posibles actividades de lavado de dinero.

5. Principales retos que implica el uso de criptomonedas en materia de lavado de activos a nivel investigativo

La irrupción de los activos virtuales -entre los cuales indudablemente se encuentran las criptomonedas- en el mundo criminal, concretamente como elementos para desarrollar nuevas modalidades de lavado de activos, impone adaptar las investigaciones a las características propias del ciberespacio, un escenario completamente diferente de aquél en que tradicionalmente se desarrolla esta particular tipología criminal.

Para las agencias encargadas de perseguir el lavado de activos ello supone nuevos obstáculos y desafíos que, a su vez, demandan nuevas estrategias y metodologías para asegurar la eficacia de su investigación.

Sobre este punto, el GAFILAT (2021: 41) sostiene que:

> En cuanto atañe a los obstáculos y desafíos, sobresalen el carácter 'extraterritorial' atribuido al ciberespacio por muchos expertos; la libertad y velocidad del intercambio de datos informáticos (incluyendo los que pueden ser relevantes como evidencia o para identificar AV susceptibles de incautación o decomiso) a través de la Internet; el fenómeno de la 'pérdida de conocimiento de la localización' de esos datos y la consecuente dificultad para establecer la ley procesal que debe regir su recolección. A ello viene a sumarse la aparición de novedosas tecnologías que impiden -o cuanto menos dificultan en gran medida- el ejercicio, por parte de las agencias policíacas, de las facultades de vigilancia que las leyes locales les confieren,

> entre las que cabe mencionar -además de las relacionadas al funcionamiento de los AV- a los nuevos métodos de comunicación que sustituyen a la Red Telefónica Pública Conmutada (RTPC), los sistemas de navegación anónima en la Internet y la encriptación de comunicaciones y contenidos almacenadas, entre otros.

Los casos analizados en el capítulo anterior exponen, con matices diferenciados, las implicancias del uso de criptomonedas con fines ilícitos, específicamente en torno al lavado de activos, dejando además en evidencia algunos de los principales retos que supone para las agencias encargadas de su persecución.

a. Pseudoanonimato. Anonimato parcial. Anonimato total. Transacciones confidenciales.

Para comenzar, hemos de referir que, en lo que respecta a la identidad de los usuarios asociados con las direcciones involucradas, la blockchain no proporciona ningún dato personal -como ser nombres, domicilios, abonados telefónicos, correos electrónicos-, dado que no es necesario brindar esa información para realizar las operaciones y el protocolo que determina su funcionamiento no prevé siquiera la inserción de esos datos en la cadena de bloques.

Asimismo, tampoco se almacenan las direcciones IP utilizadas para realizar las transferencias entre las partes. De hecho, aunque los nodos que participan en la red podrían determinar desde qué IP se origina una transacción, debido a la forma en que se distribuyen y retransmiten las operaciones en la red -donde no hay una entidad central que controle todas las transacciones, sino que son los propios nodos quienes las validan y transmiten-, resulta extremadamente complicado identificar de manera precisa qué nodo en particular inició una determinada operación.

A pesar de ello, no es del todo correcto afirmar que las transacciones con criptoactivos son completamente anónimas. En rigor de verdad, debido a sus características, es necesario utilizar métodos adicionales, más allá del simple análisis de la base de datos, para identificar a las personas detrás de cada dirección.

En este orden de cosas, el Grupo de Acción Financiera de Latinoamérica -GAFILAT- (2021: 41 y ss.) sostiene que:

> […] las distintas criptomonedas implementan una serie de desarrollos tecnológicos adicionales dirigidos a incrementar el anonimato de los/las usuarios. Así, de acuerdo al modo en que están estructuradas, estos activos virtuales pueden ofrecer cuatro niveles distintos de anonimato, a saber: 1) pseudo anonimato: derivado del uso de pseudónimos (direcciones alfanuméricas) para oscurecer la identidad del/la usuario/a; 2) anonimato parcial («set anonymity»), en el que la identidad del/la verdadero/a usuario/a puede ser una entre varias posibles, lo que se consigue mediante el uso de 'firmas en círculo'; 3) anonimato total del/la usuario/a, la cual se obtiene cuando el/la verdadero/a puede ser cualquiera de los nodos del sistema; y 4) transacciones confidenciales, en las que se garantiza que los montos transferidos también permanecen ocultos.

b. Falta de regulación global

En el plano estrictamente legal, siendo que las criptomonedas operan en una red global, no existe a su respecto una regulación uniforme, toda vez que algunos países tienen marcos legales rigurosos, mientras que en otros la regulación es laxa o inexistente,

lo que permite a los delincuentes trasladar fondos a través de jurisdicciones con baja supervisión para asegurar así el producto de sus fechorías.

Explica al respecto Adra (2021):

> Si tenemos que hablar del derecho internacional, podemos decir que no hay una regulación específica en cuanto a la comisión de delitos por el uso de criptomonedas, sino que más bien hay una guía de recomendaciones establecidas por el GAFI -a través de las llamadas FATF Recommendations- o por la 'Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional'[…]

c. Descentralización

Tampoco existe en relación a las criptomonedas una autoridad central que controle el flujo de los activos virtuales. Las criptomonedas, al estar descentralizadas, permiten a los individuos tener control total sobre sus activos, pudiendo realizar transacciones directamente entre ellos sin necesidad de intermediarios.

d. Localización

A su vez, su localización puede ser fija como no serlo; entran a jugar aquí los llamados monederos, que consisten en un medio físico, un dispositivo, un programa o un servicio utilizado por los poseedores de criptomonedas para almacenar (múltiples) claves públicas y/o privadas, necesarias para realizar todo tipo de transacciones.

Los monederos se usan para rastrear la propiedad y para recibir y gastar criptomonedas. Ahora bien, cuando se trata de monederos *online*, la información suele estar almacenada en servidores ubicados en *data centers* localizados en puntos estratégicos del globo. Además, los datos pueden estar en un solo lugar o distribuidos en varios servidores de diferentes países y reacomodarse automáticamente, o almacenados en forma redundante en múltiples copias para ser recuperados si falla un servidor.

Ello hace que, en ocasiones, ni la propia compañía que brinda el servicio de almacenamiento en la nube pueda establecer dónde se encuentra un conjunto específico de datos digitales -como puede ser un monedero Bitcoin- en un momento determinado; y que tampoco las autoridades interesadas en la investigación de dicha información, por su posible conexión con algún delito en particular, tengan acceso a ese dato.

Lo expuesto implica que, incluso frente a la necesidad de concretar la incautación o el decomiso de las criptomonedas, no se sepa con exactitud qué país tiene jurisdicción para disponer la medida cautelar.

A esta problemática en particular alude Spoenle (2010), refiriéndose a la misma como «loss of location». El autor apuntado explica que los datos en la nube se transfieren constantemente de un servidor a otro, moviéndose dentro o a través de diferentes países en cualquier momento. Sostiene que estos datos podrían reflejarse -*mirroring*- por razones de seguridad y disponibilidad y, por lo tanto, encontrarse en forma simultánea en múltiples ubicaciones dentro de un país o en varios países separados. Debido a esto, puede suceder que ni siquiera el proveedor de computación en la nube sepa dónde se ubican exactamente los datos.

Concluye su razonamiento afirmando que la ubicación, como variable constante aplicable a todos los objetos tangibles y a objetos de datos intangibles desde que Internet

también se hizo popular, ha dejado de funcionar bajo las condiciones de la computación en la nube -*cloud computing*-.

e. Tecnologías de «anonimato por diseño»

La aparición de herramientas tecnológicas que debilitan el anonimato ofrecido por Bitcoin y otras criptomonedas tradicionales ha derivado en la creación de nuevas alternativas, conocidas como *privacy coins* -monedas privadas-, que a través de la implementación de diversos mecanismos aseguran un mayor nivel de anonimato a sus usuarios. Para ejemplificar la cuestión, haremos hincapié en dos de las principales *privacy coins* que existen a la fecha, Monero y Zcash.

Monero (XMR) - a diferencia de las alternativas selectivamente transparentes, Monero es la única criptomoneda en la que cada usuario es anónimo por defecto. El remitente, el receptor y el importe de cada transacción se ocultan mediante el uso de tres importantes tecnologías: direcciones secretas, firmas de anillo y RingCT.

- *Direcciones secretas (stealth adresses)*. Las direcciones ocultas son una parte importante de la privacidad inherente de Monero. Permiten y requieren que el remitente cree direcciones únicas aleatorias para cada transacción en nombre del destinatario. El destinatario puede publicar solo una dirección, pero todos sus pagos entrantes van a direcciones únicas en la cadena de bloques, donde no pueden vincularse ni a la dirección publicada del destinatario ni a ninguna otra dirección de transacción. Al utilizar direcciones ocultas, sólo el remitente y el destinatario pueden determinar dónde se envió el pago.

En otras palabras, cada vez que alguien envía Monero, se genera una dirección única y aleatoria para esa transacción, conocida como «dirección furtiva». Esto significa que, aunque una transacción sea visible en la blockchain, no se puede vincular directamente al receptor, ya que la dirección del receptor real no se muestra públicamente.

- *Firmas de anillo (ring signatures)*. En criptografía, una firma en anillo es un tipo de firma digital que puede realizar cualquier miembro de un grupo de usuarios, cada uno de los cuales tiene claves. Por lo tanto, un mensaje firmado con una firma en anillo está respaldado por alguien de un grupo particular de personas. Una de las propiedades de seguridad de una firma en anillo es que debería ser computacionalmente inviable determinar cuál de las claves de los miembros del grupo se utilizó para producir la firma.

Por ejemplo, se podría utilizar un anillo de firma para proporcionar una firma anónima de «un funcionario de alto rango de la Casa Blanca», sin revelar qué funcionario firmó el mensaje. Las firmas en anillo son adecuadas para esta aplicación porque el anonimato de una firma en anillo no se puede revocar y porque el grupo para una firma en anillo se puede improvisar (no requiere configuración previa).

En el caso de Monero, una firma en anillo utiliza las claves de su cuenta y una serie de claves públicas (también conocidas como salidas) extraídas de la cadena de bloques mediante un método de distribución triangular. Con el paso del tiempo, los resultados anteriores podrían utilizarse varias veces para formar posibles participantes firmantes. En un «*anillo*» de posibles firmantes, todos los miembros del anillo son iguales y válidos. No hay forma de que un observador externo pueda saber cuál de los posibles firmantes de un grupo de firmas pertenece a su cuenta. Por lo tanto, las firmas en anillo garantizan

que los resultados de las transacciones no sean rastreables. Además, no hay problemas de fungibilidad con Monero dado que cada resultado de transacción tiene una negación plausible (por ejemplo, la red no puede decir qué resultados se gastan y qué no se gastan).

En términos menos complejos, esta tecnología combina las entradas de una transacción con otras entradas aleatorias en la red, de manera que es casi imposible identificar qué entrada es la real. Esto oculta al remitente de la transacción al difuminar su participación entre varias posibles entradas.

- *Ringct (ring condifential transactions)*. Es una versión mejorada de las firmas de anillo llamada «una firma de grupo anónimo espontáneo vinculable de múltiples capas», que permite ocultar cantidades, orígenes y destinos de las transacciones de forma tal que se mantienen confidenciales mientras siguen siendo verificables por los nodos de la red.
- *Zcash (zec)*. Es una criptomoneda similar a Bitcoin en su diseño (de hecho, se creó a partir del código base original de Bitcoin), pero utiliza una tecnología de privacidad que cifra la información de las transacciones y permite a los usuarios proteger sus activos.

Al igual que Monero, tiene un fuerte enfoque en la privacidad, pero permite a los usuarios elegir entre realizar transacciones públicas o privadas, ofreciendo más flexibilidad.

Utiliza una tecnología innovadora llamada zk-SNARK (Zero Knowledg-Succinct Non-Interactive Argument of Knowledge), que permite validar transacciones sin revelar detalles como las direcciones de los remitentes y receptores, o los montos involucrados.

Las pruebas de «conocimiento cero» permiten a una parte (el probador) demostrarle a otra (el verificador) que una afirmación es verdadera, sin revelar ninguna información más allá de la validez de la afirmación misma. Por ejemplo, dado el hash de un número aleatorio, el probador podría convencer al verificador de que efectivamente existe un número con este valor hash, sin revelar cuál es.

En una «prueba de conocimiento» de conocimiento cero, el demostrador puede convencer al verificador no sólo de que el número existe, sino de que, de hecho, conoce ese número, nuevamente, sin revelar ninguna información sobre el número.

A su vez, Zcash ofrece la posibilidad de llevar adelante transacciones de dos tipos: transparent y shielded (transparentes y blindadas). Si bien la mayoría de las cadenas de bloques exponen públicamente toda la información de transacciones y saldos, con Zcash existe la opción de mantener la información financiera privada (shielded) o transparente y disponible para el público como la mayoría de las otras cadenas de bloques.

He aquí una diferencia fundamental con Monero, dado que ésta oculta de forma predeterminada toda la información de las transacciones, ofreciendo privacidad total por defecto, mientras que Zcash permite elegir entre transacciones públicas y privadas, utilizando zk-SNARKs para las transacciones blindadas.

f. Plataformas de intercambio descentralizadas (DEXs)

Los DEXs son plataformas que permiten el intercambio de criptomonedas y tokens de manera descentralizada, esto es, sin la necesidad de un intermediario. A diferencia de los exchanges centralizados (CEX), donde un bróker controla los fondos y transacciones, en un DEX los usuarios tienen control total de sus activos gracias a los contratos inteligentes, que ejecutan y verifican transacciones en un entorno completamente transparente.

Este tipo de plataformas habilitan los intercambios directos P2P entre usuarios/as de criptomonedas y explotan innovaciones tecnológicas como las cuentas de fondos en custodia *-e-scrow accounts-* multi-firma para permitir que los/las usuarias intercambien activos virtuales sin necesidad de un tercero que custodie los fondos.

6. Marco regulatorio cripto

a. El panorama internacional.

La adopción de los activos virtuales -como medios de inversión, ahorro, para realizar transacciones, etc.- se presenta como una tendencia creciente a nivel global. En este sentido, dentro del índice general de adopción cripto para el año 2022 publicado por Chainalysis, cinco países miembros del GAFILAT -Brasil (7°), Argentina (13°), Colombia (15°), Ecuador (18°) y Méjico (28°)- aparecen posicionados entre los primeros 30 lugares, lo que refuerza la necesidad de emitir una regulación adecuada que cumpla con los estándares del GAFI, proporcione certeza a quienes operan con este tipo de activos dentro de la región del GAFILAT, y aborde los riesgos a los que se encuentran expuestos los diferentes actores.

En relación a la temática que nos compete en este punto, Adra (2021) afirma:

> Podemos clasificar en tres grupos las respuestas dadas por los países para combatir el lavado. El primer grupo lo integran los que han optado por la inacción, que son la mayoría de los países. Esto se debe a que no han elaborado ningún tipo de normativa regulando las criptomonedas, por la dificultad que implica el desafío de entender cabalmente todas las aristas de esta novedosa teconología...En el segundo grupo, podemos encontrar la postura que se encontraría en el otro extremo, que es la prohibición del uso de criptomonedas...Por último, se encuentran los países que optaron por la regulación. Este es el grupo más complejo, en el que cada país tiene sus matices propios con respecto a la normativa aplicable.

A nivel internacional, no existe una regulación específica o integral respecto al uso de activos virtuales para la comisión de lavado de dinero; en su lugar, aparecen las Recomendaciones del GAFI, definidas como «un esquema de medidas completo y consistente que los países deben implementar para combatir el lavado de activos […]» -GAFI, 2020), que fijan un estándar internacional que los Estados han de poner en práctica mediante la adopción de medidas ajustadas a sus circunstancias particulares, ello teniendo en cuenta la existencia de diversos marcos legales, administrativos y operacionales, y diferentes sistemas financieros.

En este sentido, según expresa Biagosch. (2018: 399):

> de acuerdo con el Grupo Internacional de Acción Financiera, la correcta aplicación de las recomendaciones sobre PLA/FT posibilita que los países puedan: I) proteger las instituciones públicas; II) aumentar la transparencia del sistema financiero; y III) facilitar la detección, investigación y enjuiciamiento del delito de lavado de activos y sus delitos precedentes, así como el recupero de los fondos sustraídos.

Entre las medidas consideradas esenciales por parte del GAFI se encuentran las siguientes:

- identificar los riesgos, y desarrollar políticas y coordinación internas;
- luchar contra el lavado de activos; financiamiento del terrorismo y financiamiento de la proliferación;
- aplicar medidas preventivas para el sector financiero y otros sectores designados;
- establecer poderes y responsabilidades (por ejemplo, autoridades investigativas, de orden público y de supervisión) y otras medidas institucionales;
- mejorar la transparencia y la disponibilidad de la información de sobre el beneficiario final de las personas y estructuras jurídicas; y
- facilitar la cooperación internacional.

Como no pretendemos aquí realizar un análisis pormenorizado del catálogo de recomendaciones del GAFI, haremos una breve reseña de las que, entendemos, se vinculan con el tópico de esta investigación.

Así entonces, la Recomendación 1 establece que los países deben identificar, evaluar y entender sus riesgos de lavado de activos/financiamiento del terrorismo, y deben tomar acción y aplicar recursos encaminados a asegurar que se mitiguen eficazmente los riesgos. Además, aplicar un enfoque basado en riesgo (EBR) para asegurar que las medidas adoptadas en pos de prevenir o mitigar el lavado de activos y el financiamiento del terrorismo sean proporcionales a los riesgos identificados.

La Recomendación 2 establece la necesidad de cooperación y coordinación nacional, aclarando que los países deben contar con políticas ALA/CFT/CFP a escala nacional, que tomen en cuenta los riesgos identificados, las cuales deben ser sometidas a revisión periódicamente, y deben designar a una autoridad o contar con un mecanismo de coordinación o de otro tipo que sea responsable de dichas políticas.

La Recomendación 3 propone tipificar el lavado de activos en base a la Convención de Viena y la Convención de Palermo, agregando que deben aplicar el delito de lavado de activos a todos los delitos graves, con la finalidad de incluir la mayor gama posible de delitos determinantes.

La Recomendación 4 sugiere la adopción de medidas similares a las establecidas en la Convención de Viena, la Convención de Palermo y el Convenio Internacional para la Represión de la Financiación del Terrorismo, que permitan a sus autoridades congelar o incautar y decomisar bienes y/o productos relaciones con el lavado de dinero.

La Recomendación 9 exhorta a asegurar que las leyes sobre el secreto de la institución financiera no impidan la implementación de las Recomendaciones del GAFI.

La Recomendación 10 se refiere a la debida diligencia del cliente, y comienza con la prohibición a las instituciones financieras de mantener cuentas anónimas o cuentas con nombres ficticios

Dispone, a su vez, la necesidad de exigir a las instituciones financieras que emprendan medidas de Debida Diligencia del Cliente (DDC) cuando: (i) establecen relaciones comerciales; (ii) realizan transacciones ocasionales: (i) por encima del umbral aplicable designado (USD/EUR 15,000); o (ii) están ante transferencias electrónicas en las circunstancias que aborda la Nota Interpretativa de la Recomendación 16; (iii) existe una sospecha de lavado de activos o financiamiento del terrorismo; o (iv) la institución financiera tiene dudas sobre la veracidad o idoneidad de los datos de identificación sobre el cliente obtenidos previamente.

A su vez, entre las medidas de DDC a adoptarse, se proponen:

> (a) Identificar al cliente y verificar la identidad del cliente utilizando documentos, datos o información confiable, de fuentes independientes. (b) Identificar al beneficiario final y tomar medidas razonables para verificar la identidad del beneficiario final, de manera tal que la institución financiera esté convencida de que conoce quién es el beneficiario final. Para las personas jurídicas y otras estructuras jurídicas, esto debe incluir que las instituciones financieras entiendan la estructura de titularidad y de control del cliente. (c) Entender, y cuando corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial. (d) Realizar una debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones que se realicen sean consistentes con el conocimiento que tiene la institución sobre el cliente, su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos.

La Recomendación 11 exige que las instituciones financieras mantengan registro de sus operaciones por espacio de al menos cinco años, ello ante posibles pedidos de información por parte de las autoridades competentes.

La Recomendación 15 demanda de los países e instituciones financieras la identificación y evaluación de los riesgos de lavado de activos que pudieran surgir con respecto al desarrollo de nuevos productos y prácticas comerciales, o a partir de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes.

La Recomendación 18 exige a las instituciones financieras la implementación de programas contra el lavado de activos, incluyendo políticas y procedimientos para intercambiar información dentro del grupo para propósitos ALA/CFT.

Las Recomendaciones 24 y 25 sostienen que los países tienen que implementar medidas para impedir el uso indebido de personas jurídicas u otras estructuras jurídicas con fines de lavado de activos.

La Recomendación 26 establece la necesidad de que las instituciones financieras estén sujetas a una regulación y supervisión adecuadas y que implementen eficazmente las Recomendaciones del GAFI.

La Recomendación 28 se refiere a las Actividades y Profesiones No Financieras Designadas, las que deben quedar sujetas a sistemas eficaces para el monitoreo y aseguramiento del cumplimiento de las normas ALA -anti lavado activos-.

La Recomendación 37 trata de la asistencia legal mutua, puntualizando en la necesidad de que los países presten rápida, constructiva y eficazmente, el mayor rango posible de asistencia legal mutua con relación a investigaciones, procedimientos judiciales y procesos relacionados con el lavado de activos.

La Recomendación 38 complementa la anterior, ordenando a los países tomen acción rápida en respuesta a solicitudes extranjeras para identificar, congelar, embargar y

decomisar bienes lavados; productos del lavado de activos y de los delitos determinantes; instrumentos utilizados en, o destinados para ser usados en, la comisión de estos delitos; o bienes de valor equivalente.

La Recomendación 39 sostiene que los países deben ejecutar constructiva y eficazmente, las solicitudes de extradición con relación al lavado de activos.

Finalmente, la Recomendación 40 insta a que los países, a través de sus autoridades, presten el mayor rango de cooperación internacional con relación al lavado de activos y delitos determinantes asociados.

b. El caso de argentina

En nuestro país no existe un marco legal unificado sino diversas regulaciones enfocadas en aspectos relacionados con la operación de los Proveedores de Servicios de Activos Virtuales -PSAV- y con los Activos Virtuales -AV- propiamente dichos.

En materia de lavado de activos, el antecedente legal más destacado lo encontramos en la sanción de la Ley 25.246 (B.O. 10/5/2000), mediante la cual se reformó el Código Penal para tipificar los delitos de LA, se creó la Unidad de Información Financiera (UIF) -organismo autónomo y autárquico que funciona bajo la órbita del Ministerio de Justicia y se encarga del análisis, el tratamiento y la transmisión de información a los efectos de prevenir e impedir el Lavado de Activos (LA), la Financiación del Terrorismo (FT) y el Financiamiento de la Proliferación de armas de destrucción masiva (FP)- y se establecieron las acciones ALA/CFT, particularmente la identificación de los sujetos obligados a informar a la UIF, las acciones de «debida diligencia» (DDC) que deben llevar adelante en materia de «conocimiento del cliente» y de información, análisis y presentación de reportes de operaciones sospechosas (ROS).

Esta norma fue modificada sustancialmente por la ley 26.683 (B.O. 21/6/2011), que produjo una reestructuración integral del delito de lavado de activos de origen ilícito al dejar de regularlo como una de las categorías propias del encubrimiento y establecerlo como un delito autónomo.

Encontramos también la ley 27.430, que modificó el sistema tributario argentino para incluir en el imputado a las ganancias los resultados obtenidos por la enajenación de monedas digitales.

Más recientemente, en lo que considero un avance importante en la materia, se sancionó la ley 27.739 (B.O. 15/3/24), mediante la cual se reformó el *sistema normativo nacional de prevención en lavado de activos y financiación del terrorismo* (LA/FT) y se crearon las definiciones básicas para la regulación y supervisión de los activos digitales o criptoactivos junto con la actividad de sus operadores.

Los ejes principales de la norma incluyen modificaciones al código penal -arts. 41 quinquies, 303 y 306-, a la Ley 25.246 y sus modificatorias -incorporación de los arts. 4 bis, 17 bis, 24 bis, 27 bis, sustitución de los arts. 5, 13, 14, 15, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, modificación del inc. g) del art. 9°, incorporación del capítulo VI, derogación de los arts. 20 bis y 21 bis-, la creación de un registro de activos virtuales (tal como dicho término se define más abajo) y la definición de la figura de los proveedores de servicios de activos virtuales -PSAV-.

A su vez, amplió el catálogo de operaciones que se deben informar a la UIF y dispuso la incorporación de los PSAV, a las personas humanas o jurídicas que realizan, en nombre

de un tercero, custodia y administración de efectivo o valores líquidos, abogados y proveedores de servicios societarios y fiduciarios.

Definió los activos virtuales como una «representación digital de valor que se puede comercializar y/o transferir digitalmente y utilizar para pagos o inversiones».

Creó también el Registro de Proveedores de Servicios de Activos Virtuales, disponiendo que estará a cargo de la Comisión Nacional de Valores -CNV-, ello con el objetivo de centralizar la información sobre individuos y empresas que ofrecen servicios relacionados con Activos Virtuales; y también el Registro Público de Beneficiarios Finales, a cargo de la AFIP, encargado de centralizar información adecuada, precisa y actualizada de aquellas personas humanas que revisten el carácter de beneficiarios finales en los términos definidos en el art. 4° bis de la Ley N° 25.246.

Por otro lado, en lo que respecta a la normativa de jerarquía inferior a las leyes, aparecen las resoluciones de la UIF, entre las cuales cobra especial relevancia la Resolución 300 del año 2014, que en su art. 1° establece que los Sujetos Obligados enumerados en los incisos 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 18, 19, 20, 21, 22 y 23 del artículo 20 de la Ley Nº 25.246 y sus modificatorias deberán prestar especial atención al riesgo que implican las operaciones efectuadas con monedas virtuales y establecer un seguimiento reforzado respecto de estas operaciones, evaluando que se ajusten al perfil del cliente que las realiza, de conformidad con la política de conocimiento del cliente que hayan implementado.

Por su parte, la Resolución General 4614/2019 de la AFIP impone a los sujetos que administren servicios de procesamiento de pagos a través de plataformas de gestión electrónica o digital a cumplir con un régimen informativo mensual sobre sus transacciones, debiendo reportar monto total de los ingresos y egresos, tipo de ingreso (efectivo, transferencia, moneda digital, moneda extranjera), saldo mensual de las cuentas en moneda de curso legal, en moneda extranjera y/o en moneda digital o criptomoneda.

Finalmente, encontramos la Comunicación A 7759 del Banco Central de la República Argentina, que prohíbe a los Proveedores de Servicios de Pago que ofrecen Cuentas de Pago realizar o facilitar a sus clientes la realización de operaciones con activos digitales -incluidos los criptoactivos y aquellos cuyos rendimientos se determinen en función de las variaciones que esos registren- que no se encuentren autorizados por una autoridad reguladora nacional competente ni por el Banco Central de la República Argentina.

c. La situación en la UE

La idea de establecer un marco regulatorio en materia de criptomonedas en la U.E. comenzó alrededor del año 2017, con el auge del Bitcoin. Tanto es así que, al año siguiente, se aprobó la Quinta Directiva contra el Lavado de Dinero (5AMLD), que incluyó a los PSAV -Proveedor de Servicios de Activos Virtuales, o CASP por sus siglas en inglés- dentro del alcance de la legislación AML/CFT de la UE por primera vez.

Esto requirió que los PSAV cumplieran con las mismas reglas que las instituciones financieras tradicionales, incluida la identificación del cliente, la verificación de identidad, el monitoreo de transacciones y la notificación de transacciones sospechosas.

A pesar de esto, muchos proveedores de servicios y activos criptográficos aún no estaban dentro del alcance regulatorio, y estos puntos ciegos dejaban a los consumidores e inversores expuestos a un riesgo sustancial.

Además, algunos estados miembros de la U.E. implementaron sus propias reglas criptográficas, quedando fuera de la regulación actual de la U.E. y generándose una fragmentación regulatoria.

Como resultado, la Comisión Europea comenzó a delinear regulaciones de armonización (MiCA) que se aplicarían en toda la U.E., y finalizó el primer borrador en 2020. Desde entonces, MiCA se ha modificado y mejorado para cubrir todos los tipos de criptoactivos y los posibles problemas que puedan surgir.

El MiCA -Markets in Crypto-Assets por sus siglas en inglés- es el marco regulatorio europeo para los criptoactivos. Se trata de una legislación integral cuyo propósito es establecer reglas uniformes para los emisores de criptoactivos que hasta el momento no han sido regulados por otras normas de la U.E.

Esta legislación abarca una amplia gama de aspectos relacionados con los criptoactivos, como su definición, requisitos de licencia para los PSAV, adopción de normativas para la protección de los inversores y medidas para prevenir su uso para actividades ilícitas.

MiCA entró oficialmente en vigor el 9 de junio de 2023. A su vez, las disposiciones sobre tokens referenciados a activos y tokens de dinero electrónico comenzaron a regir a partir del 30 de junio de 2024, y tendrán aplicación plena desde el 30 de diciembre de 2024.

En definitiva, MiCA establece un marco integral para los criptoactivos en la UE, que abarca la emisión, oferta, negociación y custodia. También introduce requisitos de licencia para los PSAV, establece reglas para las stablecoins, prohíbe el abuso de mercado y refuerza la protección del consumidor.

Esto supone mayores márgenes de certeza para las empresas que trabajan con criptomonedas, creando un sistema unificado en toda la UE, y si bien es muy probable que las regulaciones se vuelvan más estrictas, esto minimizará los riesgos tanto para las empresas como para los clientes.

d. Brasil

En diciembre de 2022, Brasil publicó la Ley 14.478, que proporciona nuevas directrices para los proveedores de servicios de activos virtuales y define los delitos y el fraude utilizando activos virtuales.

En junio de 2023, el presidente Lula da Silva promulgó el decreto gubernamental No. 11.563, por el cual se autoriza al banco central a regular y supervisar a los proveedores de servicios de activos virtuales y garantiza que muchos proyectos simbólicos que califican como valores seguirán estando bajo la competencia de la comisión de bolsa y valores de Brasil.

En mayo de 2024, el Banco Central de Brasil anunció que las propuestas regulatorias para los criptoactivos estarían finalizadas a finales de año.

En el vecino país, si bien las criptomonedas no se reconocen como moneda de curso legal, se pueden poseer, comercializar y utilizar como medio de pago.

e. EEUU

En los Estados Unidos, las regulaciones en materia de criptoactivos varían según el estado. En general, la SEC solo regula las ventas de criptomonedas si 1) constituyen la venta de un valor según la ley estatal o federal, o 2) se consideran una transmisión de dinero según la ley estatal o una acción que convertiría a una persona en una empresa de servicios monetarios según la ley federal.

En lo que respecta a la evolución de ese marco regulatorio, en 2014, el Servicio de Impuestos Internos emitió directrices y esbozó principios generales sobre la tributación de las monedas virtuales.

En 2015, Nueva York se convirtió en el primer estado de EE.UU. en regular las criptomonedas. Desde entonces, muchos estados lo han seguido.

En 2016, la *comisión de comercio de futuros de productos básicos* (CFTC) ejerció por primera vez su poder para exigir que las bolsas de criptomonedas que ofrecen contratos de futuros se registren.

Al año siguiente, Estados Unidos reguló las ofertas iniciales de monedas, que estaban bajo la jurisdicción de la *comisión de bolsa y valores* (SEC), y la SEC publicó un informe en el que se destacaba que los tokens DAO son valores.

En 2018, el *servicio de impuestos internos* (IRS) actualizó las normas fiscales relativas a las transacciones de criptoactivos y estableció una fuerza fiscal sobre delitos fiscales transnacionales y lavado de dinero que cubría los criptoactivos.

El marco AML/CFT del país se actualizó en 2020 con modificaciones a la Ley contra el Lavado de Dinero.

Más recientemente, en 2022, el presidente Biden emitió una orden ejecutiva que ordena a varias agencias tomar medidas significativas para proteger a los consumidores, ampliar el acceso a los servicios financieros, garantizar la estabilidad financiera, combatir las finanzas ilícitas y más. Estados Unidos tiene un mercado de criptomonedas sustancial y ocupa el cuarto lugar en el índice de adopción global de criptomonedas de Chainalysis. El gobierno está considerando numerosos proyectos de ley sobre criptomonedas.

En julio de 2023, la *ley de certeza regulatoria de blockchain* fue aprobada por el comité de servicios financieros. El proyecto de ley «eximiría a ciertos desarrolladores y redes de blockchain de los requisitos de informes financieros y licencias requeridos por las leyes federales y estatales actuales».

Ese mismo mes, la *ley de claridad para las monedas estables de pago* tuvo aprobación por por el comité de servicios financieros de la cámara de representantes. El proyecto de ley serviría como el primer marco regulatorio federal integral sobre las monedas estables.

En igual fecha, la comisión de servicios financieros de la cámara de representantes aprobó la Ley Keep Your Coins. El proyecto de ley «prohibiría a las agencias federales restringir el uso de moneda virtual convertible por parte de una persona para comprar bienes o servicios para el propio uso de la persona y para otros fines».

El 29 de agosto de 2023, el IRS publicó una serie de normas propuestas que «requerirían que los corredores, incluidas las plataformas de comercio de activos digitales, los procesadores de pagos de activos digitales y ciertas billeteras alojadas en activos digitales, presenten declaraciones de información y proporcionen declaraciones de

beneficiarios sobre las disposiciones de activos digitales efectuadas para los clientes en ciertas transacciones de venta o intercambio».

En abril de 2024, se presentó en el senado la ley lummis-gillibrand de monedas estables de pago. Esta legislación propone un régimen regulatorio para las monedas estables, centrándose en la protección del consumidor, las normas AML/CFT y la preservación del dominio del dólar estadounidense.

En mayo de 2024 se aprobó la ley de innovación y tecnología financiera para el siglo XXI, que busca expandir el poder regulatorio de la CFTC, aclarar el papel de la SEC y definir cuándo una criptomoneda es un valor o una mercancía.

También en 2024, el IRS publicó un borrador de su nuevo formulario para informar los ingresos generados por las transacciones de activos digitales, que deberán completar los corredores de criptoactivos a partir de 2025.

En materia de AML/CFT, los intercambios de criptoactivos y los proveedores de servicios deben registrarse en FinCEN, cumplir con los requisitos AML/CFT y reportar cierta información a los reguladores.

f. China

Como contraste con los marcos regulatorios anteriormente descriptos encontramos la situación de China, donde las criptomonedas están virtualmente prohibidas.

El primer paso de China para regular los criptoactivos se produjo en 2013, cuando el Banco Popular de China prohibió a las instituciones financieras negociar con Bitcoin u otros activos virtuales.

En 2017, el gobierno chino prohibió también las ofertas iniciales de monedas y que las bolsas de criptoactivos operaran en China; esto último obligó a muchas bolsas que tenían su sede en China -incluida Binance, la más grande del mundo- a reubicarse.

Más recientemente, en 2021, el gobierno chino prohibió la minería, ilegalizó las transacciones de criptomonedas y bloqueó a las bolsas de criptomonedas extranjeras para que ofrecieran servicios a los ciudadanos chinos.

Sin embargo, si bien estas regulaciones prohíben efectivamente las criptomonedas en China, técnicamente a los ciudadanos chinos se les permite poseer criptoactivos, a punto tal que Chainalysis ubica a China en el puesto 11 a nivel mundial en adopción de criptomonedas.

7. Conclusiones

El auge de las criptomonedas ha revolucionado el panorama financiero mundial, pero también ha introducido nuevos desafíos en la lucha contra el lavado de activos. La naturaleza pseudónima y transfronteriza de las criptomonedas -por mencionar solo algunas de sus características- las convierte en un atractivo vehículo para actividades ilícitas.

El trabajo que nos convoca expone, con meridiana claridad, que la regulación de las criptomonedas representa un desafío complejo que busca, por un lado, prevenir actividades ilícitas como el lavado de activos y, por otro, fomentar la innovación y el uso

legítimo de estas tecnologías. Lograr este equilibrio es fundamental para garantizar la integridad del sistema financiero y, al mismo tiempo, promover el crecimiento económico.

Esta particular visión coincide con lo expuesto por Dellepiane, C. (2019), quien afirma que:

> […] Si pensamos en los diferentes objetos o mercancías que fueron utilizados como dinero a lo largo de la historia, la sal, la cebada y luego las primeras monedas acuñadas, el factor común que les posibilitó cumplir con su función ha sido la confianza, la ausencia de regulación puede ser causa de una posterior degradación de los instrumentos, a medida que se detecten casos de uso ilegitimo.

En tal sentido, se impone la obligación para el Estado de adecuar su legislación, acorde a un mapa de riesgos que permita la adopción de medidas oportunas, ágiles y proporcionales, para la detección de nuevos procedimientos e instrumentos y, acorde con ello, el dictado oportuno de nuevas regulaciones; todo ello, exige la integración de los reguladores con el trabajo de expertos del sector Fintech».

En este contexto, la comunidad internacional ha respondido con una serie de regulaciones diseñadas para prevenir y detectar el criptolavado. Normativas como la Regla de Viaje y los requisitos KYC/AML han sido implementadas en numerosos países, buscando aumentar la transparencia y trazabilidad de las transacciones.

Así entonces, frente al anonimato de las transacciones que va de la mano con la utilización de criptomonedas se deberían implementar medidas de «Conozca a su Cliente» (KYC, por sus siglas en inglés) y/regulaciones anti-lavado (o AML, por sus siglas en inglés), sin sacrificar por completo la privacidad. La tecnología blockchain, al ser un libro de contabilidad público, ofrece oportunidades para rastrear transacciones sin revelar la identidad de los usuarios en todos los casos.

Por otro lado, frente a un escenario global donde existen múltiples regulaciones en la materia se estima indispensable la armonización de tales normativas. En esta armonización juega un papel sumamente relevante el Grupo de Acción Financiera Internacional (GAFI), que ha permitido establecer estándares globales para la reglamentación de los activos virtuales, adoptados por la mayoría de los Estados modernos.

Además, toda vez que el uso de criptomonedas no aparece limitado por fronteras geográficas, la cooperación internacional es esencial, sobre todo cuando se utilizan para actividades ilícitas. Es allí donde el intercambio ágil de información entre los Estados y la coordinación de esfuerzos entre las agencias que aplican la ley y las entidades gubernamentales de diferentes países puede ayudar a prevenir, mitigar y/o sancionar a quienes actúan por fuera de la ley.

A nivel interno, en lugar de aplicar una regulación uniforme a todos los actores del mercado se pueden implementar enfoques basados en el riesgo, supervisando de manera más estricta a aquellos que presentan un mayor riesgo de actividades ilícitas.

Algunas de las herramientas de prevención de lavado de activos más eficaces vienen de la mano del licenciamiento de los PSAV -esto es, exigir a las plataformas de intercambio de criptomonedas y otros PSAV una licencia para supervisión y control de sus operaciones- y la adopción de la Travel Rule -una demanda del grupo GAFI para que los PSAV compartan información relevante sobre el originador y el beneficiario de las transacciones con activos virtuales-.

Sin embargo, la rápida evolución de la tecnología y la fragmentación regulatoria a nivel mundial presentan obstáculos significativos. A pesar de los avances, persisten desafíos importantes, como la proliferación de monedas estables y el desarrollo de protocolos de privacidad más sofisticados, que plantean nuevos retos para los reguladores. Además, la falta de coordinación entre diferentes jurisdicciones facilita que los delincuentes exploten las lagunas legales.

Es por ello que la investigación del delito de lavado de activos mediante el uso de criptomonedas demanda, por parte de los órganos encargados de la persecución penal, una exhaustiva capacitación en la materia que aborde no sólo el estudio de la tecnología de blockchain y las características de las criptomonedas, sino también el conocimiento de las regulaciones nacionales e internacionales en la materia y el proceso debido en materia de preservación e incorporación de evidencia digital al proceso.

En conclusión, el criptolavado representa un desafío complejo y en constante evolución. Si bien se han logrado avances significativos en la lucha contra este delito, es necesario un esfuerzo continuo por parte de los gobiernos, el sector privado y la sociedad civil para desarrollar soluciones innovadoras y efectivas. La clave para combatir el criptolavado radica en una combinación de regulación inteligente, tecnología avanzada y cooperación internacional.

8. Referencias

Adra, R. (2021). *Lavado de activos con criptomonedas: vulnerabilidades de control*. http://revele.uncoma.edu.ar/htdoc/revele/index.php/administracion

Biagosch, Z. A. (2018). La corrupción y la prevención del lavado de activos. En N. Durrieu & R. R. Saccani (Eds.), *Compliance, anticorrupción y responsabilidad penal empresaria* (p. 399). Thomson Reuters.

Botero Bernal, A. (2003). *La metodología documental en la investigación jurídica: alcances y perspectivas*. *Opinión Jurídica, 2*(4), 109–116. https://revistas.udem.edu.co/index.php/opinion/article/view/1350

Carrizo, R. (2003). *Tipificación del delito de lavado de activos de origen delictivo*. *LA LEY*, Sup.Act 08/07/2003.

Corbino, M. (2022). *El lavado de dinero a través de criptoactivos*. http://sedici.unlp.edu.ar/bitstream/handle/10915/137487/Documento_completo.pdf

De Marco, G. (2020). *Criptomonedas y ciberseguridad. Reflexiones sobre la situación regulatoria en el país, con motivo de una reciente decisión del Tribunal Superior de Nueva Zelanda*. *LA LEY*, SJA (15/05/2020), 7.

Dellepiane, C. L. (2019). *Los activos digitales como instrumento del lavado de dinero y financiamiento del terrorismo. Respuestas obligadas desde el compliance y la cooperación internacional*. *Revista de Derecho Empresario*, 1.

Donna, S. A. (2021). *Blockchain, criptomonedas y delito*. *Revista de Derecho Penal Económico: COVID y sus consecuencias jurídico-económicas*, 2021(2). Rubinzal-Culzoni.

Eraso Lomaquiz, S. E. (2015). *Las monedas virtuales en el Derecho argentino. Los Bitcoins*. *LA LEY* 31/12/2015, 1; *LA LEY 2016-A*, 727.

Europol. (2021). *Cryptocurrencies: Tracing the evolution of criminal finances*. Europol Spotlight Report Series. Publications Office of the European Union. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

Faliero, J. C. (2017). *E-lavado de activos: aristas y perspectivas*. *LA LEY*, SJA (31/05/2017), 8.

FATF–GAFI. (2015). *Guidance for a risk-based approach. Virtual currencies*.

Finol de Navarro, T., & Nava de Villalobos, H. (1996). *Procesos y productos en la investigación documental* (2.ª ed.). Universidad del Zulia.

Flores Dapkevicius, R. (2022). *Prevención de blanqueo de capitales con criptomonedas y non fungible tokens (NFTs). Cuál debida diligencia deben realizar los sujetos obligados*. https://cijur.mpba.gov.ar/files/bulletins/Rubén_Flores_Dapkevicius_V2_12-8.pdf

GAFI. (2014). *Monedas virtuales: definiciones claves y riesgos potenciales de LA/FT*.

GAFI. (2015). *Directrices para un enfoque basado en riesgo: monedas virtuales*. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Directrices-para-enfoque-basada-en-riesgo-Monedas-virtuales.pdf

GAFI. (2020). *Recomendaciones del GAFI 2012: Actualizadas a octubre de 2020*. https://www.cfatf-gafic.org/es/documentos/recursos-del-gafic/14971-recomendaciones-del-gafi-2012-actualizadas-a-octubre-de-2020-1

GAFILAT. (2021). *Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales*. https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guía-sobre-aspectos-relevantes-y-pasos-apropiados-para-la-investigación-identificación-incautación-y-decomiso-de-AV.pdf

Gómez Iniesta, D. (1996). *El delito de blanqueo de capitales en Derecho español*. Cedecs Editorial.

González Rossi, A. (2024). *Sobre el Registro de Proveedores de criptoactivos en la Argentina*. *LA LEY*, 29/04/2024, 1; *LA LEY 2024-B*, 316; *Enfoques 2024 (julio)*, 95.

Lansky, J. (2018). Possible state approaches to cryptocurrencies. *Journal of Systems Integration*.

Lara Lara, J. A., & Muñoz Agudelo, M. A. (2017). *Análisis de los principales elementos del Bitcoin como criptomoneda y producto commodity en el comercio nacional*. Universidad La Salle.

Linares, M. B. (2019). Bitcoins: su empleo como técnica para lavar activos ilícitos. En *Temas de Derecho Penal y Procesal Penal* (p. 243 y ss.).

Linares, M. B. (2019). *Criptomonedas y lavado de activos*. *LA LEY*, DPyC (febrero), 213.

Marengo, F. (2011). *Aspectos generales del lavado de activos. El lavado de activos y la financiación del terrorismo. La problemática en el mercado de capitales*. https://www.pensamientopenal.com.ar/doctrina/28927-aspectos-generales-del-lavado-activos-lavado-activos-y-financiacion-del-terrorismo

Martínez, D. M. (2021). *Criptoactivos: ¿Nueva modalidad de lavado de activos?* https://www.pensamientopenal.com.ar/doctrina/89437-criptoactivos-nueva-modaldidad-lavado-activos

Mora, S. J. (2015). *Monedas virtuales: Una primera aproximación al Bitcoin*. *LA LEY*, 31/12/2015, 1.

MPF. (2023). *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos: Consideraciones teórico-prácticas sobre activos virtuales basados en blockchain y su investigación penal*. https://www.mpf.gob.ar/ufeci/files/2023/05/Informe_Criptoactivos.pdf

Navarro Cardoso, F. (2019). *Criptomonedas (en especial, bitcóin) y blanqueo de dinero*. http://criminet.ugr.es/recpc/21/recpc21-14.pdf

Oppel, S. (2022). *Bitcoin: herramientas de análisis para abordar investigaciones penales que incluyan operaciones con esta cripto-moneda. Lineamientos para planificar una actividad cautelar eficiente*. *LA LEY*, DPyC (julio), 75.

Ortíz, J. C. (2020). *Lavado de activos: las monedas virtuales como herramienta del lavado. ¿Su utilización contradice las recomendaciones del GAFI? LA LEY*, DPyC (junio), 37.

Pérez López, X. (2017). *Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y España*. *Revista de Derecho Penal y Criminología*, 18, 141–187. https://core.ac.uk/download/475135308.pdf

Portillo, V. H. (2018). *El delito de ciberlavado de activos*. *LA LEY*, SJA 06/06/2018, 48.

Ruiz Gordillo, F. M. (2021). *La Ley Fintech como medio de prevención del lavado de dinero por parte de las instituciones de tecnología financiera*. *LA LEY*, DPyC (julio), 121.

Sánchez, O. (2017). *Bitcoin: Qué son las criptomonedas y cómo ganar dinero fácil con ellas*. San Bernardino, California.

Silvera Méndez, C. (2019). *Los desafíos ante la presencia de nuevos bienes jurídicos con especial atención en las criptomonedas*. *LA LEY*, DPyC 2020 (febrero), 196.

Skalany, E. G. (2019). *Criptomonedas y Derecho Penal en Argentina: Introducción a la blockchain, el bitcoin y más allá*. En *Enfoques actuales en los delitos contra el patrimonio*. Rubinzal-Culzoni.

Small, S. (2015). Bitcoin: The Napster or currency. *Houston Journal of International Law, 37*, 581.

Spoele, J. (2010). *Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df

Suárez Puga, E. A. (2021). *Naturaleza y régimen jurídico de las criptomonedas*. https://www.pensamientopenal.com.ar/doctrina/89427-naturaleza-y-regimen-juridico-criptomonedas

Unidad de Información Financiera. (2014). *Resolución UIF 300/2014*. https://www.argentina.gob.ar/normativa/nacional/resolución-300-2014-231930

Valdés Trapote, A. (2022). *Estudio sobre la lucha contra el lavado de activos mediante criptoactivos*. https://www.elpaccto.eu/wp-content/uploads/2022/07/Estudio-Lavado-Criptoactivos.pdf

Zoccaro, M. (2020). *El marco regulatorio de las criptomonedas en Argentina*. https://www.economicas.uba.ar/wp-content/uploads/2020/07/El-marco-regulatorio-de-las-criptomonedas-en-Argentina.pdf

Cartapacio
Reseñas bibliográficas y jurisprudencia comentada

Revista Pensamiento Penal
Sección Derecho procesal y procesal penal
Vol. 2, núm. 4 – 2025, págs. 125–139
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/gtm94516

El derecho a la confrontación como fundamento del debido proceso

Comentario al fallo «H. R. (F) c/ B. M. N. s/ homicidio», del Tribunal de Impugnación de Río Negro

Diego Araujo[1]

Resumen

A raíz del fallo dictado el 21 de marzo del año 2024, del tribunal de impugnación de Río Negro, y la alegada violación al derecho de confrontación por parte de la defensa técnica del acusado, se propone un repaso y análisis de las cuestiones relevantes asumidas en el caso. Este análisis tiene como objetivo comprender el efectivo alcance del derecho de confrontación, como derivación necesaria del debido proceso. La confrontación, esencial para asegurar la equidad del juicio, permite a la defensa cuestionar la credibilidad de los testigos, evitando así que se presente evidencia testimonial sin la debida fiscalización. Su violación puede constituir un grave error judicial que afecta la integridad del proceso adversarial y compromete la legitimidad del sistema judicial. Al analizar este caso, es crucial entender cómo se interrelacionan el derecho de confrontación y el debido proceso, y cómo su transgresión puede tener repercusiones significativas en la justicia penal, destacando la importancia de salvaguardar estos principios para garantizar juicios justos y equitativos.

Sumario

Fallo comentado

Tribunal de Impugnación de Río Negro; «H. R. (F) c/ B. M. N. s/ homicidio»; 21/03/2024.

Palabras clave

derecho a la confrontación – error judicial estructural – juicio por jurados – derecho de defensa – debido proceso legal

[1] Defensor oficial del departamento judicial de Azul, sede descentralizada Tandil. Docente universitario, Universidad Nacional del Centro de la Provincia de Buenos Aires (UNICEN). Correo electrónico: drdiegoaraujo@hotmail.com

1. Introducción

En el presente caso, se trata de un examen de admisibilidad de evidencia con contornos bien precisos. En lo particular, se requirió el ingreso de una declaración previa, prestada durante la instrucción de la causa por una persona que entonces revestía la calidad de imputado, a fin de confrontarla en el debate, compareciendo ahora como testigo disponible. La negativa del juez técnico a admitir dicha evidencia impidió la realización de la confrontación.

De allí se abren una serie de cuestiones vinculadas: la entidad del agravio y las garantías vulneradas, el impacto en la decisión y el rol del órgano revisor, que serán objeto de análisis.

En el caso analizado, aunque no siempre sea evidente, persiste esa tensión constante entre la pretensión estatal de responder a la criminalidad y las garantías del imputado.

2. Resumen del hecho y del *iter* procesal

En el contexto de un juicio conformado por un jurado popular consta que se acusó y condenó a «B» por haber causado lesiones de carácter leves en perjuicio de «D.C.» mediante un golpe de puño en el rostro, y por haber luego dado muerte dolosamente apuñalando en el abdomen a «H» mediante la utilización de un cuchillo de fabricación casera.

Mediante sentencia del día 11 de noviembre de 2023 el juez del foro de jueces penales de la 3ra circunscripción judicial, en su carácter de juez técnico del tribunal de juicio, integrado por jurados resolvió, por decisión del jurado popular declara culpable a «B» por el delito de homicidio simple en concurso ideal con lesiones leves culposas, a título de autor, de conformidad con los artículos 79 y 94 en función del 89 y artículos 45 y 55 del código penal, en virtud de la decisión unánime a la que arribara el tribunal integrado por jurados.

La defensa técnica del imputado y la querella impugnaron la sentencia, mientras que la acusación pública se abstuvo de hacerlo, dado que le estaba vedada tal posibilidad por lo dispuesto en la legislación local (arts. 235 inciso 3, con relación a los arts. 228, y 230 del código procesal penal de Río Negro, en adelante «CPPRN»). La querella cuestionó la pena impuesta, inferior a la solicitada durante el desarrollo de la cesura del juicio, cuestión que fue resuelta por mayoría en sentido adverso a dicha pretensión.

La defensa en su escrito de impugnación solicitó al tribunal que declarase la nulidad de la sentencia porque se negó el confronte del testigo «A» con sus propios dichos recogidos durante la investigación del caso. Se adujo así, que esa decisión afectó una garantía constitucional y convencional. Ello con cita en los artículos 8 de la Convención Americana sobre Derechos Humanos y 14.3 e del Pacto Internacional de Derechos Civiles y Políticos.

En el orden local, dicha garantía se encuentra contemplada en el artículo 297 del código de procesal penal federal donde en la parte pertinente expresamente refiere «en el contra examen las partes podrán confrontar al testigo o perito con sus propios dichos o con otras versiones».

La defensa entendió que el testimonio brindado y la confrontación vedada era una cuestión relevante y así lo argumentó en la impugnación. Subsidiariamente planteó la absolución del imputado «B» por arbitrariedad de la sentencia derivada del veredicto de culpabilidad y apartamiento manifiesto de la prueba producida en el debate. Producida la audiencia, se presentaron los fundamentos y explicaciones de la decisión cuestionada, según el artículo 239 del CPPRN, y el tribunal resolvió —por mayoría— rechazar el recurso de la defensa, y dejar subsistente el veredicto de culpabilidad.

El voto en disidencia, en cambio, optó por la anulación del juicio. Entre sus razones, dio por acreditada la existencia de un error estructural al comprobarse la lesión constitucional (al debido proceso), por no permitir a la defensa confrontar la acusación hacia un testigo del hecho. Por ello, consideró que el jurado no podía dar un veredicto válido, pues carecía de los debidos elementos para su deliberación.

3. Los argumentos del tribunal

a. El voto de la mayoría

El voto de la mayoría estuvo integrado por el juez Adrián Fernando Zimmermann y la jueza María Rita Custet Llambí. En primer lugar, señalaron —con remisión a antecedentes propios— la forma y alcance de la doble instancia en un juicio por jurados, así como también sobre los límites que impone la impugnación. Así, abordaron el conflicto planteado con un criterio amplio y comprometidos con la nueva forma de enjuiciamiento.

El enfoque dado al agravio, como veremos, sustentado más en la suficiencia probatoria que en la violación del derecho de defensa, sellaría la suerte del caso.

En efecto, luego de detallar la prueba producida durante el debate, los jueces que integraron la mayoría señalaron que le asistía razón a la defensa en cuanto a que se privó de forma injustificada el uso de la declaración previa de «A» en el entendimiento que el CPPRN no limita ni condiciona a que se realice en tal o cual lugar y/o bajo alguna condición. De manera firme señalaron:

> Acreditados los extremos legales para incorporar en la etapa del control de acusación, será luego tarea del Tribunal técnico o Jurado Popular valorar la credibilidad y la intensidad de la fiabilidad del testimonio para así otorgarle la fuerza convictiva que considere en su relación con el resto de la prueba. La decisión de suprimir dicha declaración, junto con otros dos testimonios —estos últimos sin petición de parte alguna—, con el fin de efectuar una nueva valoración, genera desconcierto (considerando 7 de la primera cuestión resuelta en la sentencia).

En este contexto, y tras valorar el resto de la prueba producida durante el debate, la mayoría consideró que esta resultaba suficiente para establecer, más allá de toda duda razonable, la culpabilidad de «B».

b. El voto de la minoría

Representado por el juez Miguel Ángel Cardella, logra resolver, conforme mi criterio, la problemática suscitada durante el desarrollo del debate de manera acertada. Y ello es consecuencia directa de haberse efectuado la pregunta correcta conforme la naturaleza del juicio adversarial. Recordemos que durante el juicio se le privó a «B» —imputado— la posibilidad de confrontar el testimonio de «A», con una declaración prestada en forma previa por éste; y que el tribunal de impugnación consideró un acto injustificado.

Por ende, lo que debía evaluarse no era, prioritariamente, la suficiencia probatoria de signo acusatorio que, más allá de toda duda razonable, sustentara la decisión del veredicto de culpabilidad. Lo relevante era determinar si ese acto «injustificado», por lo que privó, tenía entidad suficiente para anular dicho veredicto.

El juez Cardella identifica la problemática y la coloca en el centro del sistema adversarial, donde el juez técnico ha de mantenerse esencialmente pasivo siendo el desarrollo del proceso controlado por las partes. Destacó en su voto que el núcleo del juicio adversarial es la confrontación mediante el contraexamen, cuya privación vacía de contenido ese derecho.

Bajo esta premisa, decidió admitir la impugnación de la defensa técnica de «B», al considerar que se había vulnerado el sistema constitucional de enjuiciamiento penal. En consecuencia, anuló el veredicto del jurado, ya que se le prohibió al imputado y su defensa acceder a una prueba directamente vinculada con la teoría del caso.

Aquí, puesto el acento en la imposibilidad de la confrontación, y en su consecuencia el contraexamen, el caso se asimila a lo resuelto por la Corte Suprema de Justicia de la Nación en «Benítez, Aníbal» del 12 de diciembre de 2006[2].

La Corte Suprema de Justicia de la Nación señaló que se vulneró el derecho de defensa al impedir que el imputado tuviera siquiera la posibilidad de controlar o contradecir a los testigos decisivos de cargo que estuvieron ausentes en el debate. Asimismo, advirtió que se desnaturaliza el derecho de defensa al presumir que del contrainterrogatorio —que no fue posible realizar— pudiera surgir un elemento favorable a la defensa o, al menos, la existencia de duda. Por otra parte, sostuvo que la legitimidad del procedimiento de incorporación por lectura puede estar justificada; sin embargo, no resulta suficiente para garantizar el derecho de defensa del acusado, debiendo velar por un uso de dicha prueba respetuoso de aquel derecho.

Finalmente, se enfatizó que el derecho de examinación exige que el imputado haya tenido una oportunidad adecuada y apropiada para desafiar y cuestionar a un testigo o a cualquier persona que hubiera hecho declaraciones en su contra, incluyendo, en este caso, a un coimputado. La consecuencia fue la remisión de la causa al tribunal de origen para que dicte un nuevo pronunciamiento adecuado.

En el presente caso, desde la visión de la minoría, se da una situación que es asimilable, pero esta vez a) la defensa pudo contrainterrogar al testigo relevante presente en la audiencia de debate; b) pero no tuvo la posibilidad de confrontarlo con una declaración previa relevante; c) es decir, se lo privó ilegítimamente de intentar demostrar su falta de credibilidad —conforme su postura—; d) el tribunal no puede constituirse en el jurado

[2] Corte Suprema de Justicia de la Nación, «Recurso de hecho deducido por la defensa de Aníbal Leonel Benítez en la causa Benítez, Aníbal Leonel s/ lesiones graves causa N° 1524C»; 12/12/2006.

número 13, para establecer o suplantar la valoración que le dio —o hubiese dado— a las declaraciones el jurado popular.

Hay en ambos fallos —en este caso en la voz de la disidencia— una construcción garantista del debido proceso —con asiento en una cuestión federal—, basada en la idea de imprescindibilidad de la posibilidad de confrontación de la prueba relevante. Hay también cierta identidad, al coincidir los pronunciamientos, en que no es posible medir el impacto de la infracción al debido proceso ante la imposibilidad de la confrontación, ya que no se lo puede presumir, ni tampoco es correcto mensurar y suplirlo jurisdiccionalmente.

Sin embargo, el magistrado Cardella va más allá y refiere que la decisión del juez técnico de no permitir que el jurado tomara conocimiento de la declaración previa de «A» para el contraexamen constituyó un error judicial estructural que lesiona el debido proceso penal. Ello, al impedir que la defensa confronte la prueba de la acusación.

Destaca así la relevancia del testimonio de «A» y a partir de allí parece establecer que aquel yerro del juez técnico fue de una entidad tal que impidió sostener y desarrollar una razonable explicación alternativa que sirviera de contrapeso de la evidencia de cargo. Y que ello incidió en el veredicto popular.

Además, el juez Cardella advierte sobre aspectos que hacen al ingreso de la evidencia, la necesidad de acceso a la información y la actividad desplegada al respecto por parte de la acusación. Luego, vuelve sobre un aspecto central, el interés del imputado de hacer ver al jurado popular que un testigo había cambiado su versión de los hechos en un tema central. La defensa tenía el derecho de confrontar al testigo «A» (antes imputado), con su declaración realizada en la sede de la Fiscalía.

4. Los contrapuntos particulares

En el caso lo sobresaliente ha sido el impedimento del derecho a la confrontación con el cual ha tenido que lidiar el imputado, y que ha sido detallado pormenorizadamente por el voto de la minoría. Y si bien puede entenderse que dicho concepto no es novedoso, sí lo ha sido entre nosotros el tratamiento dado por el juez Cardella, al adentrarse en el concepto de «error judicial estructural», asimilable en buena medida entre nosotros al vicio *in procedendo* y sus consecuencias.

De la Rúa (2000), expresa que esta distinción parte de la diferente posición en que se encuentra el juez frente al derecho, según sea sustantivo o procesal. Señala el autor respecto del derecho sustancial que el error puede consistir en una errónea valoración jurídica del hecho o en una equivocada interpretación del precepto, en tanto que la violación del derecho procesal se traduce en una contravención al comportamiento exterior que el juez o las partes debían observar al cumplir su actividad. Luego de afirmar entonces que la inobservancia de estas reglas es censurable en casación, refiere que el tribunal debe pronunciar el juicio de derecho, examinando si se trata de una infracción que pueda determinar la nulidad de la sentencia.

Así, como cuando un testigo que declara en el debate se espera que aporte información relevante para el caso, la confrontación permite compulsar esas manifestaciones en aras de establecer la calidad de la información proporcionada, su solvencia y/o nivel de credibilidad.

Cardella destaca cómo el derecho de confrontación se enlaza con el ejercicio del derecho de defensa, y el debido proceso. Señala que se produce su lesión en el momento que se limitó ilegalmente a la defensa del derecho a desacreditar a un testigo, siendo que esa herramienta es fundamental para el ejercicio del derecho a confrontar a los testigos.

Establecido dicho agravio como una lesión constitucional, cita doctrina y jurisprudencia de la Corte Suprema de los Estados Unidos (en adelante, «SCOTUS», por sus siglas en inglés), e incursiona así en lo que la doctrina anglosajona denomina error judicial estructural que anula el juicio. Con expresa referencia al caso «Crawford v. Washington», señala cómo la SCOTUS estableció que los derechos constitucionales son esenciales para garantizar un juicio justo y su relajamiento lo vulnera bajo la violación del derecho de confrontar la prueba testimonial.

El fallo, dice Cardella en su voto, rescata la estructura del proceso en donde se puede cuestionar la credibilidad del testigo bajo el procedimiento del contraexamen (o de otros medios), en donde la confrontación filtra lo confiable de lo que no es. Así, la evaluación de la credibilidad de un testigo implica haber asegurado el pasaje por el «filtro» del contraexamen y que incluye la posibilidad de su compulsa con una declaración previa.

Relacionado con ello, el magistrado Cardella introduce una crítica al razonamiento llevado adelante por la mayoría, al cual lo asimila gráficamente como la asunción postural de un jurado No. 13[3], y su incidencia en las facultades decisorias del tribunal de revisión.

El juez Cardella cuestiona este punto. Sostiene que el análisis debió limitarse a establecer la suficiencia y racionalidad de la información (sin prejuicios y sin sesgos), y no establecer o suplantar la valoración que le dio a las declaraciones el jurado popular. Insiste en la existencia de un error estructural, al decir que la falta de información adecuada debilitó la integridad del veredicto, dado que aquél que se pretendía confrontar se trataba de un testimonio decisivo.

Afirma que, sin superar el filtro procesal del contraexamen, no es posible considerar íntegro el veredicto. Esto se vincula con la idea de que cualquier error procesal que afecte las garantías constitucionales debe ser considerado perjudicial, sin importar las circunstancias.

En consecuencia, un error judicial estructural conlleva la revocación automática de la sentencia condenatoria.

También señala que no es posible determinar si hubo suficiente evidencia para una condena más allá de toda duda razonable, ya que se alteró la esencia del mecanismo procesal: el derecho a confrontar. Con base en el caso «Crawford», concluye que esta alteración vicia todo el juicio.

[3] Ley 5020 de la Provincia de Río Negro (Código Procesal Penal), art. 26, dispone que cuando la pena solicitada por el fiscal supere los doce (12) años de prisión o reclusión, el tribunal debe integrarse con doce (12) jurados titulares y al menos dos (2) suplentes.

5. La cuestión en torno al error

a. Breve reseña

El caso nos ofrece una buena oportunidad para analizar brevemente algunas cuestiones vinculadas al concepto traído por el voto de la minoría. Esto es, el error judicial estructural.

Determinar cuándo un error judicial constituye un supuesto que no puede ser tolerado por un sistema judicial respetuoso de los derechos fundamentales es una cuestión compleja y sujeta a más de una mirada

Describe Grabe (2016) que origen del error como problemática suele ubicarse en el *common law* inglés, donde se debatía entre la automática anulación de las sentencias ante la existencia de un error, y la revocación sólo en casos en que el mismo haya sido sustancial, prevaleciendo en los hechos la primera de las opciones.

Esta dicotomía se trasladó a los tribunales de apelación estadounidenses, quienes aplicaban una regla que se aproximaba a la revocación automática. Al igual que en Inglaterra, donde hubo intentos de acotar la interpretación del error a través de la ley de la judicatura primero y la ley de apelaciones penales después, en 1919 el Congreso de los Estados Unidos promulgó un estatuto federal de error inofensivo, el Judicial Code § 269, 28 U.S.C. § 391[4].

Así el énfasis se situaba en los errores que realmente afectan los derechos sustanciales de las partes involucradas, en lugar de permitir que tecnicismos menores sean la causa para anular o modificar decisiones judiciales.

Esta regla tuvo su réplica en varias normas estaduales, sin embargo, los tribunales de apelación estadounidenses continuaron anulando y revocando las sentencias con gran frecuencia durante las siguientes décadas.

En 1949 se modifican las reglas federales de procedimiento penal puestas en vigencia en 1946[5], en un nuevo intento de regular el error judicial.[6] Aquí, la disposición del error inofensivo seguía el lenguaje de la ley federal de error inofensivo de 1919, pero omitía el descriptor *técnico* antes de la palabra *errores*. Esta modificación buscaba quizás, equilibrar la necesidad de corrección de errores judiciales con la eficiencia del sistema judicial, evitando que errores menores resultaran en la anulación de veredictos y la repetición de juicios innecesarios.

La SCOTUS, en el año 1946, y en el contexto de discusión jurídica que se suscita en derredor del efecto de los errores, resuelve el caso «Kotteakos» (1946), aplicando la regla de 1919. Con base en la existencia de un error judicial no constitucional se declaró que

---

[4] Act of Feb. 26, 1919, Pub. L. No. 65-281, 40 Stat. 1181 (modificando Judicial Code § 269, 36 Stat. 1163 (1911)), disponía: «En cualquier audiencia de apelación, certiorari, recurso de error o moción para un nuevo juicio, en cualquier caso civil o penal, el tribunal deberá dictar sentencia después de un examen de todo el expediente, sin tener en cuenta errores técnicos, defectos o excepciones que no afecten los derechos sustanciales de las partes».

[5] Las reglas federales de procedimiento penal fueron adoptadas por la Corte Suprema el 26 de diciembre de 1944, transmitidas al Congreso por el fiscal general el 3 de enero de 1945 y entraron en vigor el 21 de marzo de 1946.

[6] 28 U.S.C. § 2111 establece: «En la audiencia de cualquier apelación o recurso de certiorari en cualquier caso, el tribunal dictará sentencia después de examinar el expediente sin tener en cuenta errores o defectos que no afecten los derechos sustanciales de las partes».

para afectar derechos subjetivos sustanciales un error debe tener un efecto o influencia importante y dañosa en la determinación del veredicto.

De aquí, y conforme la cita a la cual remite, se permitiría diferenciar entre el error que recae afectando principios constitucionales, cuya consecuencia sería la revocación automática, de los demás errores que deben ser sometidos a la regla del § 269.

Durante los años subsiguientes, y ya con el nuevo estatuto federal sobre error inofensivo ante la existencia de un error constitucional durante el juicio, la corte requeriría un nuevo juicio, mientras que trataba a los demás errores conforme la doctrina del error inofensivo.

En 1967 se llega a la resolución del caso «Chapman» (1967) donde el análisis del defecto denunciado se hace sobre la base del error inofensivo, pero extendiéndose también al error constitucional, aunque con algunos reparos.

No obstante, esa extensión en el nivel de análisis, «Chapman» privilegió los errores constitucionales frente a los no constitucionales. Esto se hizo mediante una exigencia más o menos rígida de la prueba. Es decir, los errores constitucionales provocan la revocación de la condena a menos que el gobierno demuestre que el error fue inofensivo más allá de toda duda razonable.

Para errores no constitucionales, la situación era diferente. En estos casos, la carga de la prueba recae en la parte que alega el error, que debe demostrar su existencia, y eventualmente el impacto perjudicial que el mismo tuvo en el veredicto del jurado.

El nuevo hito relevante con posterioridad lo constituyó el caso «Fulminante» (1991). Allí la SCOTUS, dividida en dos grandes bloques, volvió a la cuestión de si la admisión errónea como prueba, de una confesión obtenida bajo coacción debería estar sujeta a una revisión de error inofensivo según el principio sustentado en el caso «Chapman». Al responder que sí, que ello era posible, la proporcionó un marco para determinar si otros errores constitucionales deberían ser sujetos al mismo análisis[7].

Con estos precedentes, y discusiones suscitadas acerca de la existencia del error judicial en sus diversas formulaciones y sus efectos, en el año 2004 se resuelve el caso citado por Cardella, «Crawford», con la enorme relevancia sobre el derecho a la confrontación que se destacarán más abajo; y posteriormente «González-López» (2006), donde se señaló «la violación de la Sexta Enmienda no está sujeta a un análisis de error inofensivo». La privación errónea del derecho a un abogado de elección, «con consecuencias necesariamente no cuantificables e indeterminadas, califica indiscutiblemente como error estructural»

Como puede observarse, la preocupación acerca del error judicial ha tenido un largo debate a través de la historia procesal en los tribunales de Estados Unidos. Fruto de ello, las diversas posiciones sustentadas en torno al mismo y sus efectos, que se mantienen hoy en día.

[7] La Corte dividió el universo de los errores constitucionales entre errores de juicio —«errores que ocurren durante la presentación del caso al jurado y que, por lo tanto, pueden evaluarse cuantitativamente», ponderados en relación con el resto de la prueba para determinar si su admisión resultó inofensiva— y defectos estructurales en la constitución del juicio. La minoría, citando *Rose v. Clark*, 478 U.S. 570 (1986), sostuvo que la búsqueda de la verdad es central en el sistema de justicia, pero que «ciertos derechos constitucionales no están, ni deberían estar, sujetos a un análisis de error inofensivo, porque protegen valores esenciales que no se vinculan con la función de búsqueda de la verdad del juicio».

b. El derecho a la confrontación

La sexta enmienda de la Constitución de Estados Unidos. consagra el derecho a la confrontación, estableciendo que en todas las causas penales el acusado tiene derecho a carearse con los testigos en su contra y a contrainterrogarlos[8]. Este derecho, de origen histórico, se remonta al sistema judicial inglés y fue adoptado en las Colonias, consolidándose en 1791.

Su finalidad es limitar abusos estatales y garantizar un juicio justo. En palabras de Mercado (2022), se materializa en tres protecciones: (1) el careo cara a cara, (2) el contrainterrogatorio de testigos de cargo y (3) la exclusión de prueba de referencia incriminatoria. El autor citado agrega que también busca asegurar la declaración del testigo bajo juramento, permitir el contrainterrogatorio para evaluar su credibilidad y excluir pruebas de referencia inadmisibles.

A lo largo del tiempo, la jurisprudencia de los tribunales estadounidenses permitió excepciones por razones de política pública. Así en «Inadi» (1986); «Fensterer» (1985); «White» (1992), entre otros casos relevantes. En «Maryland v. Craig», la SCOTUS sostuvo que el derecho de confrontación no es absoluto, lo que amplió las excepciones a su aplicación[9]. Este conflicto entre eficacia estatal y garantías procesales también ha sido debatido en la jurisprudencia local.

El fallo «Crawford» reafirmó la importancia del derecho a la confrontación, estableciendo que el mismo se aplica a las declaraciones extrajudiciales que son de naturaleza testimonial, es decir, declaraciones que son el tipo de prueba que normalmente se ofrecería en el tribunal como testimonio. Como tal, estas declaraciones no pueden ser admitidas a menos que: (a) el testigo no esté disponible y (b) el acusado tenga oportunidad previa de contrainterrogar.

Si no se cumplen estos requisitos, la declaración se considera prueba de referencia inadmisible, incluso si encaja en una excepción a la regla de exclusión.

En conclusión: *a)* El derecho a la confrontación tiene fundamento constitucional. b) Su propósito es garantizar un juicio justo mediante la declaración del testigo en la audiencia de debate. c) Se aplica exclusivamente a declaraciones testimoniales. d) La doctrina vigente en Estados Unidos es la establecida en «Crawford». e) Su vulneración conlleva la revocación automática de la sentencia.

[8] En lo que aquí interesa, la sexta enmienda establece: «En todas las causas penales, el acusado gozará del derecho a un juicio expedito y público, por un jurado imparcial del Estado y distrito en el cual haya sido cometido el delito, distrito que será previamente fijado de acuerdo con la ley; a ser informado de la naturaleza y causa de la acusación; a carearse con los testigos en su contra; a que se adopten medidas compulsivas para la comparecencia de los testigos que cite a su favor; y a contar con la asistencia de un abogado para su defensa».

[9] En ese marco, la Corte reconoció que el derecho de confrontación cara a cara puede ser exceptuado, siempre que se cumplan dos requisitos: (1) la existencia de un objetivo gubernamental apremiante y (2) una garantía adecuada de confiabilidad del testimonio presentado.

c. El *harmless constitutional error* y el error judicial estructural

En las breves notas apuntadas se destaca el caso «Crawford» como relevante en torno a la protección del debido proceso. Sin perjuicio de que allí no se define que es un error estructural, ni tampoco refiere en forma expresa bajo esa denominación la solución que aporta al caso, determina algo esclarecedor y orientador quizás. El objetivo último del derecho de confrontación es garantizar la fiabilidad de la prueba, pero se trata de una garantía procesal y no sustantiva. No exige que la prueba sea fiable, sino que esta se evalúe de una manera particular: mediante la prueba en el tamiz del contrainterrogatorio

En «Fulminante» (1991), la SCOTUS debía determinar si la existencia de una confesión forzada podría analizarse conforme a la doctrina del error inofensivo. Señaló que un error de prueba difería notablemente de las violaciones que son defectos estructurales en la constitución del mecanismo de prueba y, por lo tanto, desafiaban el análisis mediante estándares de error inofensivos, concluyendo en el caso por mayoría -cinco votos- que el análisis de errores inofensivos se aplica a las confesiones obtenidas bajo coerción, y por ende el examen debía ceñirse a la siguiente regla de comprobación «antes de que un error constitucional federal pueda considerarse inofensivo, el tribunal debe poder declarar que cree que fue inofensivo más allá de toda duda razonable».[10]

En «Sullivan» (1993), la SCOTUS señaló además otro supuesto: la impartición de una instrucción de duda razonable constitucionalmente deficiente se encontraba entre esos errores constitucionales que requerían la revocación de una condena, en lugar de aquellos que son susceptibles de un análisis de error inofensivo. Entre nosotros podemos analizar bajo esta tesis el fallo «Brizuela» (2024) del TCBA.

En el caso «González López» (2006) la SCOTUS volvió a examinar la temática. Esta vez ante la denuncia de privación de un abogado de elección, teniendo que resolver si dicha denegación por parte de un tribunal de distrito, le da derecho al acusado a la revocación automática de su condena.

En los casos que he citado hubo mucho debate, y diversas posiciones, y a pesar de lo dicho y de la aparente firmeza de las aserciones sustentadas para fundar la existencia de errores estructurales, la aplicación de dicha regla no siempre se ha mostrado tan diáfana en el caso concreto.

Precisamente, la casuística ha permitido pervivir aquella regla en la que el error judicial pretende ser evaluado de una manera más laxa, teniendo en consideración distintos intereses: el error constitucional no perjudicial o *harmless constitutional error*. Así el TSPC en «Pueblo v Santos Santos» (2012) se ha sostenido que:

> no obstante la gravedad de toda violación constitucional, la determinación de que un error es de naturaleza estructural debe reservarse sólo para aquellas violaciones que lesionen fatalmente la naturaleza imparcial de la totalidad del proceso judicial. Por tanto, si una vez suprimida la prueba admitida erróneamente en este caso (el

[10] La minoría —cuatro votos— sostuvo que un acusado en un caso penal es privado del debido proceso legal cuando su condena se apoya, total o parcialmente, en una confesión involuntaria, sin importar su veracidad o falsedad ni la existencia de otras pruebas suficientes para sostener la condena. Cuestionaron la clasificación de errores propuesta por la mayoría, pero aun así destacaron que existen defectos que, por su gravedad, violan el debido proceso garantizado por la Decimocuarta Enmienda, reconociendo derechos constitucionales tan fundamentales para un juicio justo que su vulneración nunca puede ser tratada como un error inofensivo.
A modo de ejemplo —como en *Chapman*— señalaron: (a) el uso de una confesión forzada contra el acusado en un juicio penal, (b) la privación del derecho a contar con un abogado y (c) la realización del juicio ante un juez parcial

> Certificado de Informe Químico Forense), el resto de la prueba presentada por el Ministerio Público aún logra probar más allá de duda razonable la culpabilidad del señor…, no existe impedimento alguno para que se sostenga su convicción (III.B sexto párrafo de la sentencia).

A riesgo de ser reiterativo, el error inofensivo, además de estar contemplado en las reglas federales y en las normas estatutarias de todos los Estados, ha configurado una doctrina según la cual las sentencias no serán revocadas por errores o defectos que no afecten los derechos sustanciales de las partes.

Dicho de otra manera, no todo error de admisión o exclusión de la evidencia acarrea la revocación de la resolución o sentencia recurrida[11]. En definitiva, el análisis de un caso bajo la doctrina constitucional del error inofensivo será un análisis con sustento en los hechos, y eventualmente de la contingencia en la que los mismos sean presentados[12]. Lo que da lugar a cierta incertidumbre,[13] producto de las diversas interpretaciones que los jueces puedan hacer conforme las normas o reglas que regulen la admisibilidad de la evidencia.

Y aunque el caso «Chapman» estableció un estándar importante en relación con el error constitucional inofensivo, el mismo ha sido objeto de críticas por su falta de claridad y predictibilidad, así como por la expectativa de que no brinde en una serie de casos complejos una protección adecuada de los derechos del acusado.

De allí que «Crawford» haya sido muy bien recibido, y constituido una base sólida, sobre todo respecto de su incidencia en la protección de los derechos fundamentales, especialmente en el contexto del derecho al debido proceso y a la confrontación de testigos en juicios penales

6. Volviendo al caso

En el caso pueden observarse dos puntos de vista de la cuestión problematizada. Una donde parece evaluarse lo advertido con relación a la doctrina del error inofensivo, sostenida por la mayoría, y la otra, desarrollada por la minoría y que se compadece con la teoría del error judicial estructural.

Sin soslayar la complejidad del asunto sometido a juicio, y que aún en el orden del derecho comparado sigue suscitando debates, entiendo que conforme nuestro derecho interno la cuestión es abordable desde la grave afectación del derecho de defensa con directa incidencia en el debido proceso legal.

La remisión del juez Cardella a antecedentes del derecho anglosajón, ha sido muy atinada en orden al muy prolífico y específico desarrollo de la problemática, con relación al derecho de confrontación. Allí radica la riqueza práctica de la cuestión.

---

[11] En *Kotteakos* se cuestionó la idea de generalizar las soluciones al interpretar la regla federal de 1919. La SCOTUS destacó la importancia de diferenciar la naturaleza del error, lo que incidía en la carga de la prueba.

[12] Del voto emitido por el juez Hugo Black en *Chapman*, que lideró la mayoría, sostuvo: «La adopción de cualquier regla de error inofensivo, ya sea la propuesta por la Corte, o por la disidencia, o alguna otra regla, compromete a esta Corte a un examen caso por caso para determinar hasta qué punto consideramos inconstitucional el comentario de un acusado […] influyó en el resultado de un juicio en particular»

[13] Las críticas al estándar de *Chapman* radicaron en su carácter subjetivo y en el amplio margen que otorgaba a la interpretación judicial, además del riesgo de que ciertos errores quedaran sin reparación si los tribunales no los consideraban lo suficientemente perjudiciales para invalidar el juicio.

Pero por otra parte también puede advertirse similitudes en la jurisprudencia de los máximos organismos jurisdiccionales. Ambas cortes supremas, reconocen el debido proceso como garantía fundamental: en Estados Unidos, a través de la decimocuarta enmienda y su vínculo con otros derechos constitucionales; en Argentina, por el artículo 18 de la Constitución y los tratados internacionales de derechos humanos con jerarquía constitucional. (artículo 75 inciso 22).

La Corte Suprema de Justicia de la Nación ha trazado algunas líneas de acción en sus fallos con relación a la salvaguarda del derecho de defensa. Y lo ha hecho de forma categórica: dejando sin efecto la sentencia impugnada y ordenando un nuevo pronunciamiento con arreglo a su decisión[14].

De lo expuesto se advierte el esfuerzo por encontrar límites al poder punitivo del Estado a través de las exigencias procesales. Ello es lo que ha acontecido con el derecho a la confrontación, que rebosa de la vertiente del debido proceso legal. A partir de *Crawford*, y luego en casos posteriores como «Davis» (2006), «Meléndez Díaz» (2009), «Bryan» (2011), «Bullcoming» (2011), la prueba testimonial en el contexto de la cláusula de confrontación y las herramientas provistas para realizar dicha determinación, constituyen una realidad que difícilmente pueda ser opacada.

El caso, ya llegando al fin, suma otra circunstancia igualmente relevante y es consecuencia de la anterior. Si se adopta la tesis de la mayoría en el voto, se debe asumir el dictado de la sentencia conforme una valoración de toda la prueba con relación a los hechos controvertidos.

El problema que se plantea allí es, como bien lo encuadra el voto del Juez Cardella, si es posible asumir en este caso el rol de un jurado nro. 13[15], con indudable referencia a la jurisprudencia de la Corte Suprema de Canadá, en «R. v. W.H.», (2013).

Alguna jurisprudencia nacional, como la Cámara de Casación Penal de Paraná (2023) ha abordado esta cuestión desde otra óptica, haciendo hincapié en la falta de certeza acerca del alcance e impacto de la información mal incorporada y alegada en el juicio, en la formación del veredicto. Lo mismo puede expresarse sobre evidencia que no fue admitida en forma ilegítima. Quizás aquí se haga sentir el peso de lo resuelto en el precedente «Benítez» de la Corte Suprema de Justicia de la Nación, antes citado, cuando señaló que no es posible medir el impacto de la infracción al debido proceso ante la imposibilidad de la confrontación, ya que no puede presumirse.

Toda limitación a la confrontación ya sea que provenga de una mala decisión del juez, o aún de la propia deficiencia de una defensa técnica, que trastoque la estructura del proceso adversarial no hará más que negar en forma arbitraria aquel derecho fundamental, deslegitimando la integridad del veredicto[16].

---

[14] Corte Suprema de Justicia de la Nación, «Vázquez Cipriano s/ Abuso de armas y lesiones-Recurso de hecho», 14/09/1929.

[15] El punto de vista del análisis es especialmente interesante. El magistrado que vota en minoría expresa: «Este Tribunal no puede constituirse en el jurado número trece para valorar la prueba producida. Lo que hacemos es observar si las pruebas tenían la calidad de información suficiente y racional (sin prejuicios ni sesgos) para que un jurado razonable, más allá de toda duda, llegara al resultado que emitió sin necesidad de contar con la declaración de D.A. De ningún modo podemos establecer o suplantar la valoración que le dio a esas declaraciones el jurado. No podemos saber las determinaciones sobre la credibilidad de cada testigo que tuvo el tribunal de ciudadanas y ciudadanos cuando esta actividad se encuentra fuera de nuestra función».

[16] En ese contexto, ya no parece posible validar racionalmente el proceso cognitivo llevado adelante por el jurado popular para fijar su decisión.

La satisfacción de la regla de comprobación se encuentra indisolublemente vinculada a las formas en que los hechos deben ser acreditados. Si esas formas son alteradas significativamente, trastocando la estructura del proceso, y conculcando garantías constitucionales, la decisión acerca de la existencia de los hechos reposará sobre esos defectos, y en su consecuencia las garantías contra la arbitrariedad se habrán visto indefectiblemente rebasadas (Binder, 2014: 24-31).

7. Consideraciones finales

Es indudable que el juzgamiento por jurados populares trajo consigo una dinámica particular modificando el rol del fiscal, del defensor, y del propio juez técnico. La lógica de actuación de cada uno ha mutado, implicando planteos novedosos, cuyas respuestas jurisdiccionales de los tribunales de juicio con jueces técnicos, eran impensables de ser modificadas.

Esta nueva forma de juzgamiento significó un reto a los operadores del sistema penal, y aún genera un campo fértil para capacitaciones con los formatos más diversos en torno a estrategias de litigación penal, ética, desarrollos de destrezas, oratoria y persuasión.

La expresa referencia a jurisprudencia proveniente del derecho anglosajón y las necesarias menciones a doctrinas y/o reglas instauradas en función de aquellas resoluciones, nos invita a participar en nuevas áreas de investigación para la consolidación del sistema. Ejemplo de ello la necesidad de contar con reglas de evidencia, y normas de ética en la litigación.

Este camino que ha comenzado a recorrer fue siendo asumido sin ningún tipo de temor. Son ya varias las provincias argentinas en las cuales se van solidificando criterios frente a las problemáticas suscitadas en los juicios por jurados. Y si bien en términos generales podemos advertir ciertas similitudes en orden a la producción de prueba, pautas para resolver o sistemas de impugnación, las notas peculiarmente conflictivas que se han presentado están siendo abordadas satisfactoriamente, tal como en forma oportuna ocurriera en «Canales» de la Corte Suprema de Justicia de la Nación (2019), «Roldán» (2023), y «Pitman» (2024) ambos de la suprema corte de justicia de la provincia de Buenos Aires o en los relevantes casos del tribunal de casación penal de la provincia de Buenos Aires «Suarez» (2024), «Ocampo» (2025).

El caso comentado nos ofrece la posibilidad de reexaminar la estructura de nuestro proceso penal e identificar aquellas cuestiones que no pueden ser dejadas de lado. Aquellos errores judiciales que parecen socavar el debido proceso, como en el presente caso donde se obturaron en forma dirimente el derecho de confrontación.

La cuestión permanece abierta y en constante debate. La influencia del derecho comparado como consecuencia de la instauración de este modelo de enjuiciamiento nos impone un gran desafío: conocer, entender y lograr armonía. Además, se requiere una sistematización de orden práctico que nos permita como objetivo esencial satisfacer plenamente la garantía del debido proceso legal como nota distintiva del sistema democrático que nos merecemos

8. Bibliografía

Binder, A. (2014). *Elogio de la audiencia oral y otros ensayos*. Coordinación Editorial.

De la Rúa, F. (2000). *La casación penal*. Depalma.

Greabe, J. M. (2016). The riddle of harmless error. *Houston Law Review, 54*(1). University of New Hampshire School of Law.

Mercado, W. S. (2022). Excepciones al derecho a la confrontación cara a cara del acusado. *Revista Jurídica UPR, 85*, 268

Jurisprudencia

Arizona v. Fulminante, 499 U.S. 279 (1991).

Brizuela, S. F. s/ recurso de casación, Tribunal de Casación Penal de la Provincia de Buenos Aires, Sala I, Causa N.º 125445 (IPP 1301-6500-18), 15 de agosto de 2024.

Bullcoming v. New Mexico, 564 U.S. 647 (2011).

Cámara de Casación Penal de Paraná, Provincia de Entre Ríos, *Santini, E. A., Cejas, H. E., Cabrera, G. A., & Mildenberger, A. M. s/ robo agravado s/ recursos de casación*, Resolución N.º 209, Legajo N.º 1963/22, Sentencia N.º 115 (24 de octubre de 2023).

Chapman v. California, 386 U.S. 18 (1967).

Corte Suprema de Justicia de la Nación, *Benítez, A. L. s/ lesiones graves*, Causa N.º 1524 (12 de diciembre de 2006).

Corte Suprema de Justicia de la Nación, *Canales, M. E. y otro s/ homicidio agravado – impugnación extraordinaria, recurso de hecho* (2 de mayo de 2019).

Corte Suprema de Justicia de la Nación, *Rojas Molina, J.*, Fallos 189:34 (17 de febrero de 1941).

Corte Suprema de Justicia de la Nación, *Salvatierra, R. G. y otros s/ daño agravado (art. 184 inc. 5) y amenazas*, recurso de hecho (22 de diciembre de 2020).

Crawford v. Washington, 541 U.S. 36 (2004).

Davis v. Washington, 547 U.S. 813 (2006).

Delaware v. Fensterer, 474 U.S. 15 (1985).

El Pueblo de Puerto Rico v. Santos Santos, A., 185 D.P.R. 709 (2012).

Jaime, T. A. & Villalba, J. C. s/ queja, Suprema Corte de Justicia de la Provincia de Buenos Aires, Causa P. 137.671-Q (12 de marzo de 2024).

Kotteakos v. United States, 328 U.S. 750 (1946).

Maryland v. Craig, 497 U.S. 836 (1990).

Meléndez-Díaz v. Massachusetts, 557 U.S. 305 (2009).

Michigan v. Bryant, 562 U.S. 344 (2011).

Ocampo, R. B. s/ recurso de casación interpuesto por el fiscal, Tribunal de Casación Penal de la Provincia de Buenos Aires, Sala I, Causa N.º 138401 (IPP 0800-26402-17), 10 de julio de 2025.

Pitman, L. L. s/ queja, Suprema Corte de Justicia de la Provincia de Buenos Aires, Causa P. 137.668-Q (12 de marzo de 2024).

R. v. W.H., 2013 SCC 22, [2013] 2 S.C.R. 180 (Can.).

Roldán, J. A. – fiscal ante el Tribunal de Casación Penal – recurso extraordinario de inaplicabilidad de ley, Suprema Corte de Justicia de la Provincia de Buenos Aires, Causa P. 134.954 (3 de abril de 2023).

Rose v. Clark, 478 U.S. 570 (1986).

Suárez, G. A. s/ recurso de casación, Tribunal de Casación Penal de la Provincia de Buenos Aires, Sala I, Causa N.º 124974 (IPP 0201-2872-19), 15 de agosto de 2024.

Sullivan v. Louisiana, 508 U.S. 275 (1993).

United States v. González-López, 548 U.S. 140 (2006).

United States v. Inadi, 475 U.S. 387 (1986).

White v. Illinois, 502 U.S. 346 (1992)

Columnas & Opinión

Revista Pensamiento Penal
Sección Derecho penal
Vol. 2, núm. 4 – 2025, págs. 140–146
ISSN: 1853 – 4554

El delito de proxenetismo bajo la lupa de la garantía constitucional de reserva judicial

Por Rafael Alejandro Villegas[1]

La prostitución, entendida como la prestación de servicios sexuales a personas indeterminadas de manera habitual y a cambio de una retribución económica, nunca fue configurada como delito por la legislación penal argentina. Sin embargo, genera un debate entre las corrientes abolicionista y reservista respecto de la constitucionalidad del artículo 125 bis del código penal en relación con la garantía de reserva establecida en el artículo 19 de la constitución nacional. Desde la perspectiva reservista, dicho artículo vulnera esta garantía al penalizar a quien promueve o facilita la prostitución cuando esta es ejercida de manera libre y plenamente consentida por personas adultas, sin afectar el orden público ni los derechos de terceros. Castigar esa conducta implica una injerencia inadmisible en la esfera privada de quienes optan por modos de vida alternativos y reproduce una concepción paternalista y moralizadora del estado que debe ser rechazada en un sistema respetuoso de las libertades individuales.

*prostitución – proxenetismo – principio de reserva – delitos contra la integridad sexual – abolicionismo*

* * * * * *

a. ¿Qué es la prostitución?

La prostitución es una cuestión que desde antaño ha suscitado fuertes debates en los ámbitos sociales, jurídicos y políticos, acerca de la necesidad, tipo y alcance de la respuesta que debe brindar el Estado ante dicho fenómeno.

i. Concepto normativo de prostitución

En lo que hace al concepto normativo de la prostitución existe cierta uniformidad en la doctrina que la conceptualiza como una actividad que consiste en la entrega sexual habitual, por precio y a personas indeterminadas (Creus y Buompadre, 2007; Molina, 2021; Núñez, 2008; Soler, 1992). Sin embargo, algunos autores no comparten la nota de habitualidad (Aboso, 2015; De Luca; López Casariego, 2009). La entrega sexual implica un trato erótico a partir de a ctos físicos inequívocamente sexuales, no necesariamente con acceso carnal[2].

La habitualidad, el precio y la indeterminación de las personas/clientes

[1] Universidad Nacional del Litoral, Facultad de Ciencias Jurídicas y Sociales. Correo electrónico: rafaelvillegas.abogado@gmail.com

[2] Se emplea el término «físico» como equivalente de «corporal», con el propósito de distinguir aquellas actividades que, aun orientadas a generar placer erótico, no implican contacto corporal directo. Resulta

son elementos inescindibles de la prostitución. La habitualidad no implica cotidianeidad o ejercicio constante; el precio puede consistir en dinero o en otra prestación, beneficios o ventaja con valoración económica; y la indeterminación no implica que la persona que se prostituye deba aceptar todos y cada uno de los clientes que solicitan su servicio, sino que se encuentra predispuesta a aceptar realizar actos sexuales a aquellas personas que estén dispuestas a pagar el precio.

ii. La prostitución ¿es un delito?

Nuestro ordenamiento jurídico no considera a la prostitución como delito, en el entendimiento de que su actividad, en tanto no ofenda al orden o moral pública ni a terceros, encuadra en la garantía de reserva del artículo 19 de nuestra constitución nacional y como acciones privadas están sólo reservadas a dios y exentas de la autoridad de los magistrados. Sin embargo, nuestro sistema castiga todos aquellos hechos que germinan alrededor de la prostitución, por lo que puede considerarse como abolicionista según la clásica división tripartita de los sistemas: *reglamentarista*, *abolicionista* y *prohibicionista*.

b. La modificación del código penal a partir de la ley 26.842

La ley 26.842 ha modificado la tipificación de una serie de delitos relacionados con la prostitución como el proxenetismo, rufianería y trata de personas. Se trata de un avance decidido al castigo de aquellos hechos que implican la explotación sexual de mujeres, al punto tal que en el artículo 125 *bis* CP, en donde se reprime a quién facilita o promueve la prostitución de una persona, se elimina la distinción antes existente entre mayores y menores de edad, considerándose esta última circunstancia como agravante del tipo regulado en el artículo 126 CP, a la vez que resta todo tipo de importancia al consentimiento de la víctima.

Sobre este punto, la doctrina ha debatido intensamente sobre la constitucionalidad de la figura. Y es que, a partir de la última reforma, la ley presume sin prueba en contrario que el ejercicio de la prostitución viene precedido por una situación de explotación o aprovechamiento de la vulnerabilidad de la mujer, que le impide por sí consentir de manera libre la prestación de servicios sexuales a terceros por un precio.

c. Una discusión irreconciliable. Reservistas vs abolicionistas

i. La tesis reservista

Un sector de la doctrina que llamaré reservistas, (Aboso 2015; Arocena 2024; Buompadre, 2021; Molina, 2021) entiende que la figura, así como está redactada resulta reñida con el principio de reserva establecido en el artículo 19 de nuestra constitución, ya que al castigar a aquellos que faciliten o promueven la prostitución voluntaria de personas mayores de edad, presumiendo sin prueba en contrario la explotación y sin exigir ningún tipo de medio intimidatorio o de aprovechamiento de la vulnerabilidad de la prostituta, restándole toda eficacia a su consentimiento como sujeto de derecho plenamente capaz, el Estado adopta una postura paternalista y moralizadora que traspasa el límite previsto por nuestra constitución, resultando así un exceso punitivista injustificado.

Para la tesis reservista, resulta un contrasentido imaginar una situación de explotación consentida libremente por la persona que ejerce la prostitución. Y es que basta una simple lectura de los artículos 125 *bis* y 126 del CP para advertir que quien facilita o promueve la prostitución utilizando medios violentos, intimidatorios o aprovechándose de situaciones de vulnerabilidad, o en caso de que la víctima

necesaria una revisión contemporánea del concepto de prostitución, considerando las nuevas modalidades de prestación de servicios sexuales de manera virtual mediante plataformas digitales, entre ellas *OnlyFans* o *Cafecito*.

sea menor de edad encuadran en el tipo agravado, por lo que quedarían incluidas en el tipo genérico del artículo 125 *bis* las conductas de promoción y facilitamiento de la prostitución a personas mayores de edad que han consentido libremente la actividad. Ello resulta además reñido con el principio de lesividad. Sobre éste, es sabido que, a partir de la teoría de los bienes jurídicos, el legislador castiga aquellas conductas que lesionan o ponen en peligro determinados intereses merecedores de tutela. Ahora bien, los reservistas afirman que en el artículo en cuestión no se puede advertir con claridad cuál es el bien jurídico que se estaría lesionando o poniendo en peligro. Si bien la ubicación sistemática del tipo hace presumir que el bien jurídico es la libertad sexual o autodeterminación sexual de la persona que ejerce la prostitución, no se advierte cómo puede lesionarse la autodeterminación en el ámbito de lo sexual de una persona mayor de edad que libremente ha consentido el servicio sexual por un precio, a raíz de ciertas conductas que *per se* no pueden reputarse abusivas, como lo son el facilitamiento de un inmueble para que la prostituta pueda ejercer su actividad o la publicidad de los servicios sexuales a fines de conseguir potenciales clientes.

ii. La tesis abolicionista

Para otro sector de la doctrina, que llamaré abolicionistas, (De Luca y Lancman, 2013) el artículo 125 *bis* CP encuentra el fundamento de la punición en la especial situación de explotación y degradación de la dignidad humana que existe en toda entrega carnal a terceros indeterminados a cambio de un precio. Esta tesis rechaza la idea de que existe una *prostituta feliz* (sic) que ingresa y sale del mercado sexual cuando desea y que consiente de manera libre y pacífica su actividad. Esta postura, que coincide con los fundamentos de la reforma, sostiene que sobre toda la actividad de la prostitución subyace un tipo de explotación sexual del hombre por sobre la mujer, a partir de la cosificación de su cuerpo como mercancía a los fines de satisfacer los impuros designios del varón por dinero (Binder, 1986). En este sentido, toda conducta que tiende a la promoción o facilitamiento de este tipo de actividad, produce un intolerable menoscabo o denigración de la dignidad de la mujer como ser humano, por lo que merece ser castigado.

Los abolicionistas hacen una diferenciación sustancial en lo que hace al consentimiento. Consideran que, si bien existe consentimiento en cada trato sexual individual, lo que impide que se configure el tipo de abuso sexual con acceso carnal, no existe consentimiento en sentido global, porque la prostitución en si es degradante en el sentido de la dignidad humana y desde un punto de vista psicológico. El bien jurídico tutelado, el cual es la autodeterminación sexual de la persona, no se encuentra disponible para su titular cuando el trato sexual se da en el marco de una transacción económica y no por placer, en el sentido afectivo y erótico de la palabra.

iii. Postura ecléctica o intermedia

Las posturas reservistas y abolicionistas son irreconciliables. Es más, consideramos que se trata de una cuestión que no puede plantearse en términos eclécticos, intermedios o mixtos. Se debe tomar postura acerca de la constitucionalidad o no de la figura debido a que no existen normas más o menos constitucionales. Las normas son constitucionales o no. Esa lógica se traslada a un debate, que, sumado a las dimensiones morales, religiosas, sociales y políticas del asunto, encrudece las posiciones y está lejos de cerrarse. Mientras tanto, la norma penal está vigente y urge ser interpretada para su aplicación en la realidad. Y dicha interpretación, principalmente por los jueces, debe tener en cuenta la constitución nacional y los tratados internacionales con jerarquía supralegal, en atención a su obligación de realizar el control difuso de constitucionalidad y convencionalidad.

d. Reconstrucción histórica del artículo 125 bis del código penal

Para analizar el tipo del artículo 125 *bis,* considero saludable empezar por el principio, es decir por su antecedente

histórico inmediato, ya que entender cómo fue formada inicialmente la norma y en qué contexto, nos dará una primera y valiosa pauta de análisis para luego avanzar en la comparación de la norma actual respecto de la garantía de reserva, previa vista de las reformas que fueron operando.

i. La cuestión en el código penal original

El código penal de la república argentina original -ley 11.179 vigente desde 30/04/1922- regulaba en el libro segundo «de los delitos» título III «delitos contra la integridad sexual» en el capítulo III «corrupción, abuso deshonesto y ultrajes al pudor» el tipo penal del artículo 125, que la doctrina penal denominó delito de proxenetismo, que castigaba a «el que con ánimo de lucro o para satisfacer deseos propios o ajenos, promoviere o facilitare la prostitución, o corrupción de menores de edad, sin distinción de sexo, aunque mediare el consentimiento de la víctima[…]» renglón seguido establecía las circunstancias que habilitaban y agravaban la punición según la edad del niño o niña.

Y, por último, la circunstancia de que existiese engaño, violencia, amenaza, abuso de autoridad o cualquier otro medio de coerción, así como el vínculo de parentesco o encargado de la educación, agravaba la pena de 10 a 15 años, sin importar la edad de la víctima, pero requiriendo siempre el medio violento o intimidatorio.

Resulta valiosísimo el artículo 125 del código penal original, ya que las posteriores reformas del código, con variadas finalidades y objetivos políticos-legislativos, han girado en torno al mismo. Prueba de ello, es que el código penal vigente[3] tipifica ambas figuras históricamente reguladas en un mismo artículo, de manera separada: la corrupción de menores en el artículo 125 y el delito de proxenetismo en el artículo 125 *bis* y su agravante en el artículo 126[4].

Y digo que resulta sumamente valioso, porque el legislador del año 1921, castigaba a quien promovía o facilitaba la prostitución de menores de edad, sin distinción de sexo y sin darle relevancia al consentimiento del menor, en tanto y en cuanto el proxeneta o alcahuete, persiga un ánimo de lucro o satisfacer los deseos propios o ajenos. Y en el caso de los mayores de edad, sólo castiga al proxeneta que para promover o facilitar la prostitución ajena, utilizaba determinados medios comisivos violentos o intimidatorios, o en caso de vínculo parental o de guarda con la víctima.

Y esto resulta llamativo, repárese un momento sobre la sociedad argentina a principios del siglo pasado. Una sociedad masculina y misógina, en donde (sin miedo de caer en anacronismos) existía una aberrante e injusta desigualdad de derechos y trato entre la mujer y el varón. Una época signada por discusiones jurídicas desopilantes: se llegó a discutir sobre si la prostituta podía ser o no sujeto pasivo del delito de violación porque carecía de honestidad (Felini y Sansone, 1999), o si la mujer casada debía soportar el abuso sexual o el coito violento de su marido debido al débito conyugal (Soler, 1992).

Y es que, bajo este paradigma machista y retrógrado, el legislador argentino tomó la decisión de distinguir entre mayores y menores de edad, y sólo castigar el proxenetismo a mayores de edad cuando existan especiales situaciones de explotación como son los medios violentos o intimidatorios. Es decir, que el acto de promover una actividad como la prostitución en principios del siglo XX, en tanto se desarrolle de manera consentida por una mujer adulta, resultaba impune por ser atípico, en el entendimiento de que la

[3] La denominación de «código» se entiende como histórica, dado que la legislación penal argentina dista de constituir un conjunto sistematizado y coherente de normas jurídicas; posiblemente se utilice el término como una expresión aspiracional respecto de lo que se esperaba que el Código fuera en algún momento.

[4] La distinción entre los delitos de proxenetismo y corrupción surge de la ley 25.087. Actualmente, sigue vigente el delito de facilitamiento y promoción de la corrupción de menores, ya que no se contempla la corruptela voluntaria de un adulto, dado que resulta ilógico concebir a una persona mayor como objeto de actos corruptores.

prostitución debía ser tolerada, y en tanto se mantenga en los márgenes de la salubridad y el acato al orden público, resultaba exenta del poder de los magistrados.

Ello debería llevar a una profunda reflexión. ¿Cómo puede ser que, en la cúspide de una sociedad patriarcal, existía una concepción sumamente liberal de una actividad reprochable desde el prisma moral sigloveintesco? Mientras que nuestra ley penal vigente castiga el acto de promover o facilitar la prostitución voluntaria de mujeres adultas sin ningún tipo de medios intimidatorios o violentos, incluso cuando estas consientan de manera libre el ejercicio de una de las profesiones más antiguas conocidas por el ser humano. ¿Qué fue lo que sucedió en el medio?

En el medio sucedieron varias reformas, pero ninguna fue tan drástica como la ya mencionada ley 26.842 del año 2012, que le quitó toda relevancia al consentimiento de la persona mayor de edad en el ejercicio de su prostitución como circunstancia excluyente de la pena a quien le facilite o promueva su actividad. He aquí lo intolerable de la reforma.

e. *El artículo 125 bis como reflejo del punitivismo utópico*

i. La expansión del derecho penal

El artículo 125 *bis* es el fiel reflejo del punitivismo utópico, en donde el legislador pretende combatir el delito desde su asiento, aumentando las penas, creando nuevos delitos y bienes jurídicos, desdibujando las barreras de lo no punible y en última instancia arrasando contra todo lo que se considera un obstáculo, incluidas garantías y derechos humanos (Silva Sánchez, 2001). Además, implica el inesperado retorno del Estado a una postura paternalista y moralizadora, que alecciona a base de violencia institucionalizada el cómo se debe vivir. Esto conculca con principios tan básicos como la pluralidad de estilos de vida en una sociedad que se dice llamar democrática. Y como si fuera poco, el tipo penal consagra una presunción *iure et de iure* de la situación de explotación y vulnerabilidad de la mujer prostituta, que en términos jurídicos resulta una *rara avis* en la construcción típica, por no decir que resulta una aberración en términos de política legislativa. Y es que el derecho penal no puede construir sus tipos basándose en presunciones, si quiere salvaguardar garantías elementales como el estado de inocencia o al menos la taxatividad del tipo legal. Es tan grosera la reforma, que los abolicionistas admitirían ciertas excepciones, o al menos considerarían que existen contadas situaciones en donde la pena resulta injusta por no configurarse en los hechos la situación de explotación de la prostitución ajena. Piénsese en un locador que alquila su inmueble a una prostituta para que ésta ejerza su actividad. El artículo 125 *bis* permite subsumir esta conducta y castigar a este «infame proxeneta» a la pena de prisión no excarcelable de 4 años como mínimo. Es una pena ridícula, hasta graciosa, pero sobre todo demuestra lo peligroso que resulta el legislador cuando abraza el punitivismo y comienza a ser un gestor de la moral.

ii. El ejercicio de la prostitución como acto privado

Nuestros constituyentes de 1853 construyeron la garantía de los actos privados justamente para evitar estas indebidas intromisiones. En el ámbito de reserva es donde el ser humano desarrolla su personalidad, y no cabe el castigo de dichos actos en tanto no ofendan a la moral pública o a terceros. Según el maestro Bidart Campos ofenden a la moral pública aquellos actos que generen un peligro real y actual a las buenas costumbres, incitando conductas inmorales similares o estimulando deseos de imitación (Bidart Campos, 1980). El ejercicio de la prostitución, en tanto se desarrolle en un ámbito privado por personas adultas de manera libre y consentida, no resulta reñido ni por asomo a la moral pública.

Todas las personas tenemos derecho a la autodeterminación en el ámbito de lo sexual, de modo que somos libres para consentir o repeler actos de contenido sexual, según

nuestros propios deseos y razones, y en tanto no ofendamos a terceros ni pongamos en peligro otros bienes jurídicos, esas razones (como por ej.: placer, costumbre, necesidad de procrear, oportunidad de ganar dinero o cualquier otra razón) quedan reservadas a Dios, o si se quiere, a nuestra propia consciencia.

El consentimiento en el ámbito sexual es enteramente disponible para las personas adultas, éste puede prestarse y retirarse en todo el acto sexual. Considerar que estas no tienen capacidad para consentir actos sexuales por dinero u otro beneficio es absurdo ya que las razones que llevan a la persona a realizar actos sexuales no le deben interesar al derecho. Admitir aquello impide considerarla como sujeto de derecho por denegarle la disposición de un bien jurídico tan íntimo y personalísimo como lo es la libertad sexual, y por ende se trata de una violación arbitraria e injustificada de sus derechos humanos.

Por lo demás, si existiese explotación por parte del proxeneta o bien un aprovechamiento de situaciones de vulnerabilidad a través de medios intimidatorios o violentos, la pena estaría plenamente justificada, en tanto la acusación logre probar dicha circunstancia en el proceso penal, y no que se presuma dicha explotación sin posibilidad de probar lo contrario. De allí que le asiste razón a la tesis reservista, cuando afirma que el artículo 125 bis CP se ha vaciado de contenido, pues las conductas merecedoras de pena se encuentran tipificadas en el tipo agravado (artículo 126 CP) al exigir estos medios comisivos como la intimidación, abuso de autoridad, violencia o minoridad de la víctima.

f. Conclusión. De lege ferenda

Tipos penales como el analizado, son intolerables ya que socavan las garantías del debido proceso y el estado de inocencia, pilares inderogables de un estado de derecho, y deberían ser revisadas y/o suprimidas en una futura reforma penal.

g. Bibliografía

Aboso, G. E. (2015). Capítulo X: Promoción y facilitación de la prostitución ajena. En J. C. Faira (Ed.), *Derecho penal sexual: Estudio sobre los delitos contra la integridad sexual* (1.ª ed., pp. 367-386). Euros Editores.

Arocena, G. A. (2024). ¿Castigar la facilitación de la prostitución consentida de personas mayores de edad? Trabajo sexual, dignidad humana y autonomía personal. *Anuario del Centro de Investigaciones Jurídicas y Sociales, XXII*, 5-22.

Bidart Campos, G. J. (1980). Capítulo 2: Moralidad pública. En G. Bidart Campos (Ed.), *Poder de policía de moralidad en materia de espectáculos y publicaciones en la Capital Federal* (1.ª ed., pp. 55-56). Municipalidad de la Ciudad de Buenos Aires.

Binder, A. (1986). Pornografía, dignidad humana y represión cultural. *Revista Doctrina Penal: Teoría y práctica en las ciencias penales, 9*, 621.

Buompadre, J. E. (2021). Delitos contra la integridad sexual. En J. E. Buompadre (Ed.), *Derecho penal: Parte especial* (3.ª ed. ampliada, pp. 220-223). Editorial ConTexto.

De Luca, J. A., & Lancman, V. A. (2013). Promoción y facilitación de la prostitución. *Revista Pensamiento Penal. Código Penal Comentado.*

De Luca, J. A., & López Casariego, J. (2009). Promoción o facilitación de la prostitución de mayores de edad. En J. L. Depalma (Ed.), *Delitos contra la integridad sexual* (1.ª ed., p. 161). Editorial Hammurabi.

Fellini, Z., & Sansone, V. (1999). La mujer en el derecho penal argentino. *Anuario de Derecho Penal 1999-2000*, 1-29.

Martínez, C. I. (2024). Facilitar la prostitución ajena: Un análisis normativo sobre las razones que justifican la punición del artículo 125 bis del Código Penal. *Revista Argumentos.*

Molina, G. (2021). Promoción y facilitación de la prostitución. En G. J. Molina (Ed.), *Manual de derecho penal: Parte especial* (1.ª ed., pp. 307-312). Editorial ConTexto.

Núñez, R. C. (2008). Capítulo III: Promoción y facilitación de la corrupción y de la prostitución y delitos conexos. En V. F. Reinaldi (Actualizador), *Manual de derecho penal – Parte especial* (3.ª ed. actualizada, pp. 132-136). Lerner Editora S.R.L.

Silva Sánchez, J. M. (2001). Sobre algunas causas de la expansión del derecho penal. En J.-M. Silva Sánchez (Ed.), *La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales* (2.ª ed. revisada y ampliada, pp. 25-74). Civitas Ediciones S.L.

Soler, S. (1992). Violación, estupro y abuso deshonesto. En G. J. Fierro (Actualizador), *Derecho penal argentino (Parte Especial, Tomo III)* (4.ª ed., 10.ª reimpresión, p. 309). Tipográfica Editora Argentina.

Columnas & Opinión

Revista Pensamiento Penal
Sección Razonamiento probatorio y ciencias forenses
Vol. 2, núm. 3 – 2025, págs. 147–152
ISSN: 1853 – 4554

Análisis reconstructivo del delito

Por Cintia Belén Rojas[1]

La importancia del enfoque reconstructivo en el análisis del lugar del hecho, entendido como un proceso técnico-científico orientado a la búsqueda de la verdad fáctica. Se propone superar la fragmentación disciplinar habitual en la práctica pericial, integrando los indicios dentro de un sistema causal que permita comprender la dinámica del suceso delictivo. La metodología reconstructiva se apoya en la observación, la experimentación y la inferencia racional, pilares del método científico aplicados a la criminalística. Desde esta perspectiva, la labor pericial adquiere un valor epistemológico central: reconstruir el hecho implica ordenar la evidencia, establecer relaciones de causalidad y garantizar la objetividad en el análisis. Este abordaje contribuye a fortalecer la fiabilidad de las conclusiones forenses y la función probatoria de la ciencia en el proceso penal.

reconstrucción del delito – pericia – método científico – evidencia forense – verdad fáctica

* * * * * *

a. Introducción

En el análisis del lugar del hecho, es necesario realizar un abordaje desde una perspectiva integral reconstructiva, la naturaleza sistémica de los elementos allí hallados producidos por la acción delictiva debe ser considerada. El planteamiento de una metodología investigativa de carácter reconstructiva nace de la carencia en la bibliografía latinoamericana, donde se observa una abundante cantidad de manuales de criminalística, separados en capítulos dotados de una predomínate especificidad de las diferentes disciplinas forenses, haciendo una descripción de características, propiedades y conceptualizando el análisis de la evidencia forense de forma no asociativa con el conjunto de la evidencia procesada, recolectada y preservada.

De la misma forma, esto se reproduce en el momento de llevar a cabo la labor pericial por parte del personal técnico-científico que auxilia a justicia en la investigación, caracterizados por un procesamiento pericial que se desarrolla en pasos delimitados. El lugar del hecho se procesa mediante la identificación de la evidencia, asignándole códigos alfanuméricos, documentación escrita, planillas preimpresas, croquis a mano alzada con medidas longitudinales, fijando la ubicación de la evidencia y su geolocalización, registro fotográfico, se recolecta, se embala, se resguarda mediante cadena de custodia.

Estas acciones desarrolladas de forma automatizada en la labor diaria pericial en

[1] Perito forense. Correo electrónico: periciasforens@gmail.com

muchos casos se realizan de manera repetitiva y constante, sin considerar la excepcionalidad, el carácter de unicidad e invariabilidad propio que se presenta, por ser el lugar del hecho único e irrepetible.

b. Interrogantes de la investigación criminal

«¿Entender la mecánica del fenómeno delictivo, para aproximarse al interrogante como sucedió?» Es llevar a cabo inferencias lógicas deductivas e inductivas, a fin de generar hipótesis aproximadas de cómo aconteció ese suceso. Esto genera una coherencia lógica con los elementos hallados, los cuales deben ser concordantes con los principios científicos de las disciplinas que componen las ciencias forenses.

Existe una interrelación en la disposición de cada elemento hallado, que debe observarse dentro de un único sistema, no caer en el error de sobrevalor los resultados por separado. Reconstruir la materialidad del ilícito, permite encontrar más rastros del delito, es cuestionarse como ir más allá de la recolección de lo que allí es evidente a los sentidos.

Fomentar la búsqueda desde esta perspectiva integral es intentar inferir el fenómeno delictivo desde sus tres variantes etimológicas diagnósticas de muerte violenta (accidentes, homicidios, suicidios) permitirá conectar secuencias causales de producción de los indicios, desde la formulación de preguntas y la utilización de principios rectores sostenidos por las teorías de análisis de eventos (Bevel & Gardner, 2008).

Es un proceso multidimensional que involucra la exploración de causas, contexto, cronología y motivaciones. Generar una estructura de conocimientos indispensables para la validación del dictamen pericial criminalístico interdisciplinario, partiendo desde las relaciones de causalidad, organización, justificación que hacen a la integración de la evidencia, como una unidad, dentro de los parámetros de admisibilidad de la prueba. (Daubert v. Merrell Dow Pharmaceuticals, Inc., 1993).

c. Constatación del presunto hecho delictivo

La correcta preservación del lugar del hecho, va a influir en el resultado que arroje el análisis pericial. Este espacio físico debe ser resguardado por aquellos primeros intervinientes hasta la llegada de los peritos. Este primer interviniente se convierte en el «primer eslabón» de una cadena de actos que tendrá como finalidad el desarrollo de una investigación para lograr la aproximación a la verdad de cuándo, dónde, cómo, con qué y quién, realizó la comisión de un acto ilícito. Son quienes van a realizar una primera intervención parcial sobre el estado original de los indicios producidos, en determinados casos, a fin de auxiliar a heridos junto con personal médico, o resguardar evidencia ante condiciones climáticas que pongan en riesgo las propiedades de rastros observados y/o elementos descartados por los autores.

Se pueden producir modificaciones que afectarán a los resultados de exploración *in situ* y análisis en los correspondientes laboratorios. Por ello es imprescindible la instrucción y el constante fortalecimiento de conocimientos científicos basados en preservación de la evidencia, para que la función que cumple sobre la preservación de la intangibilidad del lugar del hecho tenga el tratamiento adecuado.

Como regla general, se debe ser cauteloso en su manipulación, usando protección de bioseguridad, adecuando la inmovilización de los elementos e informar a víctimas allí presentes, sobre futuros análisis a realizar sobre el Lugar del hecho. Por desconocimiento en muchos casos, se manipula por parte de la víctima la evidencia, tras sufrir actos traumáticos como pueden ser homicidios, robos calificados, secuestros entre otros. El aislamiento debe ser inmediato a su arribo, impidiendo el acceso de cualquier persona hasta la llegada del grupo pericia.

d. Principios de base reconstructiva

Se parte de cinco interrogantes a responder para el análisis del lugar del

hecho. se enumeran para una mejor comprensión metodológica, pero estas preguntas no deben entenderse con un orden especifico.

El interrogante (1). «¿Quién?» Me permite establecer identificaciones, autores del ilícito, participes, identificación de víctimas, es la herramienta para vincular elementos y personas dentro de espacios físicos determinados enlazando dicho interrogante con:

(2). «¿Dónde sucedió?» Es un espacio físico determinado donde ocurrió el suceso, se lo parcializa para ser analizado exhaustivamente, delimitándolo dentro de un periodo de tiempo específico.

(3). «¿Cuándo sucedió?» Es una aproximación de una franja horaria, en la cual se corroboran acciones que componen la materialidad del delito.

Las acciones que componen la materialidad del delito producen cambios en el estado de las cosas, mediante la utilización de agentes propios (armas de fuego) o impropios (herramientas, objetos etc.) para causar una lesión en la víctima, causarle la muerte y llegar a su propósito, se intenta determinar:

(4). «¿Con que lo hizo?» En muchos de los casos no es encontrado el elemento usado para la agresión, y considerando que la realización de la operación de autopsia es posterior al análisis in situ. Cuando se realiza la observación en lugar del hecho, ese momento de la investigación puede permitir encontrar gran cantidad de indicios materiales, reforzar la búsqueda y potenciar las herramientas para llevar a cabo una observación minuciosa. Esto será posible si se intenta entender la evidencia en su conjunto, preguntarse y repreguntarse posibles variables de ese mismo hecho.

Al observar la disposición de la evidencia procesada mediante su fijación, en el contexto en que ocurrió el crimen, se podrá inferir posibles movimientos, considerando la naturaleza dinámica que caracteriza al resultado material del ilícito, Según Chisum y Turvey (2011):

> La Dinámica del Crimen es esencial: considerar cómo los eventos se desarrollaron a lo largo del tiempo y cómo las acciones de las personas involucradas interactuaron entre sí. La reconstrucción debe tener en cuenta la secuencia de eventos, los movimientos de los individuos y cómo estos factores pueden haber influido en la evidencia encontrada.

Es importante integrar la evidencia en su conjunto, realizar asociaciones de producción y causalidad, para responder aquellos interrogantes mencionados. Preguntarse por qué esa evidencia hallada está ahí, entender su naturaleza, el dinamismo dado por los movimientos de los actores, acciones, posiciones que se sucedieron.

e. Metodología de la investigación científica

La materialidad del delito es de carácter objetivo, es información relevada por medios técnicos- científicos, sostenidos por principios y teorías que fundamentan su formación, producción y disposición al suceder el crimen. El método a seguir es examinar el lugar del hecho donde se cometió un acto ilícito de forma integral.

Ejemplificación 1. Analizar un hecho presuntamente delictivo, donde el cadáver es hallado en un avanzado estado descomposición, sin lesiones visibles superficialmente. Esto complejiza la búsqueda. Se tiene una única e irrepetible oportunidad de buscar la evidencia en su conjunto para poder dar con el agente posiblemente utilizado en la agresión.

El lugar se puede analizar nuevamente en ampliaciones para reforzar búsquedas, pero no solo es el paso del tiempo como lo establecido en su premisa Locard, E. (1935) «tiempo que pasa es la verdad que huye».

Es considerar que, en pericias ampliatorias del abordaje pericial primario, también influye, el paso de la presencia del primer grupo pericial, que recolecto y movió elementos durante la búsqueda. En muchos casos, esta segunda búsqueda es satisfactoria porque se da con el hallazgo de evidencia

que se encontraba oculta, a consecuencia de la poca visibilidad, o en áreas de difícil acceso o con información complementaria obtenida de la operación de autopsia.

Ejemplificación 2: Se encuentra un cadáver próximo a un cuchillo, se evidencian de forma superficial sus lesiones, aquí es importante individualizar el contexto en el cual el cadáver fue hallado, como fue producida la agresión, observar indicios de planificación, corroborar la disposición de los muebles, daños existentes o no, relación entre las distancias de hallazgo de evidencia, análisis de patrones de manchas de sangre que permitirán comprender tipo de fuerza involucrada, dirección en la que se aplicó esa fuerza, naturaleza del objeto utilizado, número aproximado de golpes, movimientos, posiciones.

Reconstruir el crimen es estructurar la información científica criminalística, respondiendo al interrogante «¿cómo sucedió?» La finalidad de este interrogante es comprender la integración del suceso, como los elementos se interrelacionan y dan como resultado la materialidad ilícita.

El fenómeno en su materialidad física, los cambios de estado en el contexto en el que se produce, se convierte en evidencia objetiva reproducible. Que sea de carácter físico hace a su aspecto científico, ubicándolo dentro del área de las ciencias fácticas-naturales, elementos observables y con capacidad de ser examinados y verificados cuando se requiera su reproducibilidad.

Principios reconstructores que considerar uno de ellos es el *principio de causalidad*, establece que las cosas no ocurren de forma aislada «es la relación necesaria existente entre causa y efecto».

Esa relación entre acontecimientos, procesos, regularidad de los fenómenos y la producción de algo, Bunge (2012). En su acepción más amplia, dice que algo es causa de un efecto, cuando el último depende del primero tanto lógicamente, como cronológicamente. Encontrar el orden de prelación de los indicios, ayudara a ordenar las acciones que constituyen la formación del delito, construir una estructura de secuenciación de incidentes allí producidos. Todo lo que allí se encuentra tiene una causal determinada. Se establece un orden de prelación de deposición de la evidencia, que permite generar una aproximación temporal, dentro de un orden cronológico para acotar espacios temporales y aproximarnos con precisión a la hora de ocurrencia.

El forense debe investigar por medio de las diferentes disciplinas científicas, cual fue el modo de producción. La materia cambia cuando se produce una interacción con otros objetos: descubrir los cambios en el lugar del hecho es esencial. Puede suceder que, ya sea por intencionalidad mediante maniobras de ocultamiento, por negligencia de manipulaciones accidentales, o factores de la naturaleza, condiciones climáticas o cronológicas por el paso del tiempo, se produzcan alteraciones. Pero mediante un abordaje metódico desde una perspectiva integral del hecho, es posible acceder a la verdad fáctica.

La simple recolección de evidencia sin una coherencia lógica, que se encuentra afectada por una especificidad de las disciplinas criminalísticas, por condicionantes de sesgos contextuales, por la falsa creencia de la existencia de estar ubicado dentro de un lado en el proceso de investigación judicial, hacen a la pérdida de objetividad.

La ciencia es una; las teorías que sustentan la evidencia científica forense son demostrables y corroborables. La interacción entre el espacio físico, sujetos involucrados (víctima y victimario), dentro del principio de causalidad produce efectos, que son examinados por medio de las bases del conocimiento científico. Con un método y procedimientos establecidos, los analistas deben describir lo observado, basados y guiados por los estudios de sus disciplinas, por los principios que reconstruyen la dinámica del crimen.

Se deben poder explicar el hallazgo, la vinculación de indicios, y no sesgarse por comentarios de funcionarios intervinientes. El perito no debe utilizar demasiado el sentido de la escucha en lugar del hecho, ya podría ser contraproducente para la

investigación. Su función es: «descripción de las personas, lugares, cosas o hechos examinados en las condiciones halladas, una relación detallada de las operaciones practicadas y sus resultados, sus conclusiones basadas conforme a los principios de su ciencia, técnica o arte»[2]

Sesgarse con comentarios que no cumplen con caracteres del método científico, es imprudente, este sentido de la escucha afecta al desarrollo de la correcta observación de la inspección ocular, que debe cumplir con condiciones de objetividad e imparcialidad. «escuchar» es perjudicial para el correcto acercamiento hacia inferencias secuenciales, este actuar caracterizado por recolectar sin razonar, individualizar sin vincular, afecta a la investigación, genera interpretaciones erróneas, carece de objetividad y puede desviar el camino hacia la verdad de lo ocurrido.

El compromiso del carácter técnico-científico de los peritos debe estar basado en el entendimiento que se está frente al relevamiento de la materialidad del delito como lo explica Bunge (1977):

> El intento de alcanzar la verdad fáctica verifica la adopción de las ideas a los hechos, recurriendo a la observación y el experimento a fin de ser controlable y reproducible. La inferencia científica es una red de inferencias deductivas (demostrativas). Lo observado, procesado como evidencia, no se amontona caóticamente, sino en un sistema de ideas; esto es, un conjunto ordenado de proposiciones.

El abordaje debe ser guiado desde la interpretación metodológica con la premisa que cada evidencia se vincula a otra, en un sistema de acciones producidos por el atacante en el proceso dinámico delictual, esto fue mencionado por uno de los propulsores del área reconstructiva de las investigaciones criminales «el principio de intercambio», establecido por Edmond Locard en su libro manual de técnica policiaca «*quiscumque tactus vestigia legat*» («*cualquier presencia en un lugar deja vestigios*»).

Este principio de transferencia, establece que cualquier presencia en un lugar deja y se lleva vestigios, sean éstos visibles o no. Planteando en su teoría la obligación de analizar cuidadosamente el lugar del crimen, aseverando la presencia de vestigios. Adelantándose en el tiempo a los análisis biológicos, entomológicos, microscópicos, químicos y toxicológicos, en una afirmación casi futurista o predictiva en su tiempo. (Locard E., 1935).

Entender la relación causal de cómo la producción de actos ilícitos produce efectos en el mundo material que permite corroborar la existencia de los autores, participes, y la descripción de sus mecanismos al emplear los medios para cometer el delito. «El trabajo en la escena de un crimen debe ser pausado, amplio y escrupuloso» (Verdú *et al.*, 2006).

f. Conclusión

La interpretación sistémica permite, la obtención de resultados verificables y la construcción conocimientos sólidos. En el ámbito forense, esta metodología se convierte en una herramienta esencial para analizar evidencia y desentrañar misterios ocultos en el escenario del crimen.

Las ciencias forenses, a su vez, representan la concreción del método científico en el ámbito judicial. Desde la recolección de pruebas en el lugar del incidente hasta el análisis minucioso en laboratorios especializados, la ciencia forense abraza cada etapa del método científico. La identificación de patrones, la reconstrucción del hecho y la deducción de conclusiones se convierten en elementos clave para resolver crímenes y establecer la verdad. La labor pericial está orientada a la recolección de la evidencia, acentuándose la

[2] Artículo 250 del Código Procesal Penal de la Provincia de Buenos Aires

problemática existente donde la metodología para llevar a cabo dicha recolección, no cumple condiciones de articulación y vinculación lógica entre los indicios. Al momento de ser levantadas, se opera bajo principios generales que sustentan las disciplinas de forma fragmentada. Careciendo de una reconstrucción conceptual sistémica que propicie una aproximada hacia la búsqueda de la verdad y permita plantear una teoría de la mecánica delictiva, para responder el interrogante de como sucedió. -

La finalidad del presente documento es generar una irrupción del carácter metodológico, a fin de que el procesamiento del lugar del hecho, que se realizado por peritos criminalísticos encargados de desarrollar este de tipo de conocimiento, para aquellos institutos que tienen la responsabilidad de capacitación y demás áreas a fines, logren comprender la importancia del papel reconstructivo de la evidencia y su abordaje metodológico en base a una lógica de relevamiento que propicie a las futuras conclusiones periciales.

Se da por olvidado, no es enseñado con las exigencias encuadradas del método científico como fundamento, donde no se entrena mediante casos prácticos, los elementos de racionalidad y objetividad que le son propios para llevar a cabo una reconstrucción. El método científico impone la búsqueda de la objetividad y la reproducibilidad, principios cruciales en las ciencias forenses:

«La imparcialidad en la recolección y el análisis de evidencia garantiza la fiabilidad de los resultados, fundamentando así las decisiones judiciales en hechos verificables y no en conjeturas» (Raffo, 2009).

Bibliografía

Bevel, T., & Gardner, R. M. (2008). *Bloodstain pattern analysis: Third edition with an introduction to crime scene reconstruction*. CRC Press.

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Bunge, M. (1960). Causality and modern science. *Nature, 187*(4732), 123–124. https://doi.org/10.1038/187123a0

Locard, E. (1935). *Manual de técnica policiaca* (J. Moneto, Trad.). Maxtrol.

Miranda, M. D. (2021). La huella en la técnica: La ciencia forense y la mirada del conocedor. *Sinergia de Ciencia Forense Internacional, 3*, 100203. https://doi.org/10.1016/j.fsisyn.2021.100203

Raffo, O. H. (2009). *Tanatología: Investigación de homicidios* (1.a ed.). Universidad de Buenos Aires.

Chisum, W. J., & Turvey, B. E. (2011). *Crime reconstruction* (2nd ed.). Elsevier.

Innett, M. R., & Brooks, J. (2000). The significance of the principles of stratigraphy in forensic science. *Forensic Science International, 112*(1), 11–18. https://doi.org/10.1016/S0379-0738(00)00233-3

Argentina. Ley No. 11.922. Boletín Oficial N.º 23.280, 23 de enero de 19.

.

Columnas & Opinión

Revista Pensamiento Penal
Sección Derecho procesal y procesal penal
Vol. 2, núm. 4 – 2025, págs. 153–161
ISSN: 1853 – 4554

La víctima en el proceso penal cubano. Principales limitaciones

Por Melvis González Figueroa[1] & Leaned Matos Hidalgo[2]

La presente contribución analiza el papel que desempeña la víctima en el proceso penal cubano, a partir de los principales cambios introducidos en la legislación nacional tras la reforma. En este sentido, se examinan las distintas formas de participación reconocidas por la ley del proceso penal, que permiten a la víctima intervenir procesalmente como testigo, tercero coadyuvante, acusador particular o parte civil. No obstante, la ley No. 143 de 2021 —ley del proceso penal— también establece determinadas pautas que pueden limitar el alcance de su actuación.

*derechos de las víctimas – garantías constitucionales – derecho comparado – acusación particular – reforma procesal*

* * * * * *

a. Introducción

La víctima como sujeto es tan antigua como la humanidad, después de ser excluida y marginada por un largo tiempo, reaparece como uno de los exponentes principales del proceso penal para poder lograr una equidad entre cada uno de los sujetos que intervienen. La situación de la víctima en un proceso penal cubano estaba limitada solamente a su participación como testigo en el esclarecimiento de los hechos, y a la acusación particular cuando se trataba de un delito de injuria o calumnia, donde intervenía como querellante y, además, podía ejercer la acción penal en los casos en los que el tribunal estimaba injustificada la solicitud de sobreseimiento libre formulada por el fiscal.

A raíz de todos los cambios normativos que se han venido dando en la isla, este sujeto procesal, se ha sido redimensionado y ahora es titular de una serie de derechos y garantías que le permite una mayor participación en el proceso y que le aleja de situaciones de victimización secundaria. En esa misma línea se debe analizar el contenido y alcance de ese estatus procesal solvente, del cual goza la víctima en nuestros días, sin dejar de percibir que la principal limitante al pleno ejercicio de sus derechos son los propios derechos del imputado/acusado, cuya posición procesal no debe verse disminuida por la participación de la víctima en el proceso penal.

Partiendo de lo antes expuesto el objetivo central de esta investigación ha sido determinar las diferentes formas y

[1] Estudiante de derecho. Alumna ayudante de la asignatura Derecho procesal penal.
[2] Licenciada en derecho. Diploma en formación de fiscales. Diploma en Derecho penal. Especialista en Derecho penal. Profesora auxiliar del departamento de Derecho de la Universidad de Granma. Correo electrónico: lmatosh@udg.co.cu

posibilidades de participación de la víctima, así como los límites de su intervención en el proceso.

b. Desarrollo

i. La víctima como sujeto del proceso penal. Generalidades

Durante muchos años se concibió la idea de que el proceso penal tenía por finalidad servir de instrumento para demostrar la inocencia o culpabilidad de un individuo ante la comisión de una conducta considerada como delito, y así poder aplicar el derecho penal conforme a las garantías. De esta forma, la víctima estaba marginada del proceso penal, limitándose solamente a intervenir como testigo; aún y cuando no estaba conforme con la acusación interpuesta por el fiscal debía aceptarla sin otro recurso procesal que sirviera para exponer su inconformidad, resultando ser sometida a maltratos durante todo el proceso, provocando, en disímiles ocasiones, una victimización secundaria.

Hasta la consolidación de la *victimología*[3], la víctima había sido totalmente despreciada por el derecho penal, el derecho procesal penal, la política criminal e incluso por la criminología.

Gracias al papel que ha desempeñado la victimología, se ha acordado reconocer, además, la tutela de los derechos de las víctimas como un nuevo fin del proceso penal. Esta idea se concibe sobre basamentos psicológicos, en los cuales se considera que, si la persona afectada por la conducta delictiva es partícipe de todo el proceso de investigación y además forma parte de la acusación, se pueden evitar situaciones de revictimización, constituyendo así un método sanador para la víctima.

De esta forma se entiende que el proceso penal defiende las garantías tanto de las víctimas como de las comisiones de delito, es decir, que no solo está a disposición de los imputados o acusados, sino también de las víctimas, logrando mantener una perfecta armonía entre ambas finalidades[4]. Jurídicamente la víctima la relacionamos con la figura del perjudicado, que muchas veces será el sujeto pasivo del delito y el cual necesita que le indemnicen los daños causados, que bien pueden ser físicos o morales[5].

La víctima durante todo el proceso tiene una especial intervención que ha sido reconocida a raíz de la nueva reforma, partiendo desde la Constitución de la República desembocando en la ley del proceso penal (en adelante, «LPP»). Este nuevo sujeto procesal está en plena formación y desarrollo.

ii. Variantes legislativas y garantías constitucionales en la participación de la víctima tras la reforma

Con el movimiento internacional que aboga por el reconocimiento del rol de las víctimas en el proceso penal, se generaron importantes reformas legislativas que pretenden introducir derechos a favor de las víctimas en las legislaciones cubanas, tomando como pauta fundamental alejarlas de dichas situaciones de calamidad que suelen sobrellevar a diario y evitar se continúe desoyendo a la misma durante todo el proceso.

Muchos ordenamientos jurídicos han reconocido nuevos derechos que permiten a determinadas partes intervenir directamente en el proceso penal, integrándolas en la aplicación de las leyes para garantizar la justicia. Nuestro país no ha sido ajeno a estos cambios, y considero que adoptar esta evolución ha sido la mejor decisión. No podemos aferrarnos al pasado; el derecho

[3] La *victimología* —derivada del inglés victimology— es una disciplina cuyo origen se remonta a mediados del siglo XX, especialmente con los aportes de Hans von Hentig, autor de la obra *The Criminal and His Victim* (Archon Books, Hamden, Connecticut, 1979), publicada originalmente en la Universidad de Yale.

[4] Véase Sanz (2008, p. 63) y Planchadell (2016, p. 120).

[5] *Diccionario Espasa escolar de la lengua española* (Espasa-Calpe, 1996), voz «víctima»

avanza a nivel global, y nosotros no debemos ser la excepción.

Por esta razón, la reforma constitucional incorporó una serie de garantías que permiten a las víctimas participar en el proceso. Al mismo tiempo, se dejó espacio para que el resto de las normas, como la ley 143 y la ley 147, establezcan las pautas necesarias para materializar este avance, ampliamente respaldado por la doctrina.

Por ello, los artículos 94 y 95 de la Constitución de la República hacen referencia a estas garantías, estableciendo el derecho de las personas a obtener reparación por daños materiales y morales, así como la correspondiente indemnización por los perjuicios sufridos. Además, garantizan la protección para el ejercicio de estos derechos en caso de que una persona sea víctima en un proceso penal (artículos 94 «h» y 95 «i»). Este último derecho, en particular, permite a la LPP incorporar disposiciones destinadas a prevenir la victimización secundaria, incluso cuando su aplicación es directa.

La víctima dentro de la ley 143 LPP. La Constitución de 2019 fortaleció el sistema de justicia penal, que exigió la promulgación de leyes que permitieran la aplicación de los principios de la tutela judicial efectiva y el debido proceso[6], y la renovación y ampliación de los derechos y garantías de los intervinientes en estos asuntos. Para el desarrollo de estos postulados constitucionales, fue necesario actualizar la legislación vigente y ofrecer a la víctima o perjudicado del delito un papel protagónico, como sujeto-parte en la relación jurídico-procesal, con todos los derechos que implicaba ese reconocimiento; entre ellos, la escucha de sus criterios y la protección requerida.

La armonización de estos derechos tuvo su expresión en las leyes 143 y 147 del 2022 (del proceso penal y del proceso penal militar, respectivamente). En estas leyes se concreta el concepto de víctima y su participación dentro del proceso penal.

Allí se califica como víctima o perjudicado a toda persona natural o jurídica que, como consecuencia de un delito, haya sufrido un daño físico, psíquico, moral o patrimonial (artículo 139, ley 143 LPP). Cabe destacar que estas leyes no hacen distinción entre víctima y perjudicado; pero el tribunal supremo popular, haciendo uso de su facultad legislativa y con el fin de lograr una mayor efectividad en la aplicación de la norma adjetiva, emitió la instrucción 277 de 2023, en la cual sí se alcanza a distinguir a la víctima como la persona afectada de manera directa, y al perjudicado, como la persona que sufre de manera indirecta los efectos del actuar ilegal.[7]

Ambas leyes procesales promueven el respeto a la dignidad de la víctima o el perjudicado, la protección a su intimidad, el derecho a ser informado de los hechos y de las circunstancias que lo rodean y a ser indemnizados por los daños ocasionados por el comisor. También se ofrece la posibilidad de establecer acuerdos reparatorios con los procesados, recibir asistencia jurídica e interponer recursos o proceso de revisión contra las resoluciones judiciales.

Pero sin lugar a dudas la mayor novedad de la reforma procesal, y la que menos se ha proyectado en la práctica, son las nuevas formas de intervención que alcanzó la víctima en el proceso penal. Es así que en la ley 143 le dedica un título a este nuevo sujeto (en el libro segundo, título VI «la víctima o perjudicado»), dándole la posibilidad de acceder a la justicia.

[6] «El debido proceso es un derecho fundamental complejo, de carácter instrumental, continente de numerosas garantías de las personas y constituido en la mayor expresión del derecho procesal. Se trata de una institución integrada a la Constitución que posibilita la adhesión de unos sujetos que buscan la tutela de sus derechos» (Agudelo, 2005, p. 2)

[7] Instrucción No. 277 de 2023, *Gaceta Oficial de la República de Cuba*, No. 14 (Edición Extraordinaria), 17 de febrero de 2023: «…la víctima es la persona natural sobre la que recae la acción directa del comisor, y el perjudicado, aquella, natural o jurídica, que sufre de manera indirecta los efectos del delito, por lo que tal consideración depende del caso concreto…».

La nueva intervención de la víctima en el proceso penal cubano. La intervención de la víctima como testigo no es algo novedoso, es un papel que viene sosteniendo desde hace muchos años, pero, aun así, el legislador cubano no dejó pasar la ocasión para introducir cambios. De manera que en la nueva ley adjetiva la víctima o el perjudicado puede solicitar que su declaración se realice de manera privada, con los representantes legales de las partes y que esta sea filmada y exhibida en el juicio oral sin necesidad de su presencia física, pero siempre tratando de lograr la mayor indemnidad posible; asimismo, cuando declaren, la autoridad actuante debe procurar no afectar la salud mental de esta. Este método fue diseñado para todas aquellas personas que son víctimas de algún delito de violencia de género o familiar, o que se encuentra en estado de vulnerabilidad (artículo 141 «j» de la LPP).

El tribunal, para garantizar el respeto a las víctimas o perjudicados, o a sus familiares, puede disponer la celebración del juicio en privado, y suspenderlo si estas enferman, no asisten o les es imposible permanecer en el referido acto. De igual modo, tienen derecho a mostrar su desacuerdo con los integrantes de la Sala o sección actuante (artículo 21 «c» de la LPP); y a presenciar la práctica de las pruebas, después de haber prestado declaración como testigo.

Además, se amplió la gama de medidas cautelares que permiten la seguridad a la víctima durante todo el proceso, y que el imputado no evada la responsabilidad por sus actos, entre las cuales figuran: la prohibición de acercamiento a la víctima, perjudicado, familiares o personas allegadas, la prisión provisional, la reclusión domiciliaria, la prohibición de salir del territorio nacional, vender determinados bienes, el pago de la fianza en efectivo, etc.

La víctima ya no es solamente un testigo, sino que también puede constituirse como parte en cualquier momento procesal[8], designando un defensor, el cual comunica la decisión de su representado a la autoridad actuante, quien debe informarle sus derechos y aceptar tal petición mediante resolución (artículo 141 «g» ley 143).

Una vez constituida como parte podrá revisar las actuaciones, proponer pruebas a las autoridades para esclarecer los hechos, interponer recursos contra resoluciones judiciales, proponer causas de nulidad, adherirse a la pretensión resarcitoria presentada por el fiscal o ejercer la acción civil de forma independiente en el mismo proceso penal y participar como coadyuvante junto al fiscal (artículo 142 ley 143); y de esta manera podrá presenciar el desarrollo del juicio oral desde el inicio.

Cumpliendo con los preceptos constitucionales que permite a la víctima participar en el proceso se le ha facultado para que intervenga como «querellante adhesivo o coadyuvante»[9] (posición doctrinal que asumió el legislador cubano), el cual garantiza la participación de la víctima en el ejercicio de la acción penal pública al tiempo que neutraliza los riesgos de desigualdad atribuidos al modelo del querellante conjunto o autónomo[10]. Su participación como coadyuvante de la acusación junto al fiscal no impiden que este goce de cierta autonomía procesal, ya que le permite ejercer cierto control sobre la acusación «desburocratizando la actuación

[8] Instrucción No. 277 de 2023. *Gaceta Oficial de la República de Cuba*, No. 14 (Edición Extraordinaria), 17 de febrero de 2023: «…la intervención en un hecho delictivo, mediante la instructiva de cargos, momento en que la víctima o el perjudicado podrán intervenir como parte en el proceso»

[9] La figura del «querellante adhesivo o coadyuvante» se caracteriza por permitir que la víctima ejerza una actuación dependiente y accesoria de la acusación pública: solo puede intervenir bajo esa condición si el fiscal ha promovido la acción penal pública, y su actuación procesal estará limitada, en lo esencial, por el contenido y alcance de la imputación oficial.

[10] El «querellante conjunto o autónomo» posee plena autonomía para ejercer la acusación en paralelo y con independencia del fiscal. Este modelo —adoptado en sistemas como el español— implica la existencia de dos acusaciones frente a una única defensa (Maier, 2003, p. 661)

de la fiscalía»[11], ofreciendo mayores garantías de transparencia, y mayores incentivos para que la víctima colabore con el esclarecimiento de los hechos, lo que incide positivamente en la eficacia de la persecución penal.

Como coadyuvante, podrá ofrecer una calificación distinta del hecho y del grado de intervención que en él tenga el acusado, solicitar la apreciación de circunstancias agravantes o reglas de adecuación no pedidas por la acusación, así como interesar una respuesta jurídica más intensa que la pedida por el fiscal.

La víctima como acusador particular tampoco es novedoso, ya que estamos acostumbrados a que, en los delitos de injuria y calumnia, sea este quien realice la acusación. Pero gracias a la reforma procesal, esa acusación particular ha evolucionado y se logró ampliar su alcance de actuación hasta otros escenarios.

En la LPP, se recoge su participación como acusador particular (artículos del 424 al 427; y 436 de la LPP) bajo presupuestos muy detallados. Solo podrá ejercer la acusación de manera particular cuando el fiscal solicite, al tribunal, el sobreseimiento definitivo de las actuaciones y este lo considere injustificado. Si una vez que el tribunal advierta al fiscal del error que puede acarrear archivar definitivamente las actuaciones y este persiste en su decisión, pues entonces aquel le informa a la víctima y le precisa su derecho de ejercer la acción penal de manera particular y que este lleve el proceso hasta la conclusión del momento cumbre, esta acusación la hará con las mismas formalidades y posibilidades que posee el fiscal.

Si durante el juicio oral, el fiscal retira la acusación que llevaba sosteniendo hasta entonces, y la víctima se mostrase inconforme con esta decisión puede ejercer la acusación particular, pues es un derecho que le será instruido por el tribunal en ese momento (artículo 549 de la LPP). Esta intervención también se va a dar cuando la víctima o el perjudicado no esté de acuerdo con los criterios de oportunidad que haya convenido el fiscal con el imputado (artículo 141 «h»; 18.3 de la LPP).

Visto de otra manera, fuera de la intervención de la víctima como acusador particular en los delitos de injuria y calumnia, este solo tendrá la posibilidad de ejercer la acción penal cuando la actuación del fiscal amenace con poner fin al proceso y aquel no se encuentre conforme.

Como sujeto procesal, la víctima, posee también, la facultad de ejercer la acción civil, dentro del mismo proceso, de manera independiente; cuando estando constituido como parte no se encuentre conforme con la exigencia de la responsabilidad civil al imputado, por parte del fiscal. Es decir que se le está dando la posibilidad de ser ella personalmente, junto a su representante legal, quien exija al comisor del delito por los daños causados, bien sean físicos, morales o patrimoniales (artículo 142 «e» y 459 de la LPP).

Nuestra LPP definitivamente ha aflorado novedosos cambios en el proceso penal, que demuestran el avance del ordenamiento jurídico cubano, cumpliendo siempre con las expectativas de la doctrina.

iii. Principales limitaciones impuestas a las nuevas formas de intervención de la víctima en el proceso penal

Los derechos de las víctimas frente a las garantías de los imputados. Durante largos años se hizo sonar la voz de la doctrina jurídica y de abogados por el reconocimiento de los derechos y garantías de los imputados, así como el respeto fiel a las mismas. Sus reclamos fueron escuchados, y a día de hoy gozan de una amplia gama de derechos constitucionales que les garantizan que el proceso llevado en su contra sea transparente. Es así que en el artículo 95 de la Constitución de 2019 se hace referencia a tales garantías. En el artículo antes mencionado se le otorga el derecho de disponer de representación letrada, que se le presuma inocente en tanto se demuestra lo

[11] La garantía de transparencia constituye una de las funciones que la doctrina alemana atribuye a la figura del actor accesorio (*Nebenklage*). Véase Planchadell (2016, pp. 52–53)

contrario mediante sentencia firme, a no declarar contra sí mismo y a ser informado sobre la imputación en su contra; solo por mencionar algunas[12].

Pero el escenario actual es otro, ahora la víctima ha regresado del lugar en el que estuvo desterrada durante mucho tiempo; y precisamente goza de los mismos derechos y garantías que el imputado, incluso hasta de nuevos derechos. Nuestra LPP no lo ha dejado al libre albedrío y en cada una de sus líneas ha plasmado, aunque no muy explícito, la opinión del legislador al respecto, de lo cual se puede deducir que la mayor limitante para el pleno ejercicio de los derechos de las víctimas es, precisamente, los derechos de los imputados. El actuar de la víctima no puede afectar a las garantías constitucionales que le son reconocidas a los imputados/acusados.

Aún y cuando el reconocimiento de los derechos de las víctimas no pretenda afectar el estatuto procesal de imputado/acusado, el ejercicio de esos derechos sí puede traer aparejada la vulneración de algún derecho o garantía del imputado; pues se le ha reconocido a aquella un estatus procesal superior a lo antes visto en el derecho procesal penal cubano. Al respecto, el profesor Gómez Colomer expresó lo siguiente: «[...] si el final es el nacimiento de un Derecho Procesal Penal de la Víctima a costa de esos derechos del acusado, vamos muy mal. Pero si no hacemos nada por las víctimas, quizás vayamos peor»[13]. Definitivamente el reconocimiento de todos los nuevos derechos de las víctimas es un gran avance en nuestro derecho positivo, pero sin lugar a dudas hay que saber aplicarlos sin afectar los derechos de los imputados/acusados.

Limitaciones de las nuevas formas de intervención. La intervención de la víctima en el proceso se encuentra limitada, y no solo por los derechos de los imputados, sino que además hay situaciones en las que su accionar estará condicionado y limitado por la norma o simplemente a la actuación de otro sujeto procesal.

Estando constituida como parte, la víctima puede intervenir en el proceso como tercero coadyuvante del fiscal, es decir, quién realizará la acción penal será el Ministerio Público, en esta modalidad de participación la víctima está despojada de ese derecho, y se limitará solamente a controlar la acusación, ayudar a la persecución penal y colaborar en el ejercicio de la acción penal pública. Cuando la víctima o el perjudicado decida personarse como acusador coadyuvante debe respetar el objeto del proceso penal que ha sido trazado por el fiscal en la primera de sus conclusiones en el escritorio acusatorio. La víctima podrá ayudar a la autoridad en la redacción del hecho imputado, con el fin de acercarlo lo más posible a las circunstancias presentes durante

la comisión del delito, pero sin introducir aspectos que determinen su modificación esencial.

Este derecho que posee el nuevo sujeto de intervenir como coadyuvante, debe desempeñarse como lo plantea el legislador; la intervención debe ser accesoria y dependiente, pues la acción penal sigue perteneciendo, única y exclusivamente al fiscal, imposibilitando que el coadyuvante redacte su propio hecho delictivo, al cual solo podrá incorporar matices (que pueden ser agravatorios), pero sin modificar sustancialmente el hecho narrado por el fiscal. Su finalidad es la de colaborar con la parte acusadora y controlar su actuación, siempre defendiendo el interés general, nunca sus propios intereses[14].

La acusación penal siempre va a pertenecer al fiscal, exceptuando cuatro presupuestos en los que tendrá lugar el ejercicio de la acción penal privada; a los cuales he hecho alusión en el epígrafe

[12] Ver artículos 94 y 95 de la «Constitución de la República de Cuba» (2019); y artículos 3, 4, 5, 7, 8 y 12 de la «Ley No. 143, LPP» (2021)

[13] (Gómez, 2014, pp. 270-271)

[14] Ver artículo 459.4 de la *LPP* (Cuba), en el cual se deduce que la terminología utilizada por el legislador —«postura asumida por la acusación»— se refiere a la obligación de la víctima de ratificar el interés del fiscal en el esclarecimiento del hech

anterior. De aquí se deriva otra de las variantes de intervención del perjudicado en el proceso: el ejercicio de la acción penal privada.

Con excepción de los casos tradicionales en los que la víctima aparece como acusador particular (delitos de injuria y calumnia), han surgido limitantes para esta nueva modalidad. En este caso podemos evidenciar como la actuación de la víctima está limitada por el parecer y accionar del fiscal.

Cuando la actuación del fiscal amenace con ponerle fin al proceso por cualquiera de las siguientes vías: sobreseimiento definitivo, aplicación de criterios de oportunidad y retirar la acusación durante la formulación de las conclusiones definitivas en el juicio oral; y la víctima o el perjudicado se encontrase inconforme con la decisión de aquel; pues entonces puede erigirse como acusador particular y continuar con el proceso, ejerciendo este la acción penal privada[15].

En caso de que la acusación particular se derive de que el fiscal haya retirado la acusación, sólo podrá ejercer ese derecho a partir de las conclusiones provisionales elaborada por el fiscal, elevarlas a definitivas o modificarlas en todo o en parte, pero sin modificar la primera de las conclusiones, a menos que no sean cambios sustanciales que alteren el hecho imputado[16].

Por otra parte, cuando la víctima decida ejercer la acción civil, por encontrarse inconforme con la responsabilidad exigida al imputado por el fiscal; cabe señalar que esta intervención debe darse dentro del mismo proceso, es decir que solo puede ejercer la acción civil dentro del proceso penal, a menos que se guarde el derecho para ejercerlo posteriormente; y que para ello debe haber estado constituida como parte.

De esta manera podemos evidenciar que, aunque el legislador cubano haya reconocido nuevas garantías para la intervención de la víctima o el perjudicado en el proceso penal, no dejó pasar la ocasión para limitar el accionar de la misma. Pero siempre planteado como máxima limitación, los derechos y garantías de los imputados.

c. Conclusiones

En primer lugar, la norma procesal penal cubana abrió espacio a las víctimas, desterró el concepto de la víctima olvidada e indefensa, dándoles paso a que intervengan en el proceso, con los mismos derechos que poseen las partes procesales. La víctima es un elemento clave en el proceso para lograr la eficacia de la persecución penal.

En segundo lugar, en un proceso penal, la víctima o el perjudicado, ya no es un testigo más, sino que ahora puede intervenir como tercero coadyuvante, acusador particular y ejercitando la acción civil. De esta forma, podrá revisar las actuaciones, proponer pruebas a las autoridades para esclarecer los hechos, interponer recursos contra resoluciones judiciales, proponer causas de nulidad, etc. Todas las nuevas posibilidades garantizan, o al menos es su objetivo central, evitar situaciones de revictimización a las que pueden estar sometidas las víctimas durante todo el proceso.

Por último, el accionar de la víctima dentro del proceso penal se encuentra muy limitado, tanto por la actuación de otros sujetos, como el fiscal; como por los derechos de aquellos. Es de especial interés sintetizar que la mayor limitante al pleno ejercicio de los derechos de las víctimas es, precisamente, los derechos de los imputados. Porque si bien el reconocimiento del papel protagónico que debe desempeñar la víctima en el proceso es un avance en nuestro ordenamiento jurídico, y que es un paso que debe ser festejado, no cabe dudas que conduce eventualmente a la vulneración de los derechos y garantías de los imputados/acusados. La reforma procesal cubana abrió paso hacia nuevos horizontes, pero no podemos dejar que destruya lo que

[15] Ver artículos 18.2, 425.3, 459.4 y 549.3 de la *LPP* (Cuba)

[16] Ver artículo 549.3 de la *LPP* (Cuba).

con tanto esfuerzo y sacrificio hemos logrado.

d. Bibliografía

Bodero C., E. R. (s. f.). *Introducción a la victimología*. Universidad Complutense de Madrid. Recuperado de https://cv4.ucm.es/introduccion_a_la_victimologia

Constitución de la República de Cuba. (2019). *Gaceta Oficial de la República de Cuba*, Edición Extraordinaria No. 5, 10 de abril de 2019.

Cuarezma Terán, S. J. (s. f.). *La victimología. Corte Interamericana de Derechos Humanos*. Recuperado de https://www.corteidh.or.cr/tablas/a12064.pdf

Díaz Colorado, F. (2006). *Una mirada desde las víctimas: el surgimiento de la victimología*. Revista Umbral Científico, (9), 1–10. Colombia. Recuperado de https://www.redalyc.org/pdf/304/30400915.pdf

Fattah, E. A., & Drapkin, I. (s. f.). *El derecho de las víctimas*. Recuperado de https://dialnet.unirioja.es

Fonte Tellería, A. (s. f.). *El tratamiento a la víctima en el proceso penal*. Particularidades en Cuba. Recuperado de https://www.monografias.com/docs110/tratamiento-victima-proceso-penal-particularidades-cuba

Gómez Colomer, J. L. (2014). *Estatuto jurídico de la víctima del delito: La posición jurídica de la víctima del delito ante la justicia penal. Un análisis basado en el derecho comparado y en las grandes reformas españolas que se avecinan*. Aranzadi.

Gómez Guerra, J. (2023). *Tratamiento jurídico a la protección, derechos y garantías de las víctimas de los delitos en Cuba*. Tribunal Supremo Popular de Cuba. Recuperado de https://www.tsp.gob.cu/tratamiento-juridico-la-proteccion-derechos-y-garantias-de-las-victimas-de-los-delitos-en-cuba

González Pérez, R., Suárez Solano, L., Rodríguez Guerra, Y., & Matos Hidalgo, L. (2023). *La víctima. Un acercamiento a su participación en el proceso penal después de la reforma en Cuba*. Recuperado de https://www.pensamientopenal.com.ar/doctrina/90827-victima-acercamiento-su-participacion-proceso-penal-despues-reforma-cuba

Instrucción No. 277 de 2023. *Gaceta Oficial de la República de Cuba*, No. 14 Extraordinaria, 17 de febrero de 2023.

Ley No. 143/2021, Del Proceso Penal, 28 de octubre de 2021. *Gaceta Oficial de la República de Cuba*, No. 140 Ordinaria, 7 de diciembre de 2021.

Ley No. 5 (1977). *Ley de Procedimiento Penal*. Recuperado de https://studylib.es/doc/7207184/ley-de-procedimiento-penal--actualizada--ley-no.-5-de-1de

Ley No. 6 (1977). *Ley de Procedimiento Penal Militar*. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/ref/cmpp.htm

Ley de Enjuiciamiento Criminal. (1882). *Boletín Oficial del Estado* (España). Recuperado de https://boe.es/buscar/act.php?id=BOE-A-1882-6036

Leyton Jiménez, J. F. (s. f.). *Víctimas, proceso penal y reparación: Los derechos de las víctimas en el marco de la Constitución Política, los tratados internacionales y el Código Procesal Penal* [Tesis de licenciatura]. Recuperado de https://www.pensamientopenal.com.ar/system/files/2021/03/doctrina49258.pdf

López Rojas, G. (2022). *El ejercicio de la acusación por parte de la víctima coadyuvante en el nuevo proceso penal cubano: posibilidades y límites*. Revista de Derecho (Valdivia), 35(2), 1–25. Recuperado de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-21502022000200111

Navarro Torres, J. D. (2005). *La importancia de la víctima del delito* [Tesis de licenciatura, Universidad Autónoma de San Luis de Potosí]. Recuperado de https://repositorioinstitucional.uaslp.mx/xmlui/bitstream/handle/i/4027/LDE1IVD00501.pdf

Planchadell Gargallo, A. (2016). *Las víctimas en los delitos de corrupción* (Panorama desde las perspectivas alemana y

española). Estudios Penales y Criminológicos, 36, 1–77.

Sanz Hermida, Á. (2008). *La situación jurídica de la víctima en el proceso penal*. Tirant lo Blanch.

Victimología: pasado, presente y futuro. (2014). *Revista Electrónica de Ciencia Penal y Criminología*, 16, 1–23. España. Recuperado de http://criminet.ugr.es/recpc/16/recpc16-r2.pdf

Columnas & Opinión

Revista Pensamiento Penal
Sección Drogas y derecho penal
Vol. 2, núm. 4 – 2025, págs. 162–170
ISSN: 1853 – 4554

Narcóticos Anónimos

Una medida alternativa al sistema penal

Por Carolina Soledad Fulqueri[1]

Debido a la gran cantidad de presos condenados en Argentina, vinculados al factor criminógeno del consumo de sustancias, decidí introducirme en esta problemática por medio de entrevistas y encuestas hechas en primera persona a personas con problemas de consumo en recuperación. Esta investigación apunta a concientizar sobre la realidad del consumo problemático, para intentar comprender por qué el consumo problemático de drogas predispone a ciertas personas a terminar en el sistema carcelario, en vez de ser atendidos mediante políticas de salud pública. Por esta razón elegí describir el funcionamiento y los efectos que produce en las personas y en la sociedad, la confraternidad de Narcóticos Anónimos, que viene a brindar una respuesta concreta y efectiva a través de un tratamiento de 12 pasos para quienes padecen esta problemática e intentan recuperarse de los efectos de la drogadicción.

*consumo problemático de drogas – narcóticos anónimos – factores criminógenos – justicia penal*

* * * * * *

a. Contexto

Teniendo en cuenta que: uno de cada tres presos dice haber crecido en hogares con alto consumo de alcohol y/o drogas; sumado a que el 42% de la población carcelaria dice haber consumido alcohol o drogas por lo menos seis horas antes del delito por el que los detuvieron[2], resulta necesario investigar cómo atender este factor criminógeno de una manera efectiva (Bergman, 2014) que evite o detenga el continuo crecimiento de la población carcelaria condenada por delitos vinculados a las drogas considerando la estrecha relación que tiene el consumo de estupefacientes con la actividad delictiva propensa a terminar en la cárcel.

Por ello, resulta indispensable entender la vinculación entre esta enfermedad crónica, progresiva y mortal llamada adicción y un Estado que propone el encarcelamiento como remedio para lidiar con este problema (National Institute on Drug Abuse, 2020).

Me parece relevante mencionar la definición utilizada por la *confraternidad de narcóticos anónimos* (N.A.), que establece a la adicción como una enfermedad crónica, que no tiene cura conocida, pero puede ser tratada con éxito (Narcóticos Anónimos, 2024). Y que muchas de esas personas que

[1]Abogada egresada de la Universidad de Buenos Aires y Especialista en Derecho penal. Corre electrónico: carolinafulqueri@hotmail.com

[2] Centro de Estudios Legales e Investigación en Victimología (CELIV). (s. f.). *Delito, marginalidad y desempeño institucional en la Argentina: Resultados de la encuesta de presos condenados. Capítulo 2: Patrones y tendencias delictivas*, p. 33.

se encuentran cumpliendo una pena y que padecen de esta problemática, se encontraban al momento de su detención con su «control de comportamiento» deteriorado, viciado, o sometido bajo los efectos de las drogas.

Ahora bien, ¿qué hacemos con este sector de la población que invade las cárceles? ¿los seguimos condenando, o les ofrecemos un tratamiento para su recuperación?

i. Introducción

Según el contexto mencionado, elegí realizar esta investigación que se enfoca en analizar el impacto que genera en la comunidad y puntualmente en la vida de las personas con problemas de consumo el hecho de tener la posibilidad de realizar un tratamiento para poder parar de consumir drogas.

Para ello el marco de investigación se basa en contar cómo funciona narcóticos anónimos en la Ciudad de Buenos Aires a través de los servicios que realizan para vincularse con la sociedad, y los cambios que se producen en el comportamiento de adictos que se encuentran en recuperación específicamente en relación a las conductas delictivas mientras consumían drogas, y el cambio que se produce cuando dejan de hacerlo.

ii. ¿Qué es narcóticos anónimos?

Narcóticos anónimos es una confraternidad que nace en California (USA) en 1953 y llega a la Argentina en 1986. Es una organización mundial sin fines lucrativos, *no religiosa* que se financia exclusivamente a través de contribuciones de sus propios miembros y de la venta de literatura. No acepta contribuciones externas, ni financiación del Estado, ya que de esa manera pueden tomar sus propias decisiones. En N.A los miembros aprenden los unos de los otros a vivir sin drogas y a recuperarse de los efectos de la adicción en su vida. Cualquier persona que quiera dejar de consumir drogas puede convertirse en miembro. Ser miembro de NA es libre, gratuito, confidencial y no tiene ninguna afiliación con ninguna organización fuera de NA, incluidos gobiernos, religiones, grupos policiales, asociaciones médicas y psiquiátricas.

b. Problemática

En argentina ¿cómo decidimos tratar el consumo problemático de drogas? ¿debe ser atendido como un tema de seguridad pública o, por el contrario, debería ser intervenido desde la óptica de la salud pública?

Cuando los científicos comenzaron a estudiar el comportamiento adictivo en la década de 1930, se pensaba que las personas adictas a las drogas carecían de moral y de fuerza de Voluntad. Estos puntos de vista moldearon las respuestas de la sociedad ante el abuso de drogas, tratándolo más como un fracaso moral que como un problema de salud (National Institute on Drug Abuse, 2020), lo que llevó a poner énfasis en el castigo y no en la prevención y el tratamiento[3].

El hecho de no referirnos al consumo problemático como lo que es: una enfermedad, resulta un impedimento para combatir esta «pandemia» que genera el consumo problemático y sus posteriores consecuencias (muerte, delito, enfermedades, violencia, etc.) (National Institute on Drug Abuse, 2020).

Como señala el Dr. Raúl Eugenio Zaffaroni «cuando el poder político decide suspender un conflicto, en lugar de resolverlo, lo criminaliza»[4] (Zaffaroni, 2000), esta frase explica el fenómeno de la sobrepoblación carcelaria relacionada a un mismo factor criminógeno: el consumo de drogas.

[3] National Institute on Drug Abuse. (2020, agosto 31). *Prefacio.* https://nida.nih.gov/es/publicaciones/las-drogas-el-cerebro-y-la-conducta-la-ciencia-de-la-adiccion/prefacio

[4] Zaffaroni, E. R. (2000). Derecho penal. Parte general (Cap. XII, II, p. 438).

Considerando que «los delitos (...) contra el patrimonio y relacionados con drogas, que constituyen el 80% de las detenciones, son flagrancia» (Bergman, 2014: 63), y que «el deterioro en el autocontrol es el sello distintivo de la adicción»[5], se reafirma que quienes realizan conductas delictivas bajo los efectos de sustancias quedan más expuestos a la criminalización (Bergman, 2014; National Institute on Drug Abuse, 2020).

Por ello, a continuación, detallare cuáles son los efectos positivos de realizar un tratamiento para personas consumo problemático en narcóticos anónimos en relación a la política criminal argentina.

c. Metodología

La manera en que lleve a cabo la investigación se basa en los siguientes puntos:

Estadísticas más relevantes respecto a esta investigación del libro «delito, marginalidad y desempeño institucional en la argentina» para entender por qué es importante tratar este factor criminógeno debido a la cantidad de personas condenadas por delitos relacionados a las drogas.

Mi experiencia al participar como oyente en una reunión maratónica[6] abierta al público de manera virtual.

Mencionare la manera en que funcionan los servicios que ofrece narcóticos anónimos, a través de dos entrevistas que realicé a dos miembros de la organización quienes hacen servicio en subcomités llamados «información pública» y «hospitales e instituciones» dentro de la confraternidad, que explican el motivo y el funcionamiento de esta organización en la comunidad.

La realización de una encuesta a través de Google forms a más de 80 miembros de narcóticos anónimos de la Ciudad Autónoma de Buenos Aires, en la cual realice 12 preguntas relacionadas con las conductas delictivas que realizaban mientras consumían drogas y las conductas desde que empezaron el proceso de recuperación (en esta publicación solo mencionare los resultados de las mismas). donde se demuestran las estadísticas de la influencia directa que proporciona un tratamiento de recuperación de adicciones en el ámbito penal.

d. Trabajo de campo y análisis

i. Encuesta a presos condenados

El análisis parte de la conclusión publicada por Marcelo Bergman (2014) que apunta a la cuestión de la familiaridad con el consumo de drogas como un factor criminógeno en la reincidencia de delitos a partir de una encuesta realizada a presos en la república argentina, de la cual destaco los siguientes datos: «uno de cada 3 presos dice haber crecido en hogares con alto consumo de alcohol y/o drogas» (Bergman, 2014: 16), además de indicar que «las mujeres (quienes son el 5% de la población carcelaria) mayormente fueron condenadas por tenencia y tráfico de drogas (en su 52%)» (Bergman, 2014: 32); y que «el 31% de los internos dice haber consumido alcohol o drogas por lo menos 6 horas antes de haber cometido el delito por el que lo detuvieron» (Bergman, 2014: 32), con esta información podemos afirmar a priori la vinculación estrecha de estar bajos los efectos de drogas y la posibilidad de ser atrapados en flagrancia, como así también la gran cantidad de mujeres presas donde «La misma se vincula con la situación de vulnerabilidad por marginalidad y pobreza (...) por lo que quizás ven como la única

[5] National Institute on Drug Abuse. (2020, agosto 31). *El uso indebido de drogas y la adicción*. NIDA. https://nida.nih.gov/es/publicaciones/las-drogas-el-cerebro-y-la-conducta-la-ciencia-de-la-adiccion/abuso-y-adiccion-las-drogas

[6] Narcóticos Anónimos – Región Argentina. (2020–presente). Formato de reunión virtual mediante plataforma Zoom.

salida laboral la venta de algún tipo de sustancia prohibida»[7].

ii. Oyente en una reunión virtual abierta de NA.

La manera en que funciona N.A. es mediante reuniones presenciales y virtuales donde los miembros comparten experiencias y aprenden a vivir sin drogas. En este trabajo de campo participé en una reunión virtual abierta al público mediante Zoom, disponible las 24 horas desde marzo de 2020 (Narcóticos Anónimos, 2024).

Me pareció interesante, ya que los efectos positivos de que exista una reunión virtual es la amplia llegada que tiene a cada rincón del país, en lugares donde no hay presencialidad, o no cuentan con algún centro de tratamiento, o de información necesaria para tratar con esta enfermedad, y mismo también la facilidad de acceso para profesionales que quieran interiorizarse con la temática o derivar pacientes. Esta propuesta innovadora hace posible que personas privadas de su libertad puedan tener acceso a una reunión de N.A.

iii. Entrevista a J.M y J.P (integrantes de subcomités de información pública y hospitales e instituciones que funcionan en narcóticos anónimos).

En las entrevistas realizadas a miembros de los subcomités de Información Pública e Instituciones y Hospitales, ambos explicaron el rol de N.A. como puente con la comunidad, brindando información, acercándose a comisarías, escuelas, hospitales y cárceles para garantizar acceso al tratamiento (entrevistas propias, 2023).

La entrevistada del subcomité de información pública nos mencionaba que se acercan a comedores, escuelas, entidades públicas, radios, y diferentes lugares de donde los llamen para llegar a distintos estratos de la sociedad. Dando charlas incluso en comisarías, destinadas a los operadores que trabajan allí brindándoles información y contando experiencias personales de cómo era su vida mientras consumían drogas y como es en la actualidad estando en recuperación.

Por otra parte, el entrevistado de hospitales e instituciones nos contaba que, en cambio, ellos se ocupan de acercarse a instituciones, cárceles y hospitales donde se encuentran adictos que no pueden llegar a las reuniones de N.A y hacen de nexo entre la Confraternidad y estos espacios para que puedan realizar reuniones allí dentro y hasta poder institucionalizar[8] esos lugares.

Podría decirse que mientras que información pública cumple una función preventiva respecto a la posibilidad de realizar un primer delito a causa de la enfermedad de la adicción, hospitales e instituciones funciona como una práctica restaurativa en relación a personas con consumo problemático que por ejemplo ya se encuentran cumpliendo una condena y pudiendo eventualmente evitar una reincidencia. Es valorable la iniciativa y la articulación que realizan como una medida alternativa donde se puede ver que mientras el sistema penal persigue y encierra a personas con la enfermedad de la adicción, en contracara existen organizaciones no gubernamentales que buscan *rescatarlos* de los efectos de la adicción.

e. Encuesta anónima a miembros de N.A

Realicé una encuesta a 88 miembros de N.A de zona AMBA de manera virtual mediante formulario de Google forms, que constó de doce preguntas de manera anónima. Las mismas están relacionadas con la actividad delictiva y el consumo de drogas, realizando una distinción temporal: mientras consumían drogas y desde que pararon de consumirlas.

Vale aclarar que siempre que hablamos de no consumir drogas esto incluye también

[7] Revista de Derecho Procesal Penal. (2017). *Alternativas a la prisión, arresto domiciliario, interés superior del niño*, p. 26.

[8] Narcóticos Anónimos – Región Argentina. (s. f.). *Posibilidad de funcionamiento de reuniones dentro de cárceles, hospitales o instituciones, mantenidas por internos que realizan el servicio*. Documento interno.

al alcohol, ya que para N.A droga es cualquier sustancia que altere el estado de ánimo, no importa si está prohibida o permitida.

1. En el grafico uno pregunte sobre la posibilidad de haber podido ser detenido/a mientras consumían drogas: solo el 4,2% respondió que *no* realizó conductas por las que podrían haberlo detenido. El resto respondió que sí: 30% por tenencia o tráfico de drogas; otro 30% por hurto o robo y un 24,5% por venta de drogas, entre otros.
2. En el grafico dos, ante la pregunta de que si mientras consumían drogas fueron detenidos: el 44,3% respondió que no fue detenido a causa de cometer delitos. Es interesante ver que quienes fueron detenidos en un 19,3% fue por causa de robo y hurto. Y un 22,7% por tenencia o tráfico de drogas. Solo un 4,5% fue detenido por venta de drogas pese a que en la respuesta anterior había un 24,5% desrealización de ese delito.
3. En el grafico tres se puede observar que, entre las personas en recuperación un 19,5% cuenta con antecedentes penales, y un 9,2% no lo sabe. Podemos ver que de un 55,7% de detenidos en la respuesta anterior, hay un 36% aproximadamente de detenciones que no concluyeron en una sentencia penal.
4. Como se observa en el grafico cuatro, ante la pregunta de cuál era su situación academia antes de conocer N.A, contestaron que: el 43,2% únicamente tenía completa la educación primaria; El 40.9% había completado los estudios secundarios; sólo un 9,1% tenían terciario completo y un 5,7% contaba con título universitario.
5. En el grafico cinco me interesaba saber si había gente derivada a N.A. por orden judicial. Solo el 2,3% personas respondieron que sí. Por otro lado, un 8% conoció N.A a través del servicio de HeI y un 5,7% por servicios de I.P. Estos dos últimos son medios de acercamiento que N.A. ofrece a la comunidad explicados en las entrevistas realizadas. Pero a la mayor parte le llega la información de que existe N.A. mediante familiares o conocidos en un 63,6%.
6. En el grafico seis se puede observar una pregunta de la encuesta con respuesta abierta. En general refieren a una *situación límite,* sufrimiento, intento de suicido y en muchos casos la pérdida de tenencia de hijos como acontecimiento que los llevo a tomar la decisión de para de consumir drogas.
7. En el grafico siete, se observa que el 90,8% no volvió a cometer delitos desde que paró de consumir drogas en Narcóticos Anónimos. En esta instancia de la encuesta es donde se pueden empezar a ver los cambios significativos en el comportamiento de las personas a causa de iniciar un proceso de recuperación, atendiendo el factor criminógeno de fondo.
8. En el grafico ocho, sorprenden las estadísticas al visibilizar que solo un 3% de los encuestados fueron detenidos desde que pararon de consumir.
9. En el grafico nueve se observa que solamente el 4,5% estuvo en situación de cárcel una vez que dejó de consumir drogas, a diferencia del 19,5% que pasó por el sistema carcelario mientras consumía drogas. En muchos casos las sentencias son por delitos anteriores a parar de consumir.
10. En el grafico diez se puede ver que, desde que pararon de consumir drogas las estadísticas se modificaron en un gran porcentaje respecto a la situación académica: a diferencia del punto N°4, disminuye el porcentaje de primaria completa a un 18,6% (que en el punto mencionado era del 43,2%), y suben

los porcentajes en el nivel de terciario completo a un 27,9% (En el punto N° 4 eran de un 9,1%) y obtuvieron título universitario un 9,3%.

11. En el grafico once, se pueden ver las respuestas ante la pregunta de que si creen que la adicción a las drogas los predispone a cometer delitos y por qué. Alrededor de un 90% de los encuestados respondieron que sí, cada uno dio su opinión sobre a qué se debe, es interesante la lectura de cada respuesta. Muchos coinciden con esta idea de que la pérdida del control y de la noción de la realidad, a causa de la desesperación por consumir sustancias y la abstinencia que genera son desencadenantes de la realización de conductas delictivas para poder conseguir dinero y seguir consumiendo, ya que *mencionan que las características de esta enfermedad son la obsesión, compulsión y pérdida del sano juicio.*
12. En el grafico doce se encuentra la pregunta final, donde respondieron sobre como creen que sería su vida en la actualidad si no conocieran la confraternidad de Narcóticos anónimos. Sus respuestas se basaron en: Cárcel, hospital y muerte.

Los gráficos se pueden observar en el anexo final.

En la encuesta realizada, los porcentajes hablan por sí solos: hay un cambio significativo y casi total en la conducta de las personas con consumo problemático respecto a la reducción de comportamientos delictivos propensos a terminar en el sistema carcelario desde que entraron en recuperación en N.A. Como así también en su calidad de vida que se ve en la evolución académica que se refleja en los encuestados.

Es indispensable brindar una herramienta como la que ofrece esta organización a la sociedad, que se encuentra al alcance de cualquier persona que lo necesite pero que, por un tema de falta de información, comunicación, difusión o derivaciones respecto al sistema judicial, se pierde la posibilidad de poder revertir un triste destino.

Los resultados muestran que quienes llegan a este tratamiento es por allegados, de boca en boca, y por los propios esfuerzos que hacen los miembros para darse a conocer a través de los servicios realizados. Es realmente una herramienta efectiva para atender esta problemática, y evitar los efectos negativos que genera la adicción para quien la padece, para su entorno y para la sociedad.

f. Normativa

Cuando nos referimos a personas con adicciones, resulta imprescindible considerar la ley 26.657 de salud mental, que establece que estas problemáticas deben ser tratadas como parte de políticas de salud pública, en contraste con la ley 23.737 que asigna un doble estatus de enfermo y delincuente (ley 26.657, 2010; ley 23.737, 1989).

En la causa *Arriola*, la corte suprema consideró que el aumento de causas por tenencia para consumo personal demostraba el fracaso del modelo represivo (C.S.J.N., 2009).

La idea de combatir el narcotráfico y disminuir el consumo a partir de la prohibición y represión de estas conductas pareciera que no conlleva en sí misma la eliminación del uso de drogas, sino por el contrario incrementa la selectividad del sistema penal en materia desigualdad social. Como vimos anteriormente con Bergman, que señala que más del 50% de las mujeres detenidas es a causa de la aplicación de esta ley respecto a la tenencia y tráfico de estupefacientes, queda en evidencia no sólo una cuestión de género sino también que se castiga más eficazmente a los eslabones inferiores de las cadenas como los consumidores o vendedores al *menudeo*, pero muy raramente a los altos mandos del narcotráfico. Y donde las autoridades de aplicación de esta ley pasan a ser jueces en materia penal previo dictamen de peritos

que aconsejan sobre la situación mental del imputado.

g. Conclusión

Luego de este recorrido, puede afirmarse que este factor criminógeno no se relaciona con cuestiones morales, sino con la pérdida de control y deterioro del sano juicio que provoca la adicción (National Institute on Drug Abuse, 2020; Narcóticos Anónimos, 2024).

Podríamos hacer un paralelismo de esta problemática con la enfermedad de la diabetes, aunque a priori la decisión de consumir drogas es voluntaria, el deterioro en el autocontrol es un factor fundamental para las personas quienes padecen esta problemática y aunque no exista hoy en día una cura para ello (así como tampoco para la diabetes) puede ser tratada con éxito.

Imaginémonos una persona que por propia voluntad empiece a comer excesivamente, que sus hábitos alimenticios pasen a ser a un comportamiento autodestructivo, que se transforme en obesidad (hoy considerada una enfermedad) y que lejos de brindarle un tratamiento, atención médica, insulina o lo que haga falta para el cuidado de su salud, en cambio la criminalizamos, estigmatizando su condición, discriminándola por lo que es, y creyendo que esa persona por propia voluntad eligió estar así, con un deterioro en su salud, cerca de la muerte y con un Estado que en vez de asistirla, porque le sea costoso o un trabajo más arduo, o no sepa cómo ayudarla por falta de información o por falta de empatía de los operadores judiciales, la convierta en delincuente, utilizando el miedo como mecanismo de control, creyendo que de esa manera las personas no va n a comer en exceso para no enfermarse eventualmente y no terminar perseguida por un sistema judicial que lejos de darle una solución, los penara.

Esto es lo que sucede en muchos casos con las personas con consumo problemático a las drogas. Pese a que tengamos una Ley de salud mental que como vimos contempla a las personas con consumos problemáticos, y prevé la obligación del Estado de tener que brindar tratamientos para su recuperación; la realidad es que el sistema punitivo llega mucho antes que las políticas en salud pública. Políticas que hacen a los principios de derechos humanos y al cumplimiento de los tratados internacionales consagrados por nuestra Constitución Nacional.

Es necesario que la legislación y la política criminal acompañen ese proceso desde el campo de la Salud Pública y evitar trasladarlo a una cuestión de Seguridad Pública. Para evitar convertir al adicto en delincuente y abandonar toda posibilidad de integrarlo socialmente. La ayuda a aquellas personas para las cuales el consumo de sustancias es problemático no debería ser objeto de procedimientos penales. Hay que determinar cuál es el bien jurídico o la preponderancia de uno sobre el otro: si la salud o la seguridad pública.

Esta investigación demuestra que más del 90% de quienes realizan tratamiento en N.A. no volvieron a cometer delitos desde que dejaron de consumir. Ello muestra la necesidad de que el Estado garantice acceso a tratamientos y no recurra al castigo como primera respuesta.

.

Mientras tanto organizaciones como N.A se encargan y se disponen a ayudar en una especie de *rescate* , mediante los servicios que realizan, a individuos que, sin un lugar de contención, de información, y de posibilidad de tratar su problemática terminan inevitablemente en cárceles, hospitales o la muerte.

h. Bibliografía

Bergman, M. (2014). *Delito, marginalidad y desempeño institucional en Argentina: Resultados de la encuesta de presos condenados*. Universidad Nacional de Tres de Febrero.

Ley 23.737. (1989). *Ley nacional de estupefacientes*. Boletín Oficial de la República Argentina.

Ley 26.657. (2010). *Ley nacional de salud mental*. Boletín Oficial de la República Argentina.

Narcóticos Anónimos. (2024). *Información sobre Narcóticos Anónimos* [PDF]. https://na.org/wp-content/uploads/2024/06/SP2302_InfoAboutNA-Spanish.pdf

National Institute on Drug Abuse. (2020, agosto 31). *El uso indebido de drogas y la adicción*. NIDA. https://nida.nih.gov/es/publicaciones/las-drogas-el-cerebro-y-la-conducta-la-ciencia-de-la-adiccion/abuso-y-adiccion-las-drogas

National Institute on Drug Abuse. (2020, agosto 31). *Prefacio*. NIDA. https://nida.nih.gov/es/publicaciones/las-drogas-el-cerebro-y-la-conducta-la-ciencia-de-la-adiccion/prefacio

Wachtel, T. (2013). *Definiendo qué es restaurativo* [PDF]. Instituto Internacional de Prácticas Restaurativas (IIRP). https://www.iirp.edu/images/pdf/Defining-Restorative-Spanish.pdf

Zaffaroni, E. R., Slokar, A., & Alagia, A. (2000). *Derecho penal. Parte general*. Ediar.

i. Anexo

Gráfico 1. *Mientras consumías drogas ¿realizaste conductas por las que te podrían haber detenido? ¿Cuáles? (Elaboración propia a partir de encuesta realizada en 2023)*

Gráfico 2. *Mientras consumías drogas ¿Fuiste detenido/a? ¿Por cuál delito? (Elaboración propia a partir de encuesta realizada en 2023)*

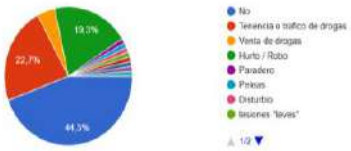

Gráfico 3. *¿Tenes antecedentes penales? (Elaboración propia a partir de encuesta realizada en 2023)*

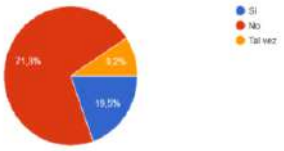

Gráfico 4. *¿Cuál era tu situación académica antes de conocer Narcóticos Anónimos? (Elaboración propia a partir de encuesta realizada en 2023)*

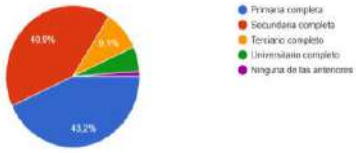

Gráfico 5. *¿Cómo conociste Narcóticos Anónimos? (Elaboración propia a partir de encuesta realizada en 2023)*

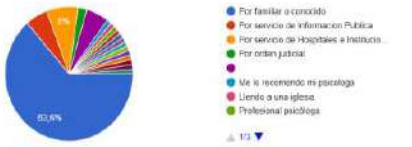

Gráfico 6. *¿Cuál fue el clic o acontecimiento que te llevo a tomar la decisión de para de consumir drogas? (Elaboración propia a partir de encuesta realizada en 2023)*

Gráfico 7. *¿Has vuelto a cometer delitos desde que paraste de consumir drogas? (Elaboración propia a partir de encuesta realizada en 2023)*

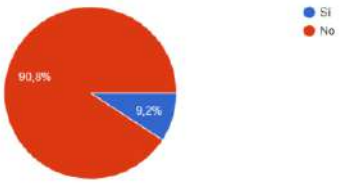

Gráfico 8. *¿Has sido detenido/a desde que paraste de consumir drogas? (Elaboración propia a partir de encuesta realizada en 2023)*

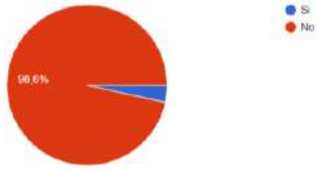

Gráfico 9. *¿Has estado preso desde que paraste de consumir drogas? (Elaboración propia a partir de encuesta realizada en 2023)*

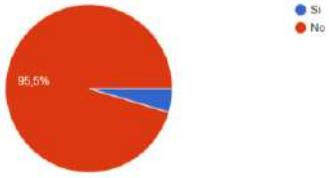

Gráfico 10. *¿Cuál es tu situación académica hoy? (Elaboración propia a partir de encuesta realizada en 2023)*

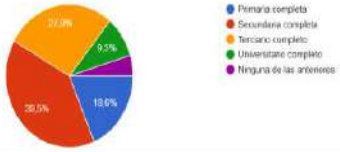

Gráfico 11. *¿Crees que la enfermedad de la adicción a las drogas te predispone a cometer delitos? ¿Por qué? (Elaboración propia a partir de encuesta realizada en 2023)*

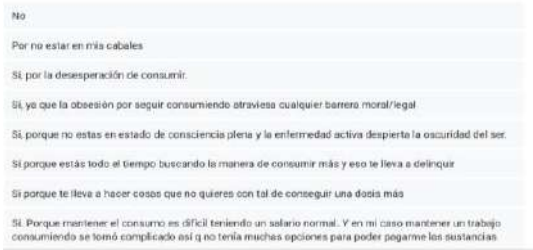

Gráfico 12. *¿Cómo crees que sería tu vida hoy si no hubieses conocido Narcóticos Anónimos? (Elaboración propia a partir de encuesta realizada en 2023)*