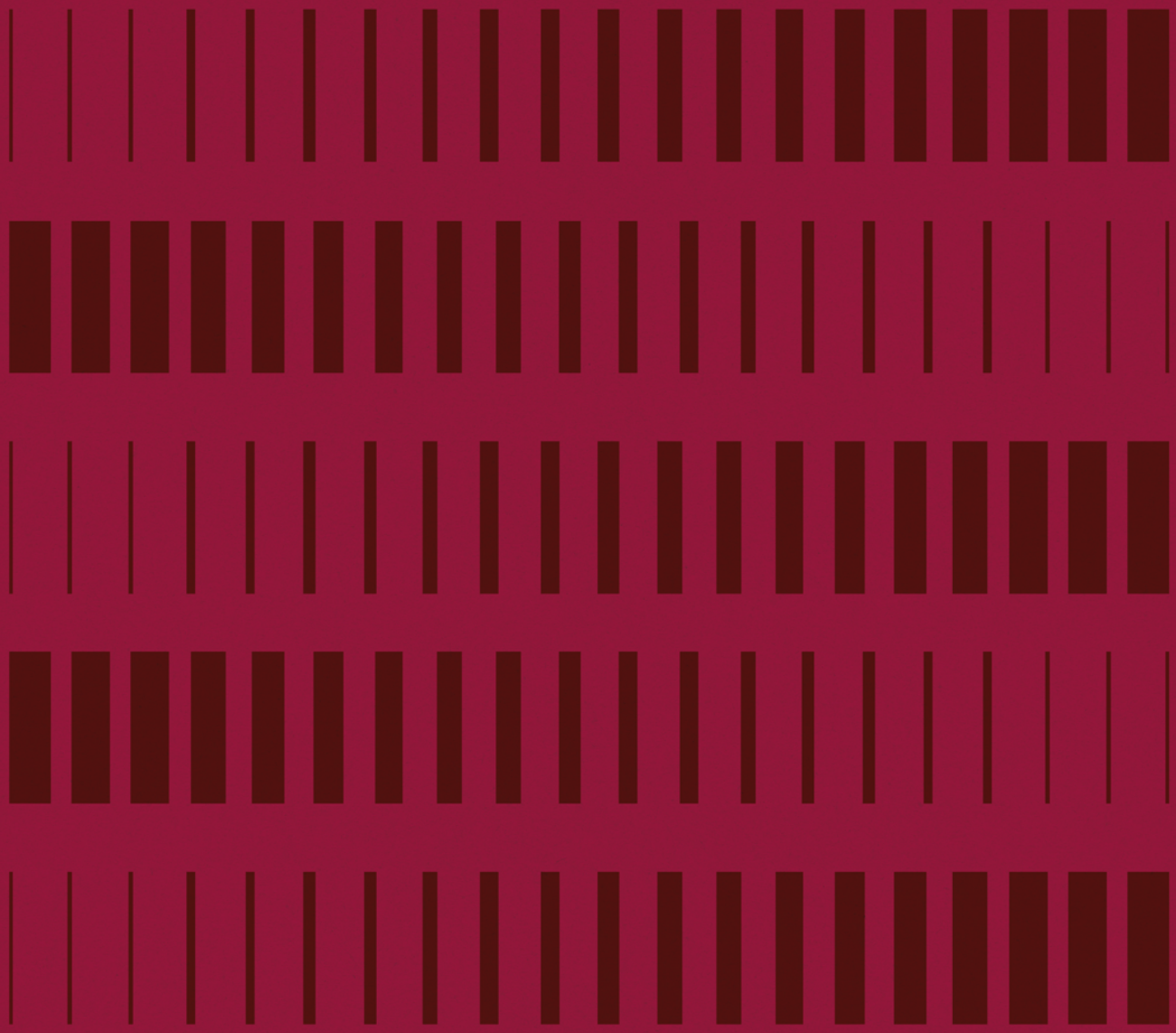

Inteligencias intrusivas

Tecnologías de interceptación y monitoreo en Argentina, Chile y Uruguay

MAPA TÉCNICO Y COMERCIAL

Lucas Domínguez Rubio

Inteligencias intrusivas

Tecnologías de interceptación y monitoreo en Argentina, Chile y Uruguay

mapa técnico y comercial

Lucas Domínguez Rubio

Diciembre 2025

SOCIALTIC

OPEN TECHNOLOGY FUND

Versión en español concluida en diciembre de 2025.
English-language manuscript completed on 1 December 2025.

ISBN 978-970-96205-0-4

DOI: https://doi.org/10.47195/INT.96205

CORRECCIÓN POR HERNÁN VILLASENÍN
MAQUETACIÓN Y DISEÑO POR BRENDA MUÑOZ ROSAS

Resumen

El mercado de tecnologías de interceptación y monitoreo utilizadas por agencias de seguridad en el Cono Sur permanece poco documentado, evoluciona con rapidez y se caracteriza por altos niveles de opacidad. Las capacidades concretas de las herramientas implementadas rara vez se hacen públicas, y los procesos de adquisición solo pueden reconstruirse de forma parcial.

Con el fin de reducir este vacío, el presente informe propone una clasificación técnica de las tecnologías de interceptación y monitoreo disponibles y reconstruye patrones de adquisición documentados en Argentina, Chile y Uruguay. Basándose en informes técnicos, folletos comerciales, licitaciones y bases de datos especializadas, el estudio identifica herramientas de vigilancia según sus capacidades operativas y traza el mapa de los principales fabricantes y sus intermediarios regionales.

La clasificación propone una taxonomía de cinco categorías: (i) software de intrusión o *spyware*, (ii) tecnologías de interceptación de señales, (iii) plataformas de interceptación e inteligencia de redes, (iv) sistemas de monitoreo del tráfico de red, y (v) herramientas de inteligencia de fuentes abiertas (OSINT). Sobre esta base, el informe analiza evidencia de adquisiciones realizadas por agencias de seguridad en los tres países y distingue entre compras confirmadas, adquisiciones probables y negociaciones documentadas, según el grado de evidencia disponible.

El análisis revela una tendencia regional hacia arquitecturas de vigilancia integradas en plataformas capaces de concentrar varias capacidades. Los tres países incorporaron, con distintos niveles de intensidad, la casi totalidad del espectro de tecnologías disponibles. Sin embargo, los perfiles nacionales difieren. Chile registra la adopción más amplia, con adquisiciones confirmadas de herramientas altamente intrusivas, incluido *spyware* comercial. Argentina muestra un ecosistema fragmentado, con múltiples intermediarios locales y una acumulación progresiva de capacidades entre distintas agencias y niveles del Estado. Uruguay exhibe un perfil diferenciado: baja probabilidad de adopción de *spyware* comercial, pero desarrollo sostenido de capacidades integradas de interceptación legal, con un modelo más institucionalizado, orientado al monitoreo a nivel de red antes que a la infiltración de dispositivos individuales. A los perfiles descritos se suma una dependencia estructural de un número reducido de países proveedores, en la que los actores locales operan casi exclusivamente como distribuidores, limitando la transparencia y el control democrático sobre herramientas de vigilancia de alto impacto.

El estudio combina así una cartografía de la oferta de tecnologías de vigilancia con una reconstrucción de la demanda institucional para identificar patrones regionales de adopción tecnológica. Sus hallazgos muestran que estas capacidades se expanden con independencia del signo político de los gobiernos, en mercados diseñados para no dejar rastro y en un vacío regulatorio que ninguno de los tres países ha resuelto.

Índice

1. Introducción

1.1. Contexto internacional: de PRISM a Pegasus

El problema resulta conocido. Diversas empresas ofrecen *soluciones* para agencias de seguridad de manera opaca. Si bien sus implementaciones conllevan importantes consecuencias políticas y sociales, se trata de tecnologías que no suelen contar con una regulación adecuada. Además, distintos tipos de abusos quedaron bien documentados en gran parte de la región y sus implicancias rara vez se discuten en el ámbito público.

Por *herramientas de cibervigilancia* —al final del reporte discutiremos los sesgos en esta noción— suele entenderse el conjunto de diferentes tipos de software y hardware utilizados por organismos de inteligencia y fuerzas de seguridad para supervisar, extraer, recopilar o analizar datos de comunicaciones. La proliferación de este mercado en las últimas décadas alcanzó números excepcionales.

Ya pasaron en efecto treinta años desde que Privacy International publicó en 1995 su primer reporte sobre el comercio internacional de tecnología de vigilancia.[1] Este informe inicial se inscribe en un momento en el que los gobiernos centrales ya estaban diseñando las redes de telecomunicaciones para hacerlas interceptables por diseño. En 1994, Estados Unidos aprobó su *Communications Assistance for Law Enforcement Act* (CALEA), que obligaba a operadoras y fabricantes a incorporar capacidades de interceptación legal en sus infraestructuras. En paralelo, el organismo europeo de estandarización ETSI —*European Telecommunications Standards Institute*— empezaba a publicar especificaciones técnicas para definir cómo debe entregarse el tráfico interceptado a las agencias de seguridad. Se trataba también del momento de las llamadas "crypto wars": el nombre que se le dio a los intentos de Estados Unidos y sus aliados de limitar el acceso público a herramientas de cifrado fuerte, ya sea mediante controles a la exportación de criptografía o mediante el diseño de sistemas con fallas de seguridad incorporadas de fábrica —llamadas *backdoors*.

Mientras se estabilizaba ese marco regulatorio y técnico, internet pasó a convertirse en una infraestructura de masas. El salto en el cambio de siglo resulta impactante. Entre 1997 y 2001, el número de usuarios pasó de 117 millones a 489 millones: un incremento del orden del 318 % en apenas cuatro años, según estimaciones de la Unión Internacional de Telecomunicaciones. Los atentados del 11 de septiembre de 2001 llevaron a desplegar nuevas capas de control sobre esa infraestructura ya masificada: en Estados Unidos, la USA PATRIOT Act reescribió en pocas semanas buena parte de las leyes de vigilancia y facilitó el acceso del gobierno a registros y metadatos de comunicaciones (mediante órdenes secretas, interceptaciones "itinerantes" y pedidos administrativos caratulados como secretos), mientras que en Europa se erigieron nuevas políticas de retención obligatoria de datos de tráfico en nombre de la lucha contra el terrorismo.

A fines de esa misma década, otro hito alteró para siempre la superficie comunicacional: de a poco, el smartphone se convirtió en la interfaz dominante para el acceso cotidiano a internet. Su conexión con el cuerpo y la vida cotidiana combinó comunicaciones con aplicaciones móviles dirigidas a todas las esferas de la experiencia.

---

1 Privacy International. *Big Brother Incorporated*. London, 1995. URL

Un primer punto de inflexión en la conversación global sobre seguridad, privacidad y tecnología llegó en 2013, cuando Edward Snowden filtró miles de documentos confidenciales de la Agencia de Seguridad Nacional de Estados Unidos (NSA, *National Security Agency*) e hizo pública la existencia del programa PRISM y otros programas de vigilancia masiva como XKEYSCORE, Boundless Informant y los sistemas de interceptación "Upstream".[2] PRISM era el nombre clave de un programa puesto en marcha por la NSA en 2007 que permitía recopilar información de las comunicaciones de las principales empresas tecnológicas estadounidenses —entre ellas Microsoft, Yahoo!, Google, Facebook (ahora Meta) y Apple. Las filtraciones mostraban tanto la captura sistemática de datos de usuarixs de grandes plataformas como el espionaje a mandatarixs y líderes de otros países, entre ellxs la canciller alemana Angela Merkel y jefes de Estado latinoamericanos, lo que disparó un escándalo diplomático global.

Esto quedaba de algún modo posibilitado por la ley FISA (*Foreign Intelligence Surveillance Act*). Esta norma fijaba los procedimientos para que las agencias de inteligencia de Estados Unidos pudieran obtener información vinculada a amenazas del exterior en el marco de la seguridad nacional, y no como parte de una investigación penal ordinaria. Por eso funcionaba como la base legal de programas como PRISM, que obligaban a grandes empresas tecnológicas a colaborar con la NSA en la entrega de datos de usuarixs. Sin embargo, las filtraciones mostraron que el alcance de la recolección de datos era mucho más amplio de lo que se admitía y tuvo también repercusiones internas: no era evidente hasta dónde llegaban las garantías que evitaban la recolección de datos de ciudadanos estadounidenses.

Si bien el proceso del cifrado del tráfico web estaba en aumento y respondía a distintas necesidades comerciales, la reacción técnica a esas revelaciones fue un giro coordinado hacia el cifrado por defecto. En pocos años el uso de protocolos que cifran la comunicación entre el navegador y el servidor —SSL/TLS (y luego HTTPS)— pasó de ser una excepción costosa a convertirse en requisito básico.

Con el tránsito de red cifrado, el eslabón más vulnerable pasó a ser el extremo: la computadora o el teléfono de las personas. Esa reconfiguración empujó el foco hacia los dispositivos. En 2012 comenzó el auge paulatino del *spyware* dirigido a smartphones, capaz de infectar dispositivos iOS y Android, y capturar comunicaciones directamente desde el aparato.

Fue en este marco que, con el tiempo, Privacy International desarrolló una base de datos que llegó a incluir 528 empresas que vendían equipos para la interceptación de comunicaciones, videovigilancia, biometría, geolocalización, *monitoreo* de internet, inspección de paquetes, extracción forense y software de intrusión. Una lástima: el *Surveillance Industry Index* (SII) fue discontinuado en 2018.[3]

Un segundo punto de inflexión dentro de esta discusión se produjo entre 2015 y 2017 con la difusión de noticias sobre la existencia de *spyware* comercial de empresas como FinFisher, Hacking Team y NSO Group. En este caso, el escándalo

---

2 Puede verse: Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1, n.º 2 (2014). DOI. // Verble, Joseph. "The NSA and Edward Snowden: Surveillance in the 21st Century." *SIGCAS Comput. Soc.* 44, n.º 3 (2014): 14–20. DOI. // Bigo, Didier, Gertjan Boulet, Caspar Bowden, et al. "Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU." *CEPS Policy Brief* 293 (2014). URL.

3 Privacy International. *The Global Surveillance Industry*. London, 2018. URL.

no estaba vinculado a un único programa de vigilancia masiva dirigido por un Estado en el que participaban gigantes tecnológicos mundiales. Empresas mercenarias como NSO Group simbolizaron una nueva etapa. Filtraciones de documentos internos y análisis técnicos mostraron cómo estas compañías vendían herramientas de intrusión extrema —capaces de tomar el control de computadoras y teléfonos— a gobiernos de todo el mundo, incluidos regímenes autoritarios, y cómo se las utilizaba contra periodistas, activistas y opositores políticos.[4]

La narrativa cambió. Las grandes empresas como Facebook/Meta, Google y Apple se lanzaron a un posicionamiento público en clave de privacidad —o *privacy washing*— con cambios de política, campañas de marketing y litigios estratégicos. De hecho, Meta, una de las principales empresas identificadas como parte de PRISM, emprendió acciones legales contra NSO Group por el uso de Pegasus contra más de 1.400 usuarios de su sistema de mensajería; lo que ponía de relieve un cambio de alineación en las exigencias de responsabilidades.[5]

Por supuesto, estos dos grandes momentos de inflexión en la discusión pública sólo muestran una pequeña parte de un entorno complejo en el que intervienen muchos actores diferentes. Sin embargo, fueron los productores privados de herramientas de vigilancia los que comenzaron a ser el foco de atención.

En 2015 se filtraron más de un millón de mails internos de la productora italiana de *spyware* Hacking Team.[6] Los reportes se sucedieron. El *spyware* comercial tomó el centro de la escena. Investigadorxs, activistas y periodistas comenzaron la ardua tarea de identificar empresas y tecnologías de este ecosistema en un esfuerzo que nunca resulta concluyente. Por el contrario, no deja de abrir conexiones, entre grupos inversores, revendedores, agencias de seguridad y denuncias múltiples.

La dificultad radica en que las compañías y las herramientas están en constante transformación. Cambian de nombre y de localización, según avanza la legislación de los distintos países. Los cambios de nombre y las estructuras corporativas opacas y complejas facilitan la evasión de las regulaciones nacionales y transnacionales. Se asocian tanto a grandes conglomerados como a revendedores regionales. Muchas veces son ejecutivos europeos que trasladan sus negocios a jurisdicciones remotas o que usan intermediarios para operaciones ilegales en sus propios países.[7]

---

4 Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak y Ron Deibert. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Citizen Lab Research Report N.º 113. University of Toronto, 2018. URL // Amnesty Tech. *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*. Amnesty International, 2021. URL // Kaster, Sean D., y Prescott C. Ensign. "Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware." *Thunderbird International Business Review* 65, n.º 3 (2023): 355-64. DOI

5 Entendiendo que la empresa tiene información de primera mano a través de su análisis de los ataques perpetrados por WhatsApp, en efecto, el diagnóstico en palabras de Meta resulta igual de preocupante: "While these 'cyber mercenaries' often claim that their services only target criminals and terrorists, our months-long investigation concluded that targeting is in fact indiscriminate and includes journalists, dissidents, critics of authoritarian regimes, families of opposition members and human rights activists." Dvilyanski, Mike, David Agranovich, y Nathaniel Gleicher. *Threat Report on the Surveillance-for-Hire Industry. Meta,* 2021, p. 2. URL

6 "WikiLeaks - The Hackingteam Archives." 2015. URL

7 Lighthouse Reports. *Surveillance Secrets: How First Wap Tracks Phones Around the World.* Lighthouse, 2025. URL

El mapa se torna aún más complejo cuando se trata de identificar compras concretas en países cuyas normativas permiten no rendir cuentas sobre la adquisición de herramientas de inteligencia.[8]

A los informes pioneros de Privacy International le continuó una investigación exhaustiva que identificaba a las empresas que ofrecían tecnologías de interceptación e intrusión en la gran feria global de tecnología para agencias de seguridad.[9] El panorama irradiaba un conglomerado de nombres, conexiones y superposiciones. Por eso, la última investigación de largo aliento que intentó determinar la forma de este conglomerado habla con precisión de una *bestia mítica* que debe ser rastreada mediante una compleja red de negocios. La base de datos de esta investigación se visualiza en un mapa de nodos siempre móvil, que incluye "cuarenta y nueve productores, junto con treinta y seis filiales, veinticuatro empresas asociadas, veinte proveedores y una combinación de treinta y dos sociedades de inversión, noventa y cinco inversionistas y ciento setenta y nueve personas físicas, entre las que se incluyen muchos inversionistas reconocidos".[10]

Sin ofrecer un conteo global consolidado, el primer informe de Privacy International de 1995 identificó más de ochenta empresas británicas y docenas de compañías adicionales en otros países dedicadas a la seguridad digital en sentido amplio: equipos físicos de contrainteligencia, inhibidores de señal, cámaras de seguridad, etc. En 2016, la misma organización trabajó con una base de 528 empresas de vigilancia registradas en el *Surveillance Industry Index*. Sobre tecnologías más precisas, un informe de 2021 del Atlantic Council registró 224 empresas que comercializan capacidades de intrusión e interceptación en las ferias de tecnologías de vigilancia más importantes del mundo. Por su parte, entre compañías productoras, holdings de inversión y revendedoras, el proyecto *Mythical Beasts* (2024) mapeó 435 entidades vinculadas al mercado global de spyware a lo largo de 42 países.

---

8 Gjesvik, Lars y Johann Ole Willers. "Beyond Control? The Political Economy of Private Interception, Intrusion, and Surveillance Markets." *Review of International Political Economy* 31, n.º 6 (2024): 1840–64. DOI

9 DeSombre, Winnona, Lars Gjesvik y Johann Ole Willers. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets." *Atlantic Council*, 8 de noviembre de 2021. URL

10 Recomendamos seguir el enlace hasta su *dashboard* para ver las formas que puede tomar esta bestia: Roberts, Jen, Trey Herr, Nitansha Bansal y Nancy Messieh. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights.* With Emma Taylor, Jean Le Roux, and Sopo Gelava. 2024. URL

Frente a este panorama, algunas iniciativas internacionales buscan aplicar controles sobre la comercialización de este tipo de "herramientas de cibervigilancia", donde la noción de *tecnologías de doble uso* cobra un sentido legal y técnico. Se llama así a las tecnologías con aplicaciones civiles, como las comunicaciones o el procesamiento de datos, que también se utilizan para fines militares, de seguridad o inteligencia. Por ejemplo, las tecnologías de gestión de tráfico de red pueden también utilizarse para bloquear contenidos o interceptar comunicaciones. El significado de las tecnologías de doble uso está estrechamente relacionado con el papel cada vez más importante que desempeñan las empresas privadas que ofrecen soluciones de vigilancia a los gobiernos.

Un mecanismo internacional clave para abordar esta cuestión fue el *Wassenaar Arrangement*, un acuerdo multilateral de control de exportaciones establecido en 1996 para promover la transparencia y la responsabilidad en la transferencia de armas y en los productos de doble uso. Desde 2012, este acuerdo ha añadido la categoría de "software de intrusión" y otras herramientas de cibervigilancia a las listas de tecnologías reguladas.[11] Cabe destacar que este acuerdo ha recibido diversas críticas. Por un lado, muchos informes enfatizan que su redacción resulta sospechosamente ambigua, lo que deja dudas sobre su alcance efectivo, además, beneficia la proliferación de ciertas empresas y tecnologías. Por otro lado, países relevantes como Israel, China y Rusia no son signatarios, y otros, como Italia, implementan sus propios controles internos de manera subordinada a las decisiones geopolíticas de sus gobiernos. Aunque desde su inicio se ha criticado la falta de inclusión de ciertas tecnologías vinculadas a la interceptación legal o la explotación de señales de telefonía celular, su relevancia radica en la inclusión de herramientas que obligan a los Estados miembros a supervisar su exportación, sobre todo cuando suponen un riesgo de represión o violación de los derechos humanos.[12]

Producto de este acuerdo, en 2021 la Unión Europea estableció un reglamento (2021/821) a partir del cual se registró una disminución de las licencias otorgadas en lo que se refiere a "tecnologías de cibervigilancia": interceptación de comunicaciones móviles, sistemas de vigilancia de red y herramientas para la generación o manejo de programas de intrusión. Sin embargo, por lo mencionado, queda ver si los capitales interesados en desarrollar este tipo de tecnologías no han optado por distintas metodologías de circunvención de este reglamento.

En Latinoamérica, sólo México y Argentina suscribieron el Wassenaar Arrangement. Con esto establecen un compromiso de mantener controles nacionales sobre la reventa de armas convencionales y tecnologías de uso dual, y de cooperar en la transparencia y el intercambio de información sobre dichas exportaciones según los estándares internacionales de seguridad.

Otra iniciativa internacional surgió tras la orden ejecutiva emitida por la Casa Blanca en 2023, que restringió el uso de *spyware* comercial por parte del gobierno federal de Estados Unidos. Poco después, otros 16 países se sumaron a una declaración conjunta que reconocía este tipo de software como una amenaza

---

11 Coalition Against Unlawful Surveillance Exports (CAUSE). *A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation*. Coalition Against Unlawful Surveillance Exports (CAUSE), 2014.

12 Bromley, Mark. "The EU Dual-Use Regulation, Cyber-Surveillance and Human Rights: The Competing Norms and Organised Hypocrisy of EU Export Controls." *Defence Studies* 23, n.º 4 (2023): 644–64.

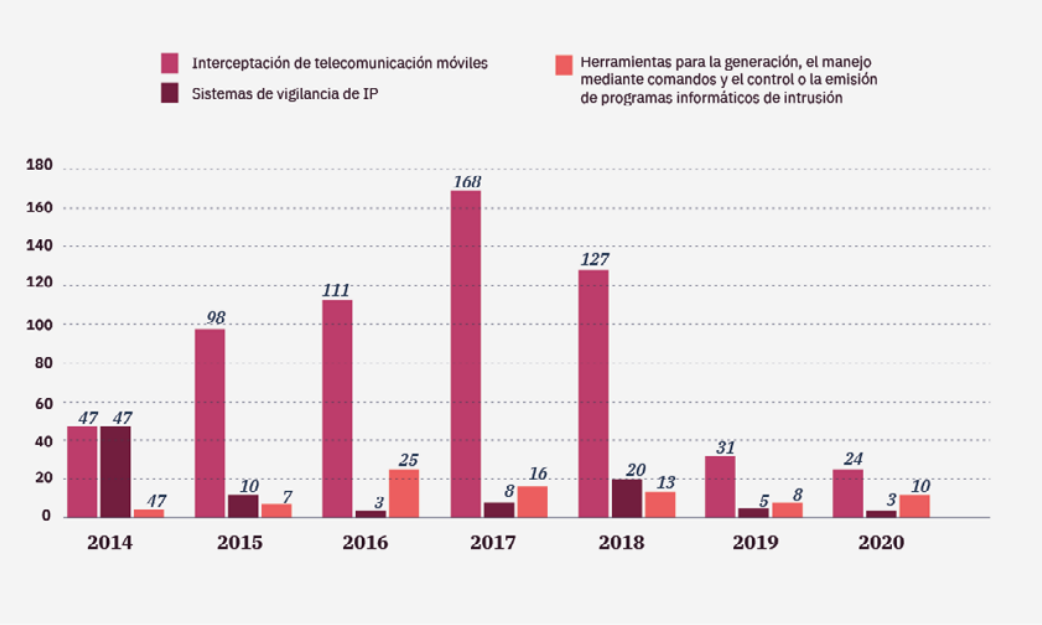

Gráfico publicado en: Comisión Europea. Informe de la Comisión al Parlamento europeo y al Consejo sobre la aplicación del Reglamento (UE) 2021/821, por el que se establece un régimen de la Unión de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso. Unión Europea, 2022 URL

tanto para la seguridad nacional como para los derechos humanos. El documento destacaba que el *spyware* se utiliza de manera indebida de forma habitual, no sólo en regímenes autoritarios, sino también en contextos democráticos. Incluso en aquel momento la propuesta de Estados Unidos fue más allá. La orden ejecutiva adoptó un enfoque integral que incluyó controles a la exportación y sanciones contra individuos involucrados en operaciones de *spyware.*[13]

No obstante, esto ya parece historia antigua. Si bien se supone que las agencias federales de EE.UU. tienen prohibido utilizar *spyware*, el actual gobierno de Donald Trump reactivó en octubre de 2025 un contrato con Paragon Solutions, a pesar de que los informes muestran que el software espía Graphite, de esta empresa, se ha utilizado contra periodistas, activistas y defensores de derechos humanos en todo el mundo. La sospecha consiste en que el Servicio de Inmigración y Control de Aduanas de Estados Unidos (ICE, Immigration and Customs Enforcement) esté utilizando Graphite para su maquinaria de deportación masiva.[14]

La Organización de las Naciones Unidas también suele tener posiciones oscilantes sobre el tema. La propuesta de su convención sobre ciberdelitos, presentada en septiembre de 2024, generó serias preocupaciones respecto a la legitimación de prácticas de vigilancia. El borrador exige que los Estados adopten facultades para acceder a datos electrónicos e interceptar comunicaciones en tiempo real. Sin embargo, la redacción no establece prohibiciones explícitas sobre la contratación de proveedores privados de *spyware* ni define con suficiente precisión las salvaguardas aplicables. Esto podría permitir que algunos Estados invoquen el

13 The White House. "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security." *The White House*, 27 de marzo de 2023. URL

14 Panagiotopoulos, Vas. "ICE Signs $2 Million Contract With Spyware Maker Paragon Solutions", *Wired*, 2025. URL

tratado para justificar el uso de herramientas de vigilancia altamente intrusivas, lo que podría brindar cobertura legal a prácticas que, en otras circunstancias, serían consideradas abusivas o ilegales.[15]

En resumen, al *Wassenaar Arrangement* se suman otros intentos de regulación coordinado, como la *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware*, lanzada por Estados Unidos en 2023, y el proyecto en curso del *Pall Mall Process*, impulsado sobre todo por Francia y el Reino Unido.[16] Si bien los éxitos a largo plazo de estas iniciativas siguen siendo inciertos, lo que resulta evidente es que no sólo el mercado de la vigilancia está en un momento pujante, sino que además estas herramientas son de relevancia geopolítica. Los distintos gobiernos buscan poseer estas capacidades y además regularlas en beneficio propio, por lo que el interés por los derechos humanos suele ser sólo una ficha de cambio ética en el debate. Documentos filtrados, investigaciones periodísticas, estudios técnicos y solicitudes de acceso a la información han confirmado de manera reiterada la expansión de estas tecnologías.

En este contexto, este reporte busca trazar un mapa del comercio de tecnologías de vigilancia estatal en el Cono Sur de América Latina, identificando las herramientas y las empresas involucradas con el fin de generar conciencia sobre las capacidades actualmente disponibles. Con ello se pretende no sólo facilitar una mejor comprensión de algunas de las herramientas que hoy están en uso, sino además incentivar un proceso de rendición de cuentas a una industria que opera bajo un manto de secretismo.

---

15 Robertson, Kate. "A Global Treaty to Fight Cybercrime—Without Combating Mercenary Spyware." *Lawfare*, Lawfare, 22 de agosto de 2024. URL

16 Bromley, Mark, and Giovanna Maletta. *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint*. SIPRI, 2025. DOI

1.2. Oferta de soluciones: clasificación técnica

Comprender la clasificación técnica de las herramientas comercializadas resulta fundamental para discutir alcances y riesgos de su implementación.

La gama de ofertas es amplia. En buena medida también es común a gobiernos de todo el mundo. Existe de hecho una gran feria internacional —la ISSWorld— en la que participan casi todas las empresas proveedoras y a la que asisten ministros de seguridad de diversos países. Por la variedad de productos y sus capacidades, el menú resulta más que tentador para cualquiera de ellos.[17]

Como hemos señalado, los nombres de los proveedores, filiales, empresas matrices, socios comerciales, revendedores e inversores conforman una red compleja, diseñada en parte para ocultar relaciones, eludir presiones y operar en las zonas grises de la legislación.[18] Al momento de registrar compras aparecen además otros problemas. Muchas veces la certificación de adquisiciones o la ausencia de ellas no dice nada. Hay que considerar que los tratados en materia de seguridad entre distintos países pueden habilitar el uso compartido de herramientas entre agencias. De modo que estas tecnologías pueden ser implementadas sin que medien compras directas.

A esto se suma que los fabricantes ofrecen sólo descripciones muy generales de los productos que comercializan. Incluso si se logra acceder a folletos específicos, la información disponible rara vez resulta precisa.

Existe, de hecho, una constante indeterminación deliberada en torno a la terminología empleada para describir el funcionamiento y las capacidades de estas herramientas. La ambigüedad y el eufemismo resultan recursos centrales de una estrategia retórica que sólo puede superarse a través de consultas directas realizadas desde agencias de seguridad.

Sin ir más lejos, aunque parezca extraño, el término *digital forensics* puede utilizarse para aludir tanto a esperables dispositivos físicos de extracción de datos, como también emplearse como eufemismo para referirse a *spyware* y hablar de extracciones o "allanamientos remotos". De manera similar, *tactical interception* parece remitir a hardware de interceptación por cercanía, pero también figura entre las múltiples etiquetas que las empresas utilizan para referirse a herramientas de *lawful interception* y pueden incluir *spyware* u otras capacidades vagas que amplían la interceptación legal sin tener al proveedor de servicios como intermediario.

Claro, por lo general, la *interceptación legal* es el proceso con base jurídica por el cual un operador de red de comunicaciones o un proveedor de servicios permite a funcionarios autorizados acceder a las comunicaciones de personas

---

17 La exposición Intelligence Support Systems World (ISSWorld) consiste en una serie de conferencias y trainings sobre interceptación legal, vigilancia electrónica e investigación digital, orientadas a fuerzas de seguridad, inteligencia y defensa. DeSombre, Winnona, Lars Gjesvik y Johann Ole Willers. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets." *Atlantic Council*, 8 de noviembre de 2021. URL

18 Roberts, Jen, Trey Herr, Nitansha Bansal y Nancy Messieh. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*. With Emma Taylor, Jean Le Roux, and Sopo Gelava. 2024. URL

u organizaciones.[19] No obstante, bajo esta categoría muchas veces también se suman módulos de inteligencia de tráfico de red o sistemas diseñados para atacar la infraestructura de señalización de las telecomunicaciones.

En consecuencia, lo habitual es que en sus catálogos web las empresas presenten soluciones en apariencia no tan conflictivas, como aquellas vinculadas a minar información de fuentes abiertas o interceptación legal, pero bajo categorías amplias y difusas, mientras que en realidad lo que están vendiendo es otra cosa.

Lo mismo sucede en licitaciones y boletines oficiales. En los pliegos públicos, se emplea un lenguaje cuidadosamente seleccionado para describir tecnologías de vigilancia avanzada y ciberseguridad sin recurrir a términos explícitos que puedan generar controversia. Así, lo que en el ámbito técnico se conoce como "*spyware*" o "software de intrusión" puede suavizarse como "módulo de explotación para análisis forense" o "tecnología de exfiltración de datos". De manera similar, las herramientas de intrusión activa, como los "*exploits*" sin interacción (zero-click), se presentan como "vectores sin intervención del usuario", y los sistemas de captura de señales móviles, conocidos como *IMSI catchers*, se describen como "unidades de monitoreo celular". Estos términos permiten que los pliegos detallen capacidades técnicas avanzadas, como la interceptación de comunicaciones o el acceso remoto, sin hacer referencia directa a prácticas de vigilancia invasiva.

Por esto, adentrarse en su funcionamiento técnico permite el análisis de sus capacidades, sus implicancias y su clasificación.

1.2.1. Spyware, software de intrusión

El *spyware* es un software más o menos sofisticado que puede monitorear de manera oculta información de teléfonos, computadoras o servidores, proporcionando acceso al dispositivo y permitiendo la exfiltración subrepticia de datos.

Su instalación inicial puede requerir acceso físico al equipo —como ocurre con los programas de control parental, las herramientas utilizadas por empresas para la supervisión de empleadxs o los *stalkerware* (que es el término para referirse al *spyware* utilizado en situaciones de acoso). Otros tipos de *spyware* solo requieren que la víctima haga clic en un enlace para iniciar la infección, mientras que las variantes más avanzadas pueden ejecutarse sin que el usuarix realice ninguna acción.

En la actualidad, el software Pegasus de NSO Group resulta el ejemplo más conocido, aunque en América Latina han circulado muchos otros, producidos por compañías como Hacking Team (Italia), Mollitiam (España), Cy4gate (Italia), Intellexa (Chipre/Israel) o FinFisher (Reino Unido/Alemania).[20] Cabe destacar que, en el marco de este reporte, sólo nos interesa el *spyware* utilizado por agencias de seguridad, y no aquel vinculado al llamado cibercrimen (para fraudes o ataques no dirigidos con fines de lucro).

---

19 Frost & Sullivan. *Lawful Interception: A Mounting Challenge for Service Providers and Governments.* London, 2011. URL

20 Una buena recopilación de los sistemas de *spyware,* sus años de uso y su revelación pública puede encontrarse en el data-set provisto por la investigación de Feldstein, Steven, y Brian Kot. *Global Inventory of Commercial Spyware & Digital Forensics*, marzo de 2023. DOI

Si bien existían antecedentes previos, las alertas sobre el tema comenzaron a emerger alrededor de 2015, cuando, tras la filtración de correos electrónicos de la empresa italiana Hacking Team, la Comisión Interamericana de Derechos Humanos (CIDH) publicó un comunicado de prensa en el que expresaba su preocupación por los riesgos que estas tecnologías representan para los derechos humanos.[21]

A menudo, estas empresas se autodefinen como proveedoras de *lawful interception* o *tactical interception*, alegando que venden únicamente a clientes con necesidades legítimas de vigilancia, como agencias de seguridad e inteligencia.[22] En la práctica, han sido utilizadas de forma reiterada para vigilar a defensorxs de derechos humanos, periodistas, académicxs, políticxs e incluso empresarixs. Los ejemplos alrededor del globo son muchos.

Con todo, estas empresas no trabajan solas. La producción de *spyware* se monta sobre toda una industria millonaria que le es subsidiaria y está destinada a detectar y comercializar nuevas vulnerabilidades, producir *exploits* para sacar provecho de ellas y proveer la infraestructura necesaria para la exfiltración de datos.[23] Todo como parte de una cadena de ataque más amplia. Por eso, si bien las empresas productoras de *spyware* están ubicadas sobre todo en Israel, Italia e India, muchas veces las compañías dentro de este circuito que buscan vulnerabilidades y producen *exploits* están radicadas en Latinoamérica y obtienen recursos humanos capacitados en estos mismos países.

En algunos pocos países, el uso estatal de *spyware* está regulado bajo ciertas condiciones. En estos casos, suelen emplearse eufemismos como "adquisición remota de evidencia" y otras variaciones. De distintos modos, Alemania, Francia, Italia y España han establecido marcos que permiten su uso en el contexto de investigaciones criminales complejas. Una selección de referencias críticas muestra que allí donde el uso de *spyware* estatal ha buscado ser "normalizado" jurídicamente, también se han generado fuertes controversias. En Alemania, las reformas al *Bundeskriminalamtgesetz* y la regulación de la *Online-Durchsuchung* ("allanamiento en línea") establecen el uso gubernamental de "troyanos estatales" como medida de investigación excepcional sujeta a orden judicial y requisitos de proporcionalidad.[24] En Italia, el Decreto Legislativo 216/2017 incorporó los *captatori informatici* ("captadores informáticos") como técnica de investigación a distancia en ciertos delitos graves. Por su parte, España reguló también el acceso remoto a equipos, la interceptación en línea y otras medidas tecnológicas

---

21 Comisión Interamericana de Derechos Humanos (CIDH), Relatoría Especial para la Libertad de Expresión, *Informe Anual de la Comisión Interamericana de Derechos Humanos 2015: Volumen II, Informe de la Relatoría Especial para la Libertad de Expresión*, OEA/Ser.L/V/II. Doc. 48/15, 31 de diciembre de 2015, URL

22 Por ejemplo, NSO Group aclara que sólo comercializa sus productos a agencias de seguridad legítimas, que no se responsabilizan por el uso final de sus productos y que no tiene acceso a los datos recopilados por sus clientes. NSO Group. *Transparency and Responsibility Report*. NSO Group, 2021. URL

23 Para un análisis del mercado de vulnerabilidades a partir de las filtraciones de la empresa italiana Hacking Team, ver: Burkart, Patrick, y Tom McCourt. "The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software." *Popular Communication* 15, n.º 1 (2017): 37–54. DOI

24 European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, *The Use of Pegasus and Equivalent Surveillance Spyware: The Existing Legal Framework in EU Member States for the Acquisition and Use of Pegasus and Equivalent Surveillance Spyware* (Bruselas, 2022). URL

mediante la Ley Orgánica 13/2015. Mientras que en Francia la Ley de Inteligencia de 2015 habilitó técnicas intrusivas de vigilancia bajo supervisión administrativa de una autoridad específica. En todos estos casos, la bibliografía coincide en que, aun con marcos legales formales, persisten tensiones sobre transparencia, control democrático y riesgo de "normalizar" el malware estatal como herramienta ordinaria de investigación.[25]

En resumen, incluso en contextos institucionalizados, el empleo de estas tecnologías sigue siendo sumamente controvertido, debido a su capacidad intrusiva y al considerable riesgo de abusos. Amnistía Internacional clasifica, de hecho, el *spyware* como "altamente invasivo", basándose en que, desde un punto de vista técnico, está diseñado para no dejar registros, operar de forma subrepticia sin mayores controles y obtener sin filtro la mayor cantidad posible de datos.[26]

En general, además, no incorporan salvaguardas que protejan los derechos de lxs usuarixs, sino sólo el modelo de negocios del fabricante y el vendedor. Una investigación reciente mostró, en efecto, que compañías como Intellexa mantienen acceso directo a la información recolectada por los compradores de sus sistemas de *spyware.*[27]

---

25 Ramiro, André. "Democratic Oversight of Government Hacking by Intelligence Agencies: A Critical Analysis of Brazil and Germany." *Weizenbaum Journal of the Digital Society* 5, n.º 2 (2025). DOI // J. J. van Berkel, A. van Uden y J.H. Goes, *Police Hacking Regulation Abroad: A Comparative Law Study into Legal Regulations and Safeguards Regarding the Quality of Data* (The Hague: WODC, 2023). URL

26 Amnesty International Security Lab, "Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products", 2023. URL

27 Amnesty International Security Lab, "To Catch a Predator: Leak Exposes the Internal Operations of Intellexa's Mercenary Spyware", 4 de diciembre de 2025. URL.

Box 1: *Spyware* / software de intrusión

Spyware	
Intrusión	Remota en dispositivos móviles.
Infección	Por explotación de vulnerabilidades 0-day, 1-day, N-day; *phishing*; instalación física (*stalkerware*, control parental); inyección de tráfico malicioso.
Tipo de ataque	Activo y dirigido.
Infraestructura necesaria	Todas las vinculadas a las distintas fases del ataque, desde la infección hasta los posibles nodos de anonimización y el monitoreo.
Tipo de acceso	Control remoto; espionaje personalizado; exfiltración de información.
Datos recolectados	Archivos, mensajes, localización, cámara.
Ejemplos en Sudamérica	Pegasus (NSO), Remote Control Access (Hacking Team), *Night Crawler* (Mollitiam), etc.

Spyware: línea de tiempo

2007

- Agencias de seguridad alemanas comienzan a usar el troyano de vigilancia "Skype Capture Unit" desarrollado por DigiTask, conocido con los nombres de "Bundestrojaner" y "R2D2".

A PARTIR DE 2010

- Expansión temprana del *spyware* comercial *(ej.: FinFisher)*.

2012

- Primeros reportes de Citizen Lab sobre FinFisher y Hacking Team.
- Se incluye el *spyware* dentro del *Wasserman Agreement*.
- Comienza el uso de Pegasus de NSO Group en Panamá.
- Comienza el uso de FinFisher en Paraguay.

2013

- Primeros usos de Hacking Team en Colombia, México, Ecuador y Honduras.
- Contactos de NSO Group (Israel) y Hacking Team (Italia) con los gobiernos de toda Sudamérica, entre ellos Chile, Argentina y Uruguay.

2014

- Chile adquiere el *spyware* de Hacking Team.
- Argentina intenta legalizar a nivel federal la "vigilancia remota sobre equipos informáticos" y mantiene negociaciones con NSO Group y Hacking Team.
- México adquiere el *spyware* FinFisher.

2015

- Filtración de correos electrónicos de Hacking Team.

2016

- Comienzan las primeras investigaciones periodísticas y reportes sobre *spyware* en América
- México adquiere Pegasus de NSO Group.
- Citizen Lab publica el primer informe forense público sobre Pegasus, identificando la infraestructura de NSO a partir de un caso concreto.

2017

- Primeros reportes de la sociedad civil que muestran el uso de *spyware* contra periodistas, activistas y políticxs a partir de muestras forenses de sus dispositivos.

2018

- Primer reporte de Security Lab de Amnesty Internacional sobre NSO.

2019

- Divulgación pública de que Brasil había adquirido RCS de Hacking Team años antes.
- WhatsApp/Meta demanda a NSO Group.
- La Comisión Interamericana de Derechos Humanos (CIDH) presenta su preocupación por los riesgos que representa el *spyware* para los derecho

2020

- Se comienza a usar Pegasus en El Salvador.

2021

- Amnesty Tech y Forbidden Stories publican, junto a una red de medios, *The Pegasus Project*: una filtración masiva y verificación forense de infecciones y objetivos en distintas partes del mundo.
- Apple demanda a NSO Group por aprovechar vulnerabilidades de iOS/iMessage para abusar de sus servicios e infectar dispositivos.
- Se conoce el uso de *spyware* desarrollado por Mollitiam y Cytrox en Colombia.
- México adquirió REIGN, el *spyware* de la empresa israelí Quadream.
- El Security Lab de Amnesty International lanza *Mobile Verification Tool* (MVT) una herramienta de análisis forense para identificar indicadores de compromiso (IOC, Indicator of Compromise) en teléfonos celulares de manera consensuada.

1.2.2. Inteligencia de señales / *Signaling Intelligence* (SIGINT)

El término abarca herramientas para la interceptación, el monitoreo, el análisis y la geolocalización de señales electromagnéticas. Esto incluye una amplia variedad de equipos empleados por agencias de seguridad: inhibidores (*jammers*) para bloquear o degradar comunicaciones en bandas específicas; analizadores de espectro para visualizar y caracterizar señales en distintas frecuencias; y sistemas de localización por dirección (DF — *Direction Finding*), como antenas portátiles que estiman la dirección de una emisión, entre otros.

En el presente informe nos referiremos a dos tecnologías concretas utilizadas para la interceptación, monitoreo y localización de dispositivos: los *IMSI catchers* y las herramientas de geolocalización que explotan el protocolo del sistema de señalización SS7.

(1.2.2.a.) *IMSI catcher*, *signaling catcher* e interceptación de señales de teléfonos móviles

Los *IMSI catchers* se utilizan en muchas partes del mundo. Al menos en comparación con lo que sucede con otras de las herramientas analizadas, su comercialización, entre fabricantes, revendedores y agencias de seguridad, suele hacerse de manera *bastante* pública. Consisten en antenas de celulares con buena señal que se hacen pasar por antenas legítimas de la empresa proveedora de telefonía con el fin de registrar los números de identificación de los teléfonos móviles que se conectan a ellas. Esto era posible porque en GSM/2G el protocolo sólo exigía que el teléfono se autenticara frente a la red, pero no exigía que la estación base se autenticara frente al teléfono, de modo que el dispositivo confiaba en cualquier antena que cumpliera la forma del protocolo. En 3G y 4G se introduce autenticación mutua entre red y terminal, pero en la práctica muchos *IMSI-catchers* comerciales fuerzan a los teléfonos a degradarse a 2G. Además, investigaciones recientes muestran que también es posible construir *IMSI-catchers* sobre LTE/4G que permiten al menos identificar dispositivos.[28] Es importante tener en cuenta que los *IMSI catchers* también se apoyan en debilidades de diseño de GSM/2G y en la posibilidad de degradar las conexiones 3G/4G hacia modos menos seguros, además de aprovechar características del protocolo y de la implementación que permiten identificar y localizar dispositivos.[29]

---

28 En 5G se introduce el identificador oculto (SUCI), que cifra la identidad permanente del abonado (SUPI) para impedir que los *IMSI-catchers* clásicos vean esa identidad. Sin embargo, trabajos recientes han demostrado ataques llamados *'SUCI-catchers'*, en los que una antena falsa usa el propio protocolo de autenticación de 5G para comprobar si un SUCI concreto corresponde a un abonado determinado o si un mismo usuario está presente en un lugar, lo que permite formas más avanzadas de rastreo pese a las mejoras de privacidad. Merlin Chlosta, David Rupprecht, Christina Pöpper y Thorsten Holz, "5G SUCI-Catchers: Still Catching Them All?," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. New York: ACM, 2021, 359–364, DOI

29 Audun Jøsang, Laurent Miralabé y Léonard Dallot, "Vulnerability by Design in Mobile Network Security," *Journal of Information Warfare* 14, n.º 4 (2015): 86–98, URL

En concreto, estos artefactos capturan tanto la identidad del suscriptor vinculada a la tarjeta SIM (o IMSI, *International Mobile Subscriber Identity*) como el identificador internacional del dispositivo (IMEI, *International Mobile Equipment Identity*).

Cuando estas antenas son instaladas en ubicaciones estratégicas por fuerzas de seguridad, pueden, por ejemplo, identificar a todxs lxs participantes en una manifestación, interrumpir servicios o, en algunos casos, incluso degradar la conexión de 4G a versiones menos seguras como 3G o 2G para poder interceptar mensajes de texto.[30]

Los productores de este tipo de hardware son muchos, e incluso existen fabricaciones locales en plantas industriales de países que no suelen desarrollar otro tipo de tecnología de interceptación. No obstante, existe un reconocido cúmulo de fabricantes que exportan *IMSI catchers* a todo el mundo, como: Almenta, L3Harris, Pat Systems, Pen-Link y Verint de los Estados Unidos; Kavit, Pisces, Septier y Phantom de Israel; a lo que se suman algunos más, como Elaman (Alemania), Neosoft (Suiza), Tykelab (Italia), X-Surveillance (Países Bajos) y Smith Myers y Revector (Reino Unido).

---

30 Park, Shinjo, Altaf Shaik, Ravishankar Borgaonkar y Jean-Pierre Seifert. "Anatomy of Commercial IMSI Catchers and Detectors." Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society (New York, NY, USA), WPES'19, Association for Computing Machinery, 11 de noviembre de 2019, 74–86. DOI

Box 2: ¿Cómo funciona un *IMSI catcher*?

Definición	**Antena móvil o fija que se hace pasar por una antena legítima del proveedor de telefonía para identificar y localizar teléfonos en un área determinada.**
Conexión	Emite como una antena con buena señal. Los teléfonos se conectan automáticamente como si se tratara de una antena del proveedor de servicios.
Identificación	Captura IMSI, IMEI y, según el modelo, también metadatos de conexión.
Localización	Mediante *Direction Finding* (DF), potencia de señal y movimiento, permite seguir objetivos específicos.
Capacidades avanzadas	Puede bloquear la conexión, degradar el tipo de conexión (a 3G o 2G) y facilitar la interceptación de llamadas y SMS.
Impacto	Opera de forma indiscriminada. Registra todos los dispositivos en la zona.

(1.2.2.b.) Ataques mediante la señalización de telefonía - *Signaling Attacks*

Estas herramientas suelen operar sobre la infraestructura de señalización de la red móvil y su interconexión global. Explotan vulnerabilidades en los protocolos de señalización SS7 y/o Diameter utilizados en la infraestructura de redes móviles e interconexiones internacionales (2G, 3G y 4G).[31]

SS7 es el sistema de señalización de la red telefónica clásica y se usa tanto en telefonía fija como en el núcleo de redes móviles 2G/3G. En LTE/4G y parte de 5G, el protocolo de señalización central pasa a ser Diameter, aunque SS7 sigue siendo necesario para interconectar estos servicios con las redes heredadas y para ciertos escenarios de roaming. El problema no radica sólo en vulnerabilidades intrínsecas de los protocolos, sino también en el despliegue de infraestruc-

31 Holtmanns, Silke, Siddharth Prakash Rao e Ian Oliver. "User Location Tracking Attacks for LTE Networks Using the Interworking Functionality." *2016 IFIP Networking Conference (IFIP Networking) and Workshops*, Mayo de 2016, 315–22. DOI // Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis y Ron Deibert. *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*. Citizen Lab Research Report N.º 133. University of Toronto, 2020. URL

tura con configuraciones inseguras que implementan —y permiten— los operadores telefónicos.[32]

Las tecnologías adquiridas por agencias de seguridad envían mensajes normalmente diseñados para el roaming internacional. Estos mensajes explotan vulnerabilidades en los protocolos SS7 y Diameter y permiten obtener la localización de abonados móviles mediante mensajes de señalización como *sendRoutingInfoForSM* o *ProvideSubscriberInfo*. Al enviar solicitudes de señalización, pueden rastrear de forma remota la ubicación del dispositivo sin el consentimiento del operador de red, monitorear sus desplazamientos internacionales mediante los servicios de roaming e identificar cuándo están activos.

Además, pueden enviar solicitudes de manera continua que generan ataques de denegación de servicios (DoS) hasta forzar la desconexión de la red y bloquear temporalmente las comunicaciones del teléfono. También pueden manipular las rutas de señalización para desviar llamadas o mensajes de texto. Esto suele lograrse enviando una indicación de desvío a la red para engañar al nodo de origen y hacer que vuelva a enrutar el tráfico a un dispositivo específico controlado por la agencia de seguridad. Así se puede interceptar SMS y comprometer su uso como segundo factor de autenticación (2FA). No obstante, en la práctica, aparentemente las agencias de seguridad emplean estas herramientas sobre todo para la geolocalización de números/usuarixs específicos.[33]

Informes técnicos recientes —como el citado estudio *Finding You* del Citizen Lab, elaborado con datos de la plataforma Mobile Surveillance Monitor (MSM)— documentan la existencia de empresas privadas que venden como servicio a actores estatales este tipo de tráfico anómalo para geolocalizar objetivos a escala global. En este caso, no hace falta que las agencias de seguridad adquieran necesariamente equipo o software para realizar este tipo de ataques de interceptación. Muchas veces, pueden adquirir el servicio a alguna de estas empresas y pagar por una cantidad de consultas que derivan de manera remota y generan una respuesta casi inmediata.[34]

También NSO Group produce una de las herramientas más conocidas en este rubro con el nombre de Circles, entre otras empresas comercializan productos similares en América Latina, como Ability (Israel), Pat Systems (EE. UU.), Rayzone (Israel), Telesoft (Reino Unido), Tykelab (Italia), Elaman (Alemania) y Verint / Cognyte (EE. UU. / Israel).

---

32 Es fundamental ver los datasets del "Network Research Workbook", que no sólo reportan la cantidad de eventos sospechosos, sino que además registran la infraestructura vulnerable que posibilita estos ataques: URL

33 Miller, Gary, and Christopher Parsons. *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure*. N.º 171. Citizen Lab, University of Toronto, 2023. URL

34 Lighthouse Reports. *Surveillance Secrets: How First Wap Tracks Phones Around the World.* Lighthouse, 2025. URL

Box 3: *Signaling Attacks* mediante SS7 / Diameter — ¿Cómo funcionan?

¿Qué son SS7 y Diameter?	Son protocolos utilizados entre proveedores de telefonía para: • saber en qué antena está un teléfono y enviar la información que le corresponde; • activar roaming; • enrutar llamadas y SMS.			
¿Cómo es el ataque?	**1** El teléfono se conecta normalmente a la empresa de telefonía.	**2** Las empresas de telefonía se envían mensajes mediante SS7 o Diameter para gestionar ubicación, llamadas y SMS de cada número.	**3** Un atacante logra enviar mensajes a través de infraestructura vulnerable, haciéndose pasar por una empresa legítima.	**4** La red confía en esos mensajes falsos y, según el mensaje, responde con cierta información.
Con esto, el atacante puede:	**A.** Saber dónde está un dispositivo ➜ La red responde y da una ubicación aproximada	**B.** En ciertos casos, usando sólo las señales internas de control, se puede averiguar información extra sobre el tráfico vinculado a ese número. ➜ El atacante puede enviar consultas “normales”, pero con intención de vigilancia (por ejemplo, mensajes que piden información de enrutamiento o estado de un número). A partir de esas respuestas, el atacante puede reconstruir en qué momentos se generan eventos, cuándo y desde dónde se comunica el objetivo.	**C.** Mediante los mismos mensajes de control se podría interferir o redirigir SMS o afectar llamadas. ➜ El atacante envía mensajes SS7 falsos que indican cambiar parámetros de enrutamiento (por ejemplo, dónde entregar los SMS). ➜ La red actualiza sus registros como si fuera una operación legítima. Los SMS pasan por una infraestructura controlada por el atacante antes de llegar al usuarix, o directamente nunca llegan.	
Entonces:	El ataque funciona haciendo consultas al sistema de señales internas entre empresas de telefonía mediante acceso al protocolo SS7 o Diameter.	Es decir: SS7/Diameter no transportan el contenido de las comunicaciones, sino las instrucciones internas que permiten que esas comunicaciones funcionen.	Aunque potencialmente podría denegar el servicio e interceptar llamadas y mensajes, el ataque se utiliza fundamentalmente como herramienta de geolocalización.	

1.2.3. Interceptación legal *(Lawful Interception - LI)* e inteligencia de red

Las tecnologías llamadas de interceptación legal se integran en la infraestructura del proveedor de servicios de comunicaciones. Su objetivo es la interceptación selectiva bajo una autorización formal según la legislación de cada país. Por lo general, se trata de herramientas adquiridas por fuerzas de seguridad —a las que también pueden tener acceso las agencias de inteligencia— que se implementan en la red del operador. Los proveedores deben cumplir a nivel estructural con requisitos de interceptación para permitir la vigilancia legal y las fuerzas de seguridad adquieren sistemas de monitoreo y análisis a los que el operador entrega la información interceptada mediante interfaces estandarizadas.[35] Innova de Italia, SS8 de Estados Unidos o Trovicor de Alemania constituyen buenos ejemplos de tecnologías de *lawful interception.*[36]

Además de la capacidad base de interceptación y entrega regulatoria, muchas de las herramientas comercializadas combinan LI con una analítica de inteligencia orientada a investigación (a veces presentada como *lawful intelligence* o "inteligencia de red"). De modo que se le pueden sumar otras fuentes, por ejemplo, producto del monitoreo de comunicaciones que hacen los proveedores de servicio.

En la práctica, esto suele materializarse como un centro de monitoreo para fuerzas de seguridad que no solo procesa la información estandarizada de interceptación legal, sino que también reconstruye comunicaciones, habilita búsquedas y filtrado, y permite correlacionar y enriquecer la información con datos de ubicación, para generar dossiers, vínculos, perfiles, series temporales y alertas. Este uso de "inteligencia de red" apunta a convertir grandes volúmenes de información de tráfico en insumos para una investigación. La inteligencia de red constituye entonces una capa de analítica que agrega correlación, enriquecimiento y procesamiento avanzado, para convertir esos datos en patrones, per-

---

35 En las normas ETSI, estos módulos estandarizados adquieren los nombres de HI2/HI3 para IRI/CC. HI2 e HI3 ("Handover Interfaces") son las interfaces de entrega definidas en estándares de interceptación. HI2: canal por el que se entrega IRI (Intercept Related Information), es decir, metadatos del evento (por ejemplo: quién se comunica con quién, cuándo, desde dónde, identificadores, etc.; no necesariamente el contenido). HI3: canal por el que se entrega CC (Content of Communication), o sea el contenido de la comunicación (voz/datos/mensajes, según el caso y autorización).

36 En el ámbito técnico-político actual, el término *SORM provider* (*Sistema Operativo de Medidas de Investigación*, del ruso COPM) se utiliza para describir a las empresas que diseñan, instalan o mantienen plataformas de interceptación legal de comunicaciones (*Lawful Interception Systems*) integradas directamente en las redes de los operadores para capturar contenido y metadatos de tráfico. En términos técnicos, *SORM* y *Lawful Interception* cumplen funciones equivalentes. Con todo, el primero se asocia históricamente a infraestructuras rusas de vigilancia estatal con acceso directo a las redes, mientras que el segundo designa sistemas regulados y auditables de interceptación legal conforme a estándares internacionales. Por lo general, se utiliza entonces el término SORM para referirse a tecnologías de origen ruso, para destacar la posibilidad de que las comunicaciones interceptadas por estos sistemas estén directamente accesibles para el servicio federal de seguridad del Estado ruso.

files, tendencias y detección de anomalías.[37] En general, operan mediante el acceso a la infraestructura, duplican o desvían el tráfico hacia funciones internas de interceptación/mediación, realizan inspección de paquetes y, según el producto, permiten el rastreo en tiempo real de la ubicación de dispositivos y el acceso a metadatos de tráfico.

La mayoría de las herramientas de este tipo requieren, en efecto, la colaboración de los proveedores de servicios y presuponen integración y mediación dentro de la red o acceso privilegiado a sus puntos de captura. Sin embargo, existe poca transparencia pública sobre la colaboración concreta y el alcance real de capacidades en cada despliegue. Sus métodos no suelen estar documentados y las especificaciones de algunas de estas herramientas insinúan estar diseñadas para conectarse a la infraestructura sin mediar permisos.[38]

Incluso cuando se puede acceder a la documentación oficial, una vez más, las descripciones de las capacidades de estas herramientas resultan ambiguas. Por ejemplo, en un catálogo de 2013, la empresa italiana Innova afirmaba que su producto EGO podía capturar comunicaciones IP mediante acceso a la infraestructura de red y decodificar y reconstruir el contenido de esas comunicaciones dentro de su interfaz. Para operar, EGO requería conexión con la infraestructura de red (proveedores, nodos intermediarios, puntos de cruce IP) para desviar el tráfico hacia el sistema de interceptación.[39] Con todo, no existe información pública verificada sobre sus métodos y capacidades, por lo que no están claras las capacidades de los distintos módulos de EGO que se siguen desarrollando hasta hoy.

La compañía alemana Trovicor es uno de los proveedores históricos de interceptación legal y ofrece elementos que se conectan al core de los operadores frente a pedidos de agencias de seguridad.[40] Del mismo modo, la compañía SS8 de EE.UU. ofrece soluciones de mediación e interceptación integrables. También empresas como Ericsson, Nokia, Utimaco y Verint/Cognyte han ofrecido (o inte-

---

37 Ver, por ejemplo, las especificaciones de estos productos en este rubro del mercado: Brookcourt Solutions Limited, "Intellego XT Monitoring Centre - SS8," Digital Marketplace (G-Cloud 14), URL; Cognyte, "Network Intelligence Solutions," URL

38 Resulta razonable suponer que se apoyan en técnicas similares a las que fueron documentadas en sistemas como los desarrollados por la Intellexa Alliance. Entre las técnicas reportadas se incluyen: inspección detallada de paquetes integrada con otras herramientas de interceptación; y sistemas de análisis de metadatos capaces de registrar los patrones distintivos de tráfico de red que se generan cada vez que un teléfono recibe un nuevo mensaje cifrado o una notificación de una aplicación de mensajería, con el objetivo de identificarlos. Para el acceso a tráfico cifrado, existen técnicas de manipulación de DNS y certificados SSL/TLS que se usan entre le usuarix y el servicio utilizado en colaboración con proveedores de servicios de internet. Amnesty Tech. "Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products." *Amnesty International Security Lab*, 6 de octubre de 2023. URL

39 Según su manual, el sistema EGO de Innova S.p.A. es una plataforma modular y escalable de interceptación legal que integra interfaces para telefonía fija y móvil, datos IP, email, MMS y comunicaciones de vídeo, permite la grabación de conversaciones, metadatos y localización GPS, dispone de un repositorio con marca temporal y firma digital para asegurar integridad, maneja casos, usuarios y auditorías centralizadas, y se adapta mediante APIs a nuevos formatos de red y transporte. El manual técnico de Innova (2011) y fuentes secundarias indican que EGO "enables to intercept, decode and restore on the same interface all types of IP communication, such as Video-communications, MMS..." Innova. "Investigations Instruments." Innova, 2013. URL

40 Trovicor. "Trovicor Intelligence Solutions." Trovicor, 2012. URL

grado) productos y componentes vinculados a la entrega regulatoria que involucra la interceptación legal.[41]

A nivel regional, el gobierno de Perú adquirió una herramienta de la compañía israelí Verint/Cognyte —a la que se le dio el nombre de Pisco— por unos 22 millones de dólares, destinada a interceptar y monitorear comunicaciones satelitales, de voz y de datos IP, lo que generó denuncias por vulnerar la privacidad de millones de ciudadanxs.[42] En la cobertura del proyecto, se menciona además que los productos adquiridos incluyen Reliant y Vantage, que son herramientas diseñadas para "interceptar, filtrar y analizar grandes volúmenes de tráfico de IP, voz y comunicación satelital".[43] Es probable que estos productos también se utilicen en otros países de la región.

Cabe destacar que muchas veces estas empresas producen distintos tipos de módulos que van desde la interceptación legal al análisis y monitoreo de tráfico de red. Por ejemplo, NarusInsight se describe como una plataforma para captura desde la red troncal de alta capacidad o *backbone*. Menciona que el tráfico interceptado puede fluir hacia un componente de interceptación (NarusInsight Intercept Suite) para almacenamiento y análisis con fines forenses o de vigilancia, mientras otros módulos se presentan como orientados a la *traffic intelligence* para gestión y seguridad de red.[44]

Las alertas sobre este tipo de tecnologías de interceptación de tráfico IP resultan tempranas y se remontan a los momentos de ampliación de acceso a internet en el cambio de siglo. En 2005, regulaciones mencionadas como CALEA (*Communications Assistance for Law Enforcement Act*) en Estados Unidos fueron ampliadas para abarcar también a proveedores de banda ancha, obligándolos a asegurar capacidades de interceptación en sus redes.[45] La advertencia inicial surgió de un caso emblemático alrededor de la empresa Narus, que desarrolló sistemas avanzados de inspección profunda de paquetes capaces de analizar grandes volúmenes de tráfico en tiempo real.[46] Ya en el 2006, su tecnología se volvió controvertida cuando se reveló que había sido utilizada por la NSA en colaboración con AT&T para realizar vigilancia masiva de comunicaciones.[47]

Más cerca en el tiempo, investigaciones de Citizen Lab mostraron casos de redirección de tráfico desde el proveedor de servicios mediante módulos de

---

41 Global Market Insights Inc. "Lawful Interception Market Size, Share, Trends & Forecasts 2034." 2025. URL

42 Associated Press, "*In Peru, Govt Buys Secret Tool for Mass Surveillance*", citado en EFF – Surveillance in Latin America: 2016 in Review, 2 de enero de 2017. URL

43 Bajak, Frank, and Jack Gillum. "With Cheap Israeli Spy Tools, Nations Are 'Monitoring Everyone.'" *The Times of Israel*, 3 de agosto de 2016. URL

44 IMB. "NarusInsight." IMB, 2009. URL // Sandvine. "PacketLogic 8000 PlatformsTM Scalable Network Intelligence and Policy Enforcement Platform." Sandvine, 2019. URL

45 Electronic Frontier Foundation. "FAQ on the CALEA Expansion by the FCC." *Electronic Frontier Foundation*, 2007. Consultado el 8 de diciembre de 2025. URL

46 Staff, WIRED. "Stumbling Into a Spy Scandal." Tags. *Wired*, 17 de mayo de 2006. URL

47 Según el testimonio del extécnico de AT&T Mark Klein, se empleaban dispositivos Narus STA 6400 para copiar y monitorear el tráfico hacia la NSA. "NARUS, Deep Packet Inspection and the NSA." *Privacy SOS*, 2013. URL

inspección profunda de paquetes, incluyendo inyección de tráfico para la instalación de *spyware*. Desde ya, esto no entraría en lo que se entiende como interceptación legal estándar según normativas europeas (ETSI), pero sí ilustra cómo capacidades en la capa de red pueden usarse con fines de vigilancia o manipulación.[48]

En este marco, sirve tener en cuenta el reporte de transparencia publicado en el 2014 por Vodafone, una de las mayores empresas de telecomunicaciones del mundo. Su informe explicaba cómo varían sus procedimientos frente a solicitudes de datos de clientes según el marco regulatorio de cada país en el que opera. Estos informes dividen en dos tipos los pedidos de información:

(1) Información sobre comunicaciones vinculadas a determinado evento, que implica la identificación de un usuarix (mediante un número de teléfono o una dirección IP), la duración de un llamado o la localización de un dispositivo y otros metadatos, pero no el contenido de la comunicación en sí misma.

(2) En segundo lugar, los pedidos de *lawful interception* (LI) que, según Vodafone, son menos comunes y sí exigen acceder al contenido de las comunicaciones.[49]

Como dijimos, en principio la mayoría de estas herramientas requieren de la colaboración de los proveedores de servicio de internet.[50] Sin embargo, aparecen ciertas dudas sobre su implementación y uso, en particular cuando hay opacidad contractual, prácticas digitales autoritarias o un control débil sobre las fuerzas de seguridad y agencias de inteligencia.

Sobre esto, la investigación académica muestra que, si un actor controla físicamente un punto de tránsito internacional o un nodo donde convergen muchas redes, puede aumentar de forma significativa su capacidad de observación/manipulación del tráfico que pasa por ese punto, aun sin cooperación plena del proveedor de internet (ISP).[51] Por esto resulta importante mencionar que existe una seria duda sobre la posibilidad efectiva de utilizar este tipo de herramientas sin la mediación del proveedor de servicio de Internet; así como la descripción de algunas de estas herramientas también sugiere que resultan independientes de pedidos formales.

---

48 Citizen Lab documenta, mediante escaneos de Internet, análisis forense de equipos PacketLogic de segunda mano y pruebas de laboratorio, que dispositivos DPI (PacketLogic) desplegados en redes de operadores —principalmente en Türk Telekom y en puntos de Telecom Egypt— se utilizaron para redirigir descargas legítimas hacia instaladores maliciosos de spyware. Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, y Ron Deibert. BAD TRAFFIC: *Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?* Citizen Lab Research Report N.º 107. University of Toronto, 2018. URL

49 Vodafone y Hogan Lovells. *Law Enforcement Disclosure Report*. Vodafone, 2015. URL

50 Ericsson. Regulatory Products: Communication Services UDM and Exposure. Ericsson, 2020. URL // Sandvine. *Sandvine Datasheet: PacketLogic15000 Platform*. Sandvine. URL // SS8. "Solutions: Compliant Mediation and Interception." SS8, 2021 URL

51 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies y James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," The Guardian, 21 de junio de 2013, URL // Murdoch, Steven J., y Roger Dingledine. "Sampled Traffic Analysis by Internet-Exchange-Level Adversaries." *Proceedings of the PET '07 Workshop on Privacy Enhancing Technologies* (2007). En este artículo se postula que un adversario que controle un IXP por donde pasa el tráfico entre cliente y servidor puede analizarlo incluso cuando no coopera el ISP original. URL

El influyente artículo de 2014 titulado *"Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet"* analizaba cómo el FBI puede acceder a comunicaciones explotando vulnerabilidades en redes más allá del camino legal.[52] Con esto, se refuerza la idea de que el acceso a las comunicaciones puede utilizar otras herramientas asociadas en combinaciones de control de infraestructura, explotación de vulnerabilidades y herramientas de intrusión. El informe de Citizen Lab recién citado constituye en efecto un buen ejemplo de esto.

Los estándares técnicos elaborados por el *European Telecommunications Standards Institute* (ETSI) sobre interceptación legal establecen, por estos motivos, que los "sistemas de las fuerzas del orden" nunca deben integrarse "directamente en la arquitectura de la red pública", con el fin de preservar la separación entre las funciones de red y las de monitoreo.[53] En Estados Unidos, en cambio, no existe un organismo único equivalente a ETSI que publique una arquitectura exhaustiva de interceptación legal. El marco se estructura en torno a CALEA, que fija obligaciones funcionales para los operadores, mientras que las especificaciones técnicas se desarrollan en organismos de estandarización de la industria (frecuentemente acreditados por el American National Standards Institute - ANSI). Estos estándares dejan un margen amplio de diseño a fabricantes y operadores sobre cómo integrar las capacidades de interceptación en redes concretas. Desde ya, aunque las herramientas comercializadas indiquen que cumplen con las normas ETSI y/o ANSI, eso no garantiza por sí solo su adecuación en los países de América del Sur, donde los marcos legales, regulatorios y de control pueden diferir (o ser menos transparentes).

Además, muchas veces puede existir un uso discrecional de los pedidos de interceptación legal. Si las fuerzas de seguridad y las agencias de inteligencia carecen de controles efectivos, los sistemas de interceptación pueden utilizarse por fuera de los mecanismos regulatorios formales. Por ejemplo, en 2008, CIPER publicó un reportaje que describe cómo funcionan las interceptaciones telefónicas legales en Chile y señala que, además del circuito formal que involucra una orden judicial y la colaboración de las compañías telefónicas, también han existido métodos paralelos o informales de obtención de comunicaciones. Esto muestra que, aun cuando el sistema esté técnicamente bien implementado, la falta de controles sobre su uso puede derivar en accesos indebidos o prácticas discrecionales.[54]

Sobre este punto, la literatura académica sostiene que las herramientas de interceptación, análisis y retención de información de comunicaciones, habilitadas por las legislaciones en casi todos los países, pueden resultar tan riesgosas en términos políticos como las que involucran ataques para comprometer dispositivos[55].

---

52 En el 2014, este paper explicaba "the viability and implications of an alternative method for addressing law enforcement's need to access communications: legalized hacking of target devices through existing vulnerabilities in end-user software and platforms. The FBI already uses this approach on a small scale; we expect that its use will increase, especially as centralized wiretapping capabilities become less viable". Bellovin, Steven M., Matt Blaze, Sandy Clark, and Susan Landau. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet." *Northwestern Journal of Technology and Intellectual Property* 12, n.º 1 (2014): 66. URL

53 ETSI, *Lawful Interception* (LI): *Concepts of Interception in a Generic Network Architecture* (ETSI TR 101 943 V2.2.1, noviembre de 2006), 28 de noviembre de 2006,URL

54 Peña, Cristóbal y Sebastián Minay, "Así se hacen los cuestionados 'pinchazos' telefónicos legales." Investigación. CIPER Chile, 29 de octubre de 2008.URL

55 Por ejemplo: White, Matthew. *Surveillance Law, Data Retention and Human Rights: A Risk to Democracy*. Routledge, 2024. DOI

Box 4: Algunas soluciones de interceptación legal

Producto	Fabricante	Función principal	Referencia
EGO	Innova (Italia)	Interceptación de tráfico IP. Captura/decodificación de comunicaciones; requiere acceso del operador.	*Innova – catálogo*
ULIS (Unified Lawful Interception Suite)	Thales (Francia)	Suite de interceptación legal para operadores, permite la interceptación transparente en tiempo real de comunicaciones de voz, datos y multimedia.	*Ficha técnica*
NarusInsight Intercept Suite	Narus (EE. UU.; adquirida por Boeing en 2010)	Suite de interceptación enfocada a "precision targeting" en tiempo real: captura y reconstrucción de tráfico IP (incluido webmail) y recolección de datos a nivel paquete/flujo/aplicación para análisis forense, vigilancia o cumplimiento regulatorio.	*Nota*
Trovicor LI Solutions	Trovicor (Alemania)	*Lawful interception. Gateways* de interceptación legal integrados con el core de operadoras.	*Company overview*
SS8 Intercept & Mediation	SS8 (EE. UU.)	Mediación e inteligencia de metadatos. Correlación y entrega de datos de comunicaciones y localización.	*Sitio oficial*
Verint *STAR-GATE* (o STAR-GATE Lite)	Verint / Cognyte (Israel/EE. UU.)	Interceptación en infraestructura. Plataformas de LI y análisis.	*Verint STAR-GATE Mediation Device Configuration*
Ericsson LI-IMS	Ericsson (Suecia)	Sistemas regulatorios de interceptación legal. *Gateways* de cumplimiento normativo (LI) integrados en el core de red de operadores.	*Soluciones Ericsson*

1.2.4. Gestión y monitoreo de tráfico

La gestión del tráfico de red abarca herramientas de inspección profunda de paquetes (DPI) y filtrado de contenido. Si bien son empleadas por los proveedores de servicios de Internet (ISP), sus capacidades y usos hacen necesario que sean consideradas como soluciones de vigilancia.

Estas herramientas permiten analizar y clasificar el tráfico de datos mediante el procesamiento de paquetes, protocolos de comunicación, solicitudes de URL y consultas DNS. Su finalidad típica es la optimización del funcionamiento de la red, su seguridad y analítica de uso; además pueden bloquear dominios/IPs, priorizar, degradar aplicaciones, o aplicar distintas políticas de filtrado. Entre las técnicas más habituales se encuentran la inspección profunda de paquetes (DPI), que examina información incluso en capas superiores del protocolo (como cabeceras HTTP cuando el tráfico no está cifrado, o metadatos del "*handshake*" TLS cuando está cifrado); el análisis de consultas DNS, utilizado para identificar los dominios visitados; y el análisis de flujos, que agrupa métricas como volumen, duración y destino del tráfico.

Entre las herramientas comerciales líderes en esta categoría —tanto en América Latina como en otras regiones— se destacan empresas como Sandvine (Canadá/EE. UU.) y Blue Coat ProxySG (E.E. U.U.), así como soluciones de Cisco y Palo Alto Networks, todas integradas en la infraestructura de operadores o grandes redes para facilitar la gestión del tráfico de red.[56]

Debido a su capacidad para observar y controlar comunicaciones a nivel granular, el potencial de censura o vigilancia de estas tecnologías también fue advertido desde hace muchos años.[57] De hecho, Citizen Lab documentó el uso de dispositivos de Blue Coat como ProxySG en Siria, Sudán e Irán, asociados a censura, filtrados y monitoreos abusivos de tráfico web.[58]

Por estas razones, las organizaciones civiles abocadas a estos temas suelen poner la lupa en estas capacidades de los operadores.[59] En el ámbito latinoamericano, existen indicios de contratos regionales que involucran a múltiples empresas de telecomunicaciones. De acuerdo con información publicada por AppLogic Networks, Sandvine habría suscrito un acuerdo por aproximadamente 12 millones de dólares con operadores troncales (Tier 1) de gran escala que cubren once países de la región, orientado a la implementación de capacidades de análisis de tráfico y casos de uso de inteligencia de red, aunque no se identifican

---

56 Privacy International *Monitoring Centres: Force Multipliers From The Surveillance Industry.* 29 de abril de 2014. URL

57 Fuchs, Christian. *Implications of deep packet inspection (DPI) Internet surveillance for society.* Centre for Science, Society & Citizenship, 2012. URL

58 Marquis-Boire, Morgan, Collin Anderson, Jakub Dalek, Sarah McKune y John Scott-Railton. *Some Devices Wander by Mistake: Planet Blue Coat Redux*. Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, 2013. URL

59 Lara, Juan Carlos, y Francisco Vera. *Responsabilidad de los prestadores de servicios de internet* n.º 3. Policy Papers. Derechos Digitales, 2013. URL

los proveedores específicos involucrados.[60] Cabe tener en cuenta que Sandvine enfrentó restricciones regulatorias tras haber sido incluida en la "Entity List" del Departamento de Comercio de EE. UU., en febrero de 2024, acusada de vender tecnologías utilizadas para vigilancia o represión política, aunque fue removida de la lista en octubre de 2024 tras reformas corporativas.[61]

Desde la perspectiva que nos interesa, una división posible para abordar estas herramientas de monitoreo sería por el nivel de profundidad con el que se analiza el tráfico. 1. Herramientas de análisis de flujos o metadatos: no capturan el paquete completo, sino conexiones, tiempos, volúmenes y destinos. Permiten analizar relaciones, patrones y atribuciones, sin acceder al contenido. 2. Tecnologías de captura de paquetes completos: si no hay cifrado, brindan acceso al contenido y, en todos los casos, permiten una reconstrucción de las conexiones. 3. Inspección profunda de paquetes (DPI): más allá de las cabeceras, permite identificar y clasificar tráfico para registrar, bloquear o repriorizar, además de extraer mayores metadatos de aplicación.

Esta categoría se superpone en parte con la anterior. La distinción entre las herramientas de monitoreo de internet (como Blue Coat) y las de interceptación con inteligencia de red (como Innova, SS8 o Utimaco) suele basarse en el nivel de intrusividad, el propósito de uso y el contexto legal en el que operan. Sin embargo, esta división se vuelve cada vez más difusa debido a la convergencia de estas tecnologías.

Sandvine resulta un ejemplo perfecto. Herramientas originalmente diseñadas para el monitoreo y gestión de tráfico, como Sandvine PacketLogic, han incorporado funciones como la inspección profunda de paquetes, el análisis automatizado de metadatos y técnicas para clasificar tráfico incluso cuando está cifrado (sin acceder al contenido, pero con capacidades que reproducen parte de las de los sistemas de inteligencia y sugieren un potencial de uso para vigilancia a nivel de red). En consecuencia, desde una perspectiva técnica, ambos tipos de tecnologías están cada vez más interconectados. En cuanto a sus usos y objetivos, la línea entre el monitoreo corporativo de redes y la vigilancia orientada a la inteligencia también se ha vuelto cada vez más ambigua. Investigaciones técnicas han mostrado, por ejemplo, casos en los que dispositivos PacketLogic fueron utilizados para redirección, inyección y despliegue de *spyware* a nivel ISP, lo que ilustra el potencial de abuso de estas capacidades.[62]

Como conclusión, conviene distinguir cuatro tipos de herramientas:

I. **La interceptación legal (LI)**, que es la interceptación selectiva y autorizada de los llamados "selectores/objetivo" (usuarios, IPs, IMSI, IMEI). Su rasgo distintivo es la entrega estandarizada desde el proveedor hacia la autoridad, transportando datos asociados y, cuando corresponde, también contenido.

---

60 AppLogic Networks. *Sandvine Wins USD 12 Million Network Intelligence Contract Covering 11 Latin American Countries.* AppLogic Networks, 6 de abril de 2019. URL

61 Light Reading. "US Adds Sandvine to Entity List over Surveillance Sales." *Light Reading*, octubre de 2024. URL

62 Gjesvik, Lars, and Johann Ole Willers. "Beyond Control? The Political Economy of Private Interception, Intrusion, and Surveillance Markets." *Review of International Political Economy* 31, n.º 6 (2024): 1840–64. DOI

II. El monitoreo de red (*network monitoring*) operado por el proveedor de servicio que apunta a garantizar disponibilidad, performance, capacidad y detección de fallas.

III. Las herramientas de DPI (*Deep Packet Inspection*), una técnica de inspección más profunda que permite clasificar tráfico y aplicar políticas, incluyendo escenarios de filtrado o bloqueo según el contenido, y por eso suele aparecer como "motor" integrado dentro de soluciones de seguridad, monitoreo o analítica.

IV. La inteligencia de red (*Network Intelligence*), que suma datos provistos de algún modo por el monitoreo de red, pero les agrega correlación, enriquecimiento y analítica para producir patrones, perfiles, tendencias y detección de anomalías.

Cabe destacar que hay estándares técnicos muy claros sobre la interceptación legal y sobre cuáles deben ser los datos retenidos, pero no existe un estándar que obligue o regule que el ISP entregue a fuerzas de seguridad sus datos operacionales de monitoreo / DPI (tal como salen de las herramientas Sandvine, Allot, etc.) de manera sistemática. Lo que sí suele existir es un marco legal o procesal que define cuándo y por qué puede pedirse dicha información.

Box 5: Network Traffic Management: funciones y riesgos

Aspecto	Descripción / Función principal	Ejemplos de herramientas	Usos legítimos	Riesgos y controversias
Inspección profunda de paquetes (DPI)	Analiza el contenido de los paquetes de datos más allá de las cabeceras, incluso en capas de aplicación.	Sandvine PacketLogic, Huawei eSight, Blue Coat ProxySG	Optimización del tráfico, control de congestión, detección de malware o intrusiones.	Invasión de privacidad, censura de contenido, vigilancia masiva, discriminación del tráfico, violación de la neutralidad de red.
Filtrado y bloqueo de tráfico	Identifica y bloquea URLs, IPs o dominios según reglas o listas excluyentes.	Blue Coat, Palo Alto Networks, Cisco Umbrella	Protección *anti phishing*, control parental, cumplimiento de políticas corporativas.	Censura de información política o social, bloqueo arbitrario de contenidos, restricción de libertades digitales.
Análisis de consultas DNS	Examina patrones de resolución de nombres de dominio para inferir qué sitios visitan los usuarixs.	ZTE NetNumen, soluciones ISP integradas	Mejora de rendimiento y seguridad de red, detección de anomalías.	Trazado de hábitos de navegación, elaboración de perfiles de usuarix, vigilancia sin consentimiento.
Análisis de flujos	Evalúa estadísticas agregadas del tráfico: volumen, duración, destinos y puertos.	Cisco NetFlow, Huawei eSight	Gestión de capacidad, diagnóstico de rendimiento, planificación de infraestructura.	Identificación indirecta de usuarixs o grupos, correlación con metadatos de vigilancia, pérdida de anonimato.
Inspección de tráfico cifrado	Intercepta o analiza tráfico HTTPS mediante certificados o análisis de metadatos.	Sandvine, Palo Alto Networks, Blue Coat SSL Visibility Appliance	Monitoreo corporativo de seguridad, detección de amenazas cifradas.	Quebrantamiento de privacidad, exposición de datos personales, abuso gubernamental o corporativo.
Convergencia tecnológica (monitoreo y vigilancia)	Integración de funciones de monitoreo, inteligencia y control en una misma infraestructura.	Sandvine, Huawei eSight, Blue Coat ProxySG	Unificación de sistemas de gestión de red, mejora de eficiencia.	Difuminación de límites legales, uso dual civil–militar, vigilancia masiva bajo apariencia de gestión técnica.

Box 6: Algunas soluciones de monitoreo de red

Herramienta / fabricante	Funcionalidades relevantes	Presencia o uso documentado en América Latina	Nota
Sandvine (Active Network Intelligence, PacketLogic, etc.) (Canadá)	DPI, clasificación de tráfico, análisis de aplicación, políticas, gestión del tráfico, análisis en tiempo real.	Usada por operadores, los principales proveedores de infraestructura (Tier-1) en varios países latinoamericanos.	Ha vendido módulos "use case" en 11 países de LATAM. (*AppLogic Networks*) Su tecnología puede usarse tanto para optimización como para bloqueo o perfilado.
Huawei eSight / Huawei soluciones de red (China)	Gestión de red, monitoreo, análisis, visibilidad del tráfico.	Huawei ofrece soluciones para ISPs latinoamericanos (por ejemplo, "Premium Wi-Fi 2.0" para ISPs en Latinoamérica) (*es.hi-network.com*).	eSight está más orientado a la gestión (aunque puede incluir monitoreo de tráfico) (*Huawei Enterprise*). La presencia de equipos de Huawei en redes de Latinoamérica es amplia, lo que podría facilitar la integración de funciones DPI u otros módulos.
Blue Coat ProxySG / Blue Coat PacketShaper (EE.UU.)	Filtrado de contenido web, inspección SSL/TLS, control de aplicaciones, proxy inverso, categorización.	Entre otros países de la región, distintos productos de Blue Coat son utilizados en Argentina, Chile y Venezuela (*The Citizen Lab*).	Citizen Lab documentó que dispositivos ProxySG y PacketShaper han sido usados para censura y vigilancia. (*The Citizen Lab*).
Allot (Service Gateway / DART; HomeSecure/ NetworkSecure/ WebSafe) (Israel)	DPI, clasificación e identificación de tráfico, analítica por aplicación, aplicación/ usuario/ dispositivo, analítica en tiempo real y enforcement de políticas y gestión de congestión	Operador fijo Tier-1 en LATAM para HomeSecure (2023) y Más Móvil Panamá para NetworkSecure (2025).	Tecnología de doble uso: puede emplearse para optimización/ QoE y ciberseguridad, pero también habilita filtrado/perfilado/ bloqueo (p.ej., listas negras de URL por "cumplimiento regulatorio") dependiendo de las políticas configuradas. *Allot* (Fuera de LATAM, hubo reportes sobreuso de DPI de Allot en contextos de censura). *URL*

Box 7: Monitoreo de red vs. Inteligencia de red

La distinción entre las herramientas de *monitoreo* de internet (como Blue Coat) y las de *interceptación e inteligencia de red* (como EGO, Utimaco, SS8) suele basarse en la capacidad para individualizar tráfico según criterios específicos centrados en individuos o grupo de individuos, en la capacidad de post-procesamiento de lo capturado, el nivel de intrusividad, el propósito de uso y el contexto legal en el que operan. Si bien, entonces, esta distinción es útil, también es cierto que esta división se vuelve cada vez más difusa debido a la convergencia de estas tecnologías.

Tipo de Herramienta:	Monitoreo de red	Inteligencia de red
Objetivo principal	Rendimiento de la red, restricciones legales, estadísticas	Investigación, perfilado, geolocalización, interceptación
Datos típicos	Métricas, *logs*, *NetFlow* (registro de flujo de red: protocolos, puertos, bytes enviados, duración), PCAP (*Packet Capture*, para resolución de errores: cabeceras + datos).	Metadatos enriquecidos, transcripciones, perfiles, correlaciones históricas
Contenido vs. metadatos	Principalmente metadatos; ocasionalmente paquetes para diagnóstico	Ambos; énfasis en la correlación de metadatos y contenido cuando la ley lo permite
Tiempo	Tiempo real	Tiempo real y análisis retrospectivo
Integración con proveedor	Normalmente desplegado por el propio ISP/operador	Exige la ingesta de datos desde operador o módulos de interceptación legal.

1.2.5. OSINT/WEBINT

Las herramientas de inteligencia sobre fuentes abiertas (OSINT, *Open Source Intelligence)* monitorean contenidos en redes sociales y todo tipo de páginas web. Esto incluye imágenes, textos, videos y audios a lo largo del tiempo, y entonces, a su vez, identificación biométrica, de objetos, de lugares, de emociones, de perfiles, de vínculos... Y mucho más. Estas herramientas también pueden integrarse con otros sistemas de WEBINT, orientados a su complementación con otras bases de datos privadas, policiales, sociales, judiciales o de información diversa disponibles tanto en sitios públicos como en la *deep web* o *dark web.*[63]

63 Trottier, Daniel. *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Routledge, 2016. DOI

Además, estas herramientas de inteligencia permiten generar patrones, identificar conductas consideradas sospechosas y vigilar interacciones en redes sociales. En este rubro también pueden sumarse funcionalidades predictivas. Entre las empresas líderes del mercado se encuentran Palantir Technologies (con su plataforma *Foundry*), Geofeedia (ahora parte de Verint) y Social Sentinel (USA). Algunas empresas ofrecen ediciones "gubernamentales" y otras para empresas —"enterprise intelligence"— con capacidades especiales que, en principio, no están a la venta al público general.[64]

El neologismo *ciberpatrullaje*, frecuentemente mal utilizado para describir el uso de herramientas OSINT, asimila una actividad policial de prevención del delito en ámbitos públicos a una actividad de inteligencia, con todos los riesgos que esto implica. Se trata así de un eufemismo sesgado y engañoso, con implicancias sociales y políticas, ya que las redes sociales no son "ámbitos públicos", sino privados y están sujetos a condiciones de uso contractuales específicas. Por ejemplo, compartir imágenes en redes sociales no implica aceptar que éstas puedan ser procesadas por herramientas de identificación biométrica.

En los últimos años, el uso de herramientas comerciales OSINT por parte de agencias de seguridad ha generado repetidos cuestionamientos por monitorear actividades sociales o políticas. Algunos ejemplos.

- En Estados Unidos, la empresa Dataminr, que utiliza análisis en tiempo real de X/Twitter y otras redes abiertas, fue señalada por proveer información a fuerzas policiales durante las protestas de Black Lives Matter en 2020, pese a las restricciones impuestas por las propias plataformas sobre el uso de datos con fines de vigilancia.[65]
- Del mismo modo, la compañía Voyager Labs, especializada en análisis de comportamiento y minería de redes sociales mediante inteligencia artificial, fue demandada por Meta (Facebook) por acceder y recopilar de manera automatizada información de millones de perfiles para ofrecer servicios de monitoreo a agencias gubernamentales.[66]
- También en Estados Unidos, un tercer caso conflictivo involucró al sistema Social Sentinel. En un principio, fue implementado por al menos 39 universidades estadounidenses para monitorear publicaciones en redes sociales con el fin de detectar posibles amenazas o comportamientos de riesgo. Investigaciones periodísticas revelaron que, en varios casos, la herramienta también se utilizó para vigilar protestas y actividades políticas estudiantiles, lo que suscitó críticas sobre su transparencia y su impacto en la libertad de expresión.[67]

---

64 Brennan Center for Justice, "Third-Party Vendors of Social Media Monitoring Tools for Law Enforcement Agencies," 15 de diciembre de 2021. URL

65 Sam Biddle, "*Dataminr Fed Police Real-Time Tweets from BLM Protests.*" *The Intercept*, 9 de julio de 2020. URL

66 Levin, Sam, and Johana Bhuiyan. *"Meta Alleges Surveillance Firm Collected Data on 600,000 Users via Fake Accounts." The Guardian*, 12 de enero de 2023. URL

67 *The Dallas Morning News*. "*How colleges use AI to monitor student protests" Dallas Morning News Interactive*, 2022. URL // The Dallas Morning News. "The Black Box: Social Sentinel's AI Misses the Mark on Threat Detection." *Dallas Morning News Interactive*, 2022. URL

Durante 2022, el Centro de Estudios de la Legislación en América Latina (CELE) coordinó un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay respecto del uso estatal de OSINT para vigilancia dentro de su política de seguridad interna. Este informe menciona que existen casos documentados que muestran que el estado operó con inteligencia basada en fuentes abiertas entre 2017 y 2020, y que probablemente continuó haciéndolo.[68]

Como destacan estos reportes, el uso de este tipo de herramientas resulta conflictivo por motivos aún no considerados en toda su radicalidad. No sólo porque potencialmente violan los términos y condiciones aceptados por sus usuarixs, sino que además la recolección sistemática, almacenamiento y análisis masivo de datos puede vulnerar derechos fundamentales.[69] En tanto permiten la creación de bases de datos que perfilan a ciudadanxs, activistas o periodistas con criterios ideológicos o políticos, pueden generar límites a la libertad de expresión y asociación, riesgos de vigilancia selectiva y autocensura (o *chilling effect*).[70] Por algunos casos relevantes, la Comisión Interamericana de Derechos Humanos ha manifestado preocupación por el uso sistemático y poco transparente de este tipo de monitoreo continuo de espacios digitales y de perfilamiento de personas.[71]

---

68 CELE, *Intelligence based on open sources (OSINT) and human rights in Latin America: a comparative study in Argentina, Brazil, Colombia, Mexico and Uruguay*, CELE, 2023. URL

69 Ucciferri, Leandro. *Seguidores que no vemos: una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence (SOCMINT)*. ADC, 2018. URL

70 Jon Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", *Internet Policy Review*, 2017. URL

71 Díaz Charquero, Patricia, y Jorge Gemetto. *Ciberpatrullaje: Los límites borrosos de la vigilancia policial en Uruguay*. Datysoc, 2022. URL // Schatzky, Agustina Del Campo, Morena y Mmdg. "Cyber Patrol or Intelligence?" CELE, 8 de octubre de 2020. URL

Box 8: Algunas herramientas OSINT/WEBINT de uso global

Herramienta / Fabricante	Uso por fuerzas de seguridad	Notas / fuentes
Babel Street / BabelX (EE. UU.)	Monitoreo multiplataforma de redes sociales, análisis de emociones, búsquedas cruzadas en múltiples idiomas.	"Third-Party Vendors of Social Media Monitoring Tools for Law Enforcement". *URL*
Digital Stakeout (EE. UU.)	Monitoreo de redes sociales y *dark web*, alertas personalizadas, visualización de datos públicos.	Brennan Center. *URL*
Skopenow (EE. UU.)	Extracción automática de datos de redes sociales, alertas de cambios o actividad de perfiles públicos.	Brennan Center. *URL*
Cobwebs / Tangles (Cobwebs Technologies, Israel)	Plataforma de inteligencia web (WEBINT/OSINT) que realiza monitoreo en tiempo real, análisis de interacciones y relaciones sociales.	Brennan Center; sitio oficial Cobwebs. *URL*
Cognyte (Israel)	Plataforma de *situational intelligence* y análisis de redes sociales, sucesora de Verint Intelligence Solutions; provee soluciones a agencias policiales y de defensa.	Información corporativa de Cognyte. *URL*
i2 Analyst's Notebook / i2 Limited (Reino Unido)	Herramienta de análisis visual de inteligencia criminal y vínculos, usada por fuerzas policiales y militares en más de 150 países. Funciona como motor de análisis conectado a otras fuentes OSINT.	IBM Security / i2 Limited. *URL*
Palantir / Palantir Technologies (EE. UU.)	Plataforma de análisis de grandes volúmenes de datos (*Foundry, Gotham*), utilizada por agencias de defensa, policía e inteligencia.	Información pública y reportes. *URL*

Herramienta / Fabricante	Uso por fuerzas de seguridad	Notas / fuentes
PenLink (EE. UU.)	Plataforma de interceptación y análisis de comunicaciones y datos OSINT para investigaciones criminales.	Sitio oficial: *URL*
Social Links (Ucrania / global)	Plataforma OSINT para agencias de aplicación de la ley, integración con Maltego, búsqueda en redes sociales, *dark web* y fuentes abiertas.	Sitio oficial. *URL*
Voyager Labs / Voyager Analytics (Israel)	Plataforma de análisis de redes sociales basada en IA para inteligencia policial, identificación de amenazas y vínculos sociales.	Reporte NYT y sitio corporativo. *URL*
ShadowDragon / SocialNet / OIMonitor (EE. UU.)	Vigilancia digital de redes sociales, detección de patrones, vinculación de alias, alertas automatizadas.	Wikipedia. *URL*
Dataminr (First Alert) (EE. UU.)	Detección temprana de eventos en tiempo real, alertas basadas en publicaciones sociales y señales de crisis.	Criminal Legal News. *URL*
Pagefreezer (Canadá/EE. UU.)	Monitoreo y archivo de contenido digital (web, redes, mensajería) para agencias públicas.	Sitio oficial. *URL*
Kaseware (EE. UU.)	Plataforma de análisis e investigación criminal con módulos OSINT y gestión de casos.	Sitio oficial. *URL*

Box 9: Categorías de inteligencia

Categoría	Definición	Ejemplos de herramientas
SIGINT *(Signals Intelligence)*	Inteligencia derivada de la recolección y análisis de señales electrónicas, comunicativas y no comunicativas (radar, telemetría).	Jammers / inhibidores, *IMSI catcher*s, explotaciones de los protocolos de telefonía SS7 / Diameter etc.
COMINT *(Communications Intelligence)*	Subcategoría de SIGINT enfocada en la interceptación y análisis de comunicaciones.	Sistemas de escuchas telefónicas, interceptores VoIP, monitoreo satelital de comunicaciones.
OSINT *(Open Source Intelligence)*	Obtención y análisis de información de fuentes abiertas: medios de comunicación, publicaciones, redes sociales, bases de datos públicas. A veces se distingue una subcategoría llamada SOCMINT (Social media intelligence), dedicada a las redes sociales.	Maltego, OSINT Framework, Google Dorks, TheHarvester, Palantir *Foundry*.
WEBINT *(Web Intelligence)*	Se centra en la web, incluida la, *deep web* y la *dark web*).Permite recopilar y analizar datos digitales en línea, no sólo de fuentes abiertas.	Social Sentinel, Echosec, Geofeedia (Verint), DarkOwl, SpiderFoot.

Box 10: Tecnologías y empresas

Spyware
NSO Group (Israel)
Paragon Solutions (Israel)
Saito Tech (anteriormente Candiru) (Israel)
Intellexa Consortium
RCS Labs (Italia)
Memento Labs (anteriormente Hacking Team) (Italia)
Quadream (Israel)
MerlinX Ltd (Israel)
Gamma Group (Alemania / Reino Unido)
Interionet (Israel)
Mollitiam (España)
Movia (Italia)
Negg Group (Italia)

SS7-Diameter Explotation
Ability (Israel)
PAT Systems (EE.UU.)
Rayzone (Israel)
Telesoft (Reino Unido)
Tykelab (Italia)
Elaman (Alemania)
Verint (EE.UU.-Israel)
Cognyte (Israel)
Circles (vinculada a NSO Group) (Israel)

IMSI catchers
L3 Harris Technologies (EE.UU.)
Septier (Israel)
BAE Systems (Reino Unido)
Cobham (Reino Unido)
Cognyte (Israel)
Jacobs (EE.UU.)
Verint (EE.UU. - Israel)
Rohde & Schwarz (Alemania)

Interceptación legal (LI)
Innova (Italia)
Narus / NarusInsight (EE.UU.)
Trovicor (Alemania)
Utimaco (Alemania-EE.UU.)
SS8 Networks (EE.UU.)
Procera Networks (EE.UU.)
Group 2000 (Países Bajos)
AQSACOM (Francia)
Squire Technologies (Reino Unido)
Subsentio (EE.UU.)
VOCAL Technologies (EE.UU.)
Thales (Francia)
BAE Systems (Reino Unido)
Septier (Israel)

DPI
AppLogic Networks (anteriormente Sandvine) (Canadá)
Huawei Technologies (China)
Cisco Systems (EE.UU.)
Qosmos (parte de Enea)
NICE Systems (Israel-EE.UU.)
Geedge Networks (China)
Blue Coat Systems (EE.UU.)
VAS Experts (Rusia)
ZTE (China)
A10 Networks (EE.UU.)
Narus (EE.UU.)
Rohde & Schwarzl (Alemania)
Allot (Israel)
Palo Alto Networks (EE.UU.)
Check Point (Israel)
Hewlett Packard Enterprise (EE.UU.)
IBM (EE.UU.)

OSINT
Babel Street / BabelX (EE.UU.)
Digital Stakeout (EE.UU.)
Skopenow (EE.UU.)
Cobwebs Technologies / Tangles (Israel)
Cognyte (Israel)
i2 Analyst's Notebook / i2 Group
Palantir (EE.UU.)
PenLink (EE.UU.)
Social Links (EE.UU.)
Voyager Labs / Voyager Analytics (Reino Unido -Israel)
Clearview AI (EE.UU.)

1.2.6. Herramientas de extracción y análisis forense

Se trata de herramientas de informática forense orientadas a la extracción y análisis de datos de dispositivos móviles y de otros soportes. Muchas de ellas incorporan *exploits* en continuo desarrollo que fuerzan el acceso al dispositivo. Las plataformas especializadas en teléfonos móviles, como UFED (Universal Forensic Extraction Device) de Cellebrite, XRY de MSAB o Magnet AXIOM, permiten realizar extracciones del sistema de archivos; así como recuperar datos borrados y, en ciertos casos, obtener acceso privilegiado a dispositivos bloqueados, copias de seguridad y servicios en la nube vinculados a ellos.

Junto a estas soluciones, existen *suites* forenses de propósito general, como EnCase y Mobile Investigator (OpenText), FTK (Exterro/AccessData) o las estaciones de trabajo FRED (Digital Intelligence), que combinan capacidades de adquisición con funciones avanzadas de análisis posterior de la evidencia digital. Su utilización por fuerzas de seguridad suele estar regulada por la legislación procesal vigente y, en principio, requiere una base legal específica, que puede incluir orden judicial, consentimiento del titular del dispositivo u otros supuestos previstos por la norma.

Aunque hasta ahora no se han detectado abusos en América del Sur, los riesgos que involucran son discutidos. Diversos informes internacionales señalan que estas mismas empresas comercializan sus productos en países donde se violan los derechos humanos.[72] En la práctica, en Estados Unidos estas extracciones suelen realizarse sin la autorización judicial correspondiente.[73] En Brasil, se ha documentado un uso indiscriminado.[74] Y en Serbia existen registros del empleo de estas herramientas para desbloquear dispositivos con el fin de instalar *spyware* y de esta manera lograr persistencia en el monitoreo.[75]

Por esto, las discusiones a su alrededor son numerosas. Las herramientas forenses comerciales no poseen auditorías independientes y no permiten establecer estándares de fiabilidad, transparencia y admisibilidad. Las agencias de seguridad simplemente depositan allí su confianza sin mayores garantías. Además, puede plantearse que el uso de *exploits* sobre vulnerabilidades no parcheadas podría producir cambios incontrolables sobre el dispositivo, comprometiendo la cadena de custodia de información y, en consecuencia, la validez de la prueba digital presentada ante un tribunal.[76] Asimismo, se ha demostrado que las pro-

---

72 Pisanu, Gaspar y Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad,* Deployed at Home. 2021. URL

73 Koepke, Logan, Emma Weil, Urmila Janardan, Tinuola Dada y Harlan Yu. *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones. Upturn,* 2020. URL

74 Ramiro, André, Amaral, Pedro, Canto, Mariana y Pereira, Marcos César. *Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil.* Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2022. URL

75 Amnesty Tech. *A Digital Prison: Surveillance and the Suppression of Civil Society in Serbia.* Amnesty International, 2024. URL

76 P. Dimpe, "Impact of Using Unreliable Digital Forensic Tools," *Proceedings of the World Congress on Engineering and Computer Science* (San Francisco: IAENG, 2017), 118–125. URL

pias herramientas tienen vulnerabilidades de seguridad que podrían ser explotadas con datos alojados en los teléfonos y, en consecuencia, alterar la prueba o el correcto funcionamiento de las herramientas forenses.[77]

Como en el mencionado caso de Serbia, a esto se suma el hecho de que estas herramientas puedan operar sin dejar rastros en el dispositivo habilita su uso espurio con fines ilegales. Y, como está documentado, pueden convertirse fácilmente en instrumentos de represión.

1.2.7. Videovigilancia y biometría

En comparación con otras tecnologías, el rápido avance en la implementación de sistemas de videovigilancia y tecnologías biométricas en la región ha sido objeto de un análisis y debate más amplio, por lo que existe un mayor conocimiento sobre las empresas involucradas.[78] Entre ellas se encuentran Idemia/Morpho, Cross Match, AnyVision, Hikvision, Dahua, Huawei, ZTE, NEC y NTechLab.[79] Sus usos, sin embargo, son más difíciles de rastrear. En tanto estos productos también se comercializan con empresas privadas, las ofertas y registros de importación no siempre reflejan con precisión su uso por parte de organismos estatales y los mismos permisos de instalación son objeto de debates permanentes.

77 Existen casos documentados de vulnerabilidades explotables en UFED y EnCase. URL

78 Díaz Charquero, Patricia, *Fuera de control: Ampliación del informe y resultados del litigio sobre uso policial del reconocimiento facial automatizado en Uruguay.* Montevideo: Datysoc, 2022. URL // Maguire, Méabh, and Ángela Alarcón. *Remote Biometric Surveillance in Latin America Are Companies Respecting Human Rights?,* Access Now, 2023. URL

79 Asociación por los Derechos Civiles (ADC). *Tecnologías de vigilancia en Argentina*. ADC, 2021.

Discusión del alcance del reporte - Convergencia de capacidades

La implementación de dispositivos de extracción forense, biometría y videovigilancia ha sido abordada con mayor profundidad en estudios e informes recientes sobre la región.[80] En consecuencia, este reporte no se ocupa de ellos. O, mejor dicho, los menciona sin sumar nueva información al respecto y sin dedicarles un análisis detallado.

También quedan fuera de esta categorización las herramientas de vigilancia operativa focalizada o táctica (como micrófonos, cámaras u otros dispositivos similares) y sistemas de contramedidas (como bloqueadores de señales o dispositivos para detectar y neutralizar distintos tipos de equipos de vigilancia).

I. En concreto, el objeto de este reporte son los productos de interceptación y monitoreo destinados a fuerzas de seguridad y organismos de inteligencia: software de intrusión o *spyware*;

II. herramientas de interceptación de señales (SIGINT), enfocándonos en *IMSI catchers* y aquellas de explotación de los protocolos de telefonía SS7/Diameter;

III. interceptación legal e inteligencia de comunicaciones IP,

IV. monitoreo de redes y

V. herramientas de inteligencia de fuentes abiertas OSINT.

Es cierto que cada vez más, existen plataformas que integran múltiples capacidades. Y, si bien muchas herramientas de vigilancia pueden ubicarse de manera general dentro de más de una de las categorías propuestas, esta clasificación sigue siendo útil para comprender técnicamente los tipos de soluciones disponibles.

Un ejemplo destacado es Intellexa Nova Suite, cuyas funcionalidades incluirían, aparentemente, *exploits* para infiltración, capacidades de inteligencia de señales (SIGINT), análisis de inteligencia de fuentes abiertas (OSINT) y geolocalización activa (mediante SS7/Diameter).[81] Estas herramientas son, en efecto, combinadas en su uso para lograr la infección de un determinado dispositivo, en un proceso que implica etapas de reconocimiento y compromiso (mediante tecnologías OSINT y WEBINT) previas a la infección. De modo que, por ejemplo, empresas como Cobwebs Technologies o Cognyte suelen proveer las herramientas necesarias para instalar el *spyware* de Cytrox. En paralelo, algunas empresas como Black Cube, Bluehack CI o Belltrox, ofrecen el conjunto completo de soluciones integradas en una sola suite.[82]

Con todo, el mapeo realizado muestra que gran parte de las capacidades de vigilancia actuales no se centran en el acceso directo al contenido de las comunicaciones, sino en el análisis sistemático de metadatos, patrones de tráfico

---

80 Pisanu, Gaspar, y Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad*, Deployed at Home. 2021. URL

81 Amnesty Tech. "Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products." *Amnesty International Security Lab*, 6 de octubre de2023. URL

82 Dvilyanski, Mike, David Agranovich, and Nathaniel Gleicher. *Threat Report on the Surveillance-for-Hire Industry*. Meta, 2021. URL

y comportamientos de red. Técnicas como el DPI, el *fingerprinting* y la detección de anomalías permiten inferir relaciones, rutinas y perfiles de uso incluso cuando los datos están cifrados. Esto desplaza el eje de la vigilancia desde el contenido hacia el "cómo, cuándo y con quién se comunica", ampliando significativamente el alcance poblacional y reduciendo las barreras legales y técnicas para su implementación.

Por esto, aunque el OSINT/WEBINT suele presentarse como una forma de recolección menos intrusiva, el cuadro a continuación evidencia su rol estratégico como capa de amplificación del resto de las técnicas. La automatización del *scraping*, el uso de APIs integradoras y el procesamiento de grandes volúmenes de datos permiten convertir información pública o semipública en insumos para sistemas de perfilado, segmentación y predicción de conductas. Integrado con biometría o inteligencia de red, el OSINT deja de ser un recurso auxiliar y pasa a funcionar como un componente central de arquitecturas de vigilancia escalables y de bajo costo político.

Del mismo modo, el problema transversal no reside en cada tecnología de forma aislada, sino en su potencial de integración. El siguiente cuadro muestra cómo OSINT, interceptación de red, *spyware*, análisis forense y biometría pueden combinarse en sistemas coherentes que permiten vigilancia persistente, dirigida o masiva. Su convergencia transforma herramientas específicas en infraestructuras amplias, donde los límites entre vigilancia puntual e inteligencia poblacional se diluyen. El riesgo, por tanto, resulta sistémico: la consolidación de dispositivos abiertos con capacidad de expansión continua y escasa rendición de cuentas.

Tabla 1: Herramientas de vigilancia digital: categorías

Categoría	Spyware	SIGINT	Network intelligence interception	Monitoreo de red
Tipo de acceso	Intrusión remota en dispositivos.	Interceptación de señales físicas de radiofrecuencia.	Análisis de paquetes de datos digitales en redes IP (TCP/IP, HTTP, VoIP, etc.).	Captura del tráfico de red.
Ubicación de ataque	Dispositivo (móvil/ PC).	Señales, infraestructura de la red de telefonía (core, antenas, pasarelas SS7, etc.).	Núcleo de red, *backbone*, ISP.	Núcleo de red, *backbone*, ISP.
Técnicas	Explotación de vulnerabilidades (0-day, 1-day, N-day), *phishing*, instalación física (caso *stalkeware*), gestión remota (C2).	Captura y análisis de radiofrecuencias, manipulación de protocolos GSM/SS7/LTE/Diameter, triangulación de señales.	Análisis de metadatos, copia de tráfico IP, *fingerprinting sniffing*, Deep Packet Inspection (DPI), mirror ports, SSL/TLS interception, protocol reconstruction, inyección de paquetes, etc.	Deep Packet Inspection (DPI), análisis de patrones, detección de anomalías, *fingerprinting*, interceptación SSL/ TLS.
Interacción con el objetivo	Oculta y dirigida	Oculta, dirigida (en el caso de explotación del protocolo SS7), parcialmente dirigida (en el caso de los IMSI catcher).	Oculta y dirigida.	Pasiva y no dirigida (sin especificar usuarixs).
Infraestructura requerida	Servidores, vulnerabilidades, *exploits*, técnicas de instalación, nodos de anonimización de los operadores.	Antenas falsas, acceso a infraestructura móvil, equipos especializados en análisis de frecuencias.	Acceso a ISP, routers, servidores monitoreo.	Equipos de red especializados, servidores de monitoreo.
Objetivo	Control del dispositivo, espionaje dirigido, control remoto, acceso a cámara y micrófono.	Identificar y rastrear dispositivos, escuchar llamadas, ubicar usuarixs.	Interceptar tráfico, analizar patrones, leer o reconstruir comunicaciones.	Observar patrones de uso, detectar “anomalías”, filtrar tráfico.
Tipo de datos recolectados	Archivos, mensajes, localización, cámara, micrófono.	Llamadas, SMS, ubicación por antenas, metadatos.	Tráfico IP, protocolos, dominios, patrones.	IPs, protocolos, dominios, patrones, tráfico.
Empresas con implementaciones en América del Sur	Pegasus (NSO Group), Galileo (Hacking Team), *Invisible Man* / *Night Crawler* (Mollitiam), FinFisher.	IMSI catchers, SS7 signaling attacks, EGO (Innova), Hydra (Cy4gate), ULIS (Verint), NiceTrack, Palantir’s covert tools, SkyLock / Engage GI2 (Verint)	Innova S.p.A. (Italia), Pat Systems (EE.UU), Cy4gate (Italia), Rohde & Schwarz (Alemania),	Blue Coat, Sandvine, Huawei eSight, Network Critical Limited.
Argentina	Alguna probabilidad de *Night Crawler* / *Invisible Man* (Mollitiam), Epeius (Cy4gate), RCS (Hacking Team), Pegasus (NSO Group).	Al menos: PICSIX (Israel), TITAN (EE.UU.), Kavit (Israel), Pat Systems (EE.UU.), Phoenix Cy4gate (Italia), Rohde & Schwarz (Alemania)	Pat Systems (US), Cy4gate (Italia), Rohde & Schwarz (Alemania), Ericsson (Suecia), Nokia (Finlandia), Innova S.p.A. (Italia).	Blue Coat (US), Sandvine, (Canadá), Ericsson (Suecia), Nokia (Finlandia), Innova S.p.A. (Italia).
Chile	Pegasus (NSO, Israel), Phantom / Remote control System - Galileo (Hacking Team, Italia).	Almenta Group (EE.UU.) NSO / CIrcles (Israel) ELT group / Cy4gate (Italia) RCS Lab (Italia) Pat Systems (US) Rohde & Schwarz (Alemania)	Innova S.p.A. (Italia) Cognyte (Israel) Pat Systems (EE.UU.) ELT group / Cy4gate (Italia)	Blue Coat (EE.UU.), Sandvine (Canadá), CISCO (EE.UU.), Palo Alto Networks (EE.UU).
Uruguay	Poca probabilidad de Galileo de Hacking Team (Italia) o Pegasus de NSO (Israel).	Innova S.p.A. (Italia).	Teleimpresores SA (Uruguay), Digitro Tecnologia Ltda (Brasil) Innova S.p.A. (Italia), Nokia (Finlandia).	Nokia (Finlandia), Huawei (China)

Categoría	OSINT / WEBINT	Extracción forense	Videovigilancia y biometría
Tipo de acceso	Contenido digital y procesamiento automatizado de datos.	Acceso físico al dispositivo.	Captura de imagen y datos biométricos en entornos físicos.
Ubicación de ataque	Plataformas web, redes sociales, bases de datos públicas o semiprivadas.	Dispositivo físico, plataformas virtuales asociadas al dispositivo.	Espacios públicos, fronteras, edificios.
Técnicas	*Scraping*, APIs públicas, *crawlers* automatizados, Natural Language Processing (NLP), minería de textos y análisis de redes sociales, biometría sobre fotografías, identificación de objetos y lugares.	Acceso físico, clonado de memoria, cracking de claves, análisis de RAM, *exploits* JTAG para hardware y software	Reconocimiento facial, térmico o corporal, matching automático con bases.
Interacción con el objetivo	Indirecta y automatizada; dirigida o masiva.	Directa, física	Invisibilizada, automatizada.
Infraestructura requerida	*Crawlers*, plataformas cloud, scrapers, APIs, servidores para análisis y capacidad de almacenamiento y procesamiento.	Estaciones de trabajo físicas, software privativo (UFED, Magnet AXIOM), acceso físico controlado, expertos. hardware y software de análisis forense.	Cámaras, sensores biométricos, bases de datos faciales y biométricas.
Objetivo	Obtener información pública para perfilar individuos, grupos y conductas.	Extraer datos de dispositivos incautados.	Vigilar y rastrear físicamente a personas mediante sus rasgos biométricos.
Tipo de datos recolectados	Opiniones, perfiles, publicaciones, scores de riesgo, predicciones, segmentos sociales, afiliaciones.	Archivos, mensajes de aplicaciones, contraseñas, historial de llamadas, datos en la nube.	Rostros, huellas, placas, trayectorias, biometría.
Empresas con implementaciones en América del Sur	D-SINT (Cy4gate), i2 Limited (IBM), Huawei, Babel X, Voyager Labs, Maltego, Palantir Gotham	UFED (Cellebrite), GrayKey, Oxygen, entre otros.	Clearview AI, Hikvision, Dahua, Visionlabs, AnyVision.
Argentina	Al menos Cy4gate (Italia), I2 Technologies / IBM (EE.UU.), Minerva IA (España) Rafael - Verint / Cognyte (Israel), IPS Intelligence Spa (Italia).	Cellebrite (Israel), Digital Intelligence (EE. UU.), EnCase Forensic (US), MOBILedit Forensic (República Checa), MSAB (Suecia), Oxygen Forensics (EE.UU), Silicon Forensics (EE.UU).	3M Electronics Monitoring Inc. (EE.UU.),AnyVision / Oosto (Israel) BGH Tech Partner (Argentina), Clearview AI (EE.UU.), Haivision (Canadá), Hikvision and Dahua (China), Huawei and ZTE (China), IDEMIA (Francia), Incode (EE.UU), Jumio (EE. UU), NEC (Japón), NtechLab (Rusia), Veridas (España), Speech Technology Center (STC Group) / Speech Pro (Rusia).
Chile	Al menos: Cognyte (Israel), ELT group / Cy4gate (Italia) Cellebrite.	Cellebrite (Israel) Toka Group (México) Oxygen (EE.UU).	Clearview AI (EE.UU.) Verint / Cognyte / Intellicene (Israel) NEC (Japón), Dahua Technology (China) Luxriot / VisionLabs (Rusia), AnyVision / Oosto (Israel), Hikvision (China), Dahua (China), Huawei (China), ZTE (China), Veridas (España), Jumio (US), IDEMIA / Morpho (Francia).
Uruguay	Innova S.p.A. (Italia) Digitro Tecnologia Ltda (Brasil), Analytic Technologies (US), Social Links (E.E. U.U.).	Cellebrite (Israel) Magnet AXIOM (Canadá) Belkasoft Evidence Center X (E.E. U.U.).	Hikvision (China), Dahua (China) Huawei (China), ZTE (China), IDEMIA(Francia), NEC (Japón), Clearview AI (EE. UU.), M Electronics Monitoring Inc. (EE. UU.) .

1.3. Contexto regional: México, Brasil y Colombia en foco

Los países del Cono Sur no suelen aparecer entre los de mayor control de la información. Distintos informes anuales no los incluyen entre aquellos con cortes de internet, censura sistemática de contenido o aplicaciones vedadas.[83] Aun así el panorama no deja de ser complejo.

En un marco global en el que Estados Unidos protege a sus propios ciudadanos con leyes específicas y Europa ha logrado imponer su Reglamento General de Protección de Datos (GDPR), lxs ciudadanxs de América del Sur carecen de mayores amparos legales frente a grandes, medianas y pequeñas compañías que acumulan y comercializan datos.

Muchas veces, en estos países tampoco resulta obligatorio cumplir con estándares internacionales que rigen el funcionamiento de las comunicaciones y las normas técnicas de la interceptación legal, como las elaboradas por el European Telecommunications Standards Institute (ETSI) o el American National Standards Institute (ANSI) de Estados Unidos. Si bien por su país de origen los productos de vigilancia comercializados suelen declarar su cumplimiento con este tipo de estándares, estos carecen de validez cuando son adquiridos por fuera de los espacios geográficos específicos.

Una característica general observada en toda la región es el hecho de que la adquisición de tecnologías de vigilancia se realiza en ausencia de legislación específica. Por eso, resulta necesario remitirse a tratados internacionales o a marcos jurídicos más amplios para siquiera especular sobre sus límites legales. Muchos reportes recientes procuran, por esto, determinar cuáles son las normativas que aplicarían según el país en cuestión.[84] A esto se suma que existen disposiciones especiales que habilitan la compra de tecnología de inteligencia con fondos reservados o bajo acuerdos de importación que quedan por fuera de las licitaciones públicas y los registros de importación. E incluso hay testimonios de compras realizadas en efectivo para evitar rastros de la operación.[85]

En general, las agencias de seguridad tienen acceso a un mercado descontrolado del que hacen uso. Los abusos quedan sin documentar y esto genera que las discusiones políticas, sociales y legales que los involucran no alcancen la relevancia necesaria.

El panorama regional muestra en efecto su complejidad. Más allá del Cono Sur, existe una tendencia preocupante hacia la expansión de las tecnologías de vigilancia y la adopción de medidas de seguridad cada vez más represivas. Los ejemplos más notorios en la región son México, Colombia y Brasil.

---

83 Ver por ejemplo los índices de Freedom House para Argentina, Uruguay y Chile en 2024 y 2025. Freedom Huse, "Country Profile.", 2025. URL // Internet Society, "Internet Society - Pulse". URL // Access Now. "Access Now." URL

84 García Muñoz, Luis Fernando, Ana Gaitán Uribe, José Flores Sosa, Santiago Narváez Herrasti y Milán Trnka Osorio. *El Estado de la vigilancia Red de Defensa de los Derechos Digitales* (R3D), 2025. URL

85 Garay, Vladimir, y Zack Rogoff. *Tecnología y vigilancia en la operación Huracán: Una revisión del trabajo periodístico realizado en torno al caso* (2018). Derechos Digitales, 2018. URL

A través de registros de contrataciones públicas en distintos gobiernos municipales de México, ha sido posible rastrear las asombrosas sumas de fondos públicos que diversos estados mexicanos han destinado a la adquisición de estas tecnologías. Los informes continúan acumulándose.[86] Además de *spyware* de alto perfil como Pegasus, se han confirmado compras de FinFisher (Reino Unido - Alemania), Hacking Team (Italia) y Quadream (Israel). Se registran además compras de equipos de interceptación y geolocalización que explotan el protocolo SS7 / Diameter provenientes de empresas israelíes como Ability, Rayzone y Circles; así como de sistemas de monitoreo de tráfico web, como Citadel (Rusia) y EGO de Innova (Italia). También se registran adquisiciones de *IMSI catchers* de compañías como Elaman (Alemania), L3Harris (Estados Unidos) y Kavit (Israel). En relación a los sistemas OSINT, un informe reciente documenta monitoreo de redes con un "Sistema Multifuente" preventivo.[87]

El caso de Colombia resulta igualmente llamativo.[88] El país se ha convertido en uno de los principales compradores de software intrusivo, incluyendo productos de Cytrox/Intellexa, Hacking Team (Italia), NSO Group (Israel) y Mollitiam (España)[89]. Además, adquirió herramientas de interceptación y geolocalización de Ability Inc.; bloqueadores de señal de Allen Vanguard; *IMSI catchers* de Comstrac (Reino Unido), Phantom Technologies (Israel) y L3Harris Technologies (Estados Unidos). También se adquirieron sistemas de monitoreo de Network Critical Limited (Reino Unido), PKI Electronic Intelligence (Alemania), Rohde & Schwarz (Alemania), NICE Systems (Israel/EE.UU.), así como herramientas de inteligencia web y de fuentes abiertas de la empresa estadounidense Palantir.[90] Asimismo, Colombia —junto con Ecuador y Paraguay— figura entre los países que adquirieron paquetes avanzados de vigilancia de Septier Communication, Verint y Vas Tech, que incluyen *IMSI catchers* y perfilamiento OSINT.[91] De hecho, a través de una licitación, la Policía Nacional (DIPOL) abrió un proceso para adquirir un sistema de ciberinteligencia con IA para monitorizar redes sociales y mensajería.[92]

En Brasil también se ha documentado el uso de una amplia gama de *spyware*. En distintos momentos, se han desplegado herramientas desarrolladas por Hacking Team, NSO Group, Candiru, Cytrox, FinFisher y Cognyte; en conjunción

---

86 Rodríguez, Aitana, Mariana Recamier, Dalia Souza y Darwin Franco. "Vigilad@s: Jalisco invierte millones en tecnologías para espiar y monitorear." *Zona Docs*, 2024. URL

87 Article 19. *Informe sobre prácticas OSINT en México*. 2023. URL

88 Fundación Karisma y TEDIC. *Uso de herramientas digitales y amenazas de seguridad digital en personas defensoras de derechos humanos en Paraguay y Colombia.* Karisma- TEDIC, 2024. URL

89 Suárez, Astrid. "EEUU admite que financió la compra del software espía Pegasus en Colombia." World News. *AP News*, 8 de noviembre de 2024. URL

90 Privacy International. *The Global Surveillance Industry*. 2016. URL

91 Fundación Karisma y TEDIC. *Uso de herramientas digitales y amenazas de seguridad digital en personas defensoras de derechos humanos en Paraguay y Colombia*. Karisma- TEDIC, 2024. URL

92 Fajardo, Carolina; Pardo, Daniel. "Colombia: Police Plans to Procure Cyber Intelligence System to Monitor Social Media and Instant Messaging Platforms." *Global Compliance News*, 19 de septiembre de 2020. URL

con formas de *spyware* menos sofisticadas como Packrat y FoxSpy.[93] Asimismo, se registró la presencia de *IMSI catchers* de Kavit (Israel), sistemas rusos de monitoreo de Citadel y, al igual que en el caso de Colombia, un conjunto diverso de herramientas de interceptación suministradas por Comstrac (Reino Unido).[94]

En este contexto, cabe preguntarse cuántas de estas herramientas han sido documentadas en los países del Cono Sur.

93 InterSecLabm, *Unveiling Celular 007: An In-Depth Analysis of Brazilian Stalkerware and Strategies for Collective Protection*. 2025. URL

94 Ramiro, André, Amaral, Pedro, Canto, Mariana y Pereira, Marcos César. *Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil.* Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2022. URL

2. Argentina

2.1. Contexto

En 2011, Argentina lanzó una ambiciosa base de datos biométrica conocida como SIBIOS (Sistema Federal de Identificación Biométrica para la Seguridad). Ese mismo año, la Jefatura de Gabinete firmó un acuerdo marco con la empresa estadounidense Cross Match Technologies, especializada en sistemas biométricos para agencias de seguridad.[95] Entre otras cosas, a través de ese convenio, el Estado pudo adquirir lectores de huellas dactilares —los escáneres utilizados para registrar y verificar identidades— destinados a organismos de seguridad, control fronterizo y gestión de documentación personal.

Seis años más tarde, WikiLeaks reveló que la *Office of Technical Services* (OTS), una dependencia de la CIA, operaba un sistema global de recolección biométrica provisto a servicios de enlace en todo el mundo, con la expectativa de que compartieran voluntariamente los datos capturados. Los componentes centrales de ese sistema estaban basados en productos de la empresa Cross Match. Cuando el intercambio "voluntario" se consideraba insuficiente, la CIA utilizaba una herramienta encubierta denominada *ExpressLane*, que se instalaba bajo la cobertura de una actualización de software y permitía extraer subrepticiamente las bases de datos biométricas de esos sistemas.[96] La existencia de un acuerdo marco entre Cross Match y el Estado argentino habilitaba compras directas de equipamiento biométrico a través de un catálogo preaprobado, reduciendo tiempos y trámites respecto de las licitaciones ordinarias.[97] Pese a la controversia que generó la empresa en países como India, no hay registro de que el acuerdo argentino haya sido revisado o sometido a una investigación pública específica a la luz de estos hechos.[98]

Desde entonces, Argentina fue pionera en identificación biométrica. Diversas acciones legales impulsadas por organizaciones de la sociedad civil —como Fundación Vía Libre, la Asociación por los Derechos Civiles (ADC), el CELS (que forma parte del Centro de Estudios en Libertad de Expresión y Acceso a la Información, CELE) y el Observatorio de Derecho Informático Argentino (ODIA)— han logrado suspender algunos de estos sistemas en Buenos Aires. Gracias a sus investigaciones, además, fue posible identificar a muchas de las empresas involucradas en los contratos gubernamentales. Desde gigantes tecnológicos globales hasta firmas especializadas en vigilancia, la combinación de estas empresas revela una red de

---

95 "Acuerdo Macro de Cooperación y colaboración entre la jefatura de gabinete y Crossmatch Technologies Inc.", 2011. URL

96 Rachel Chitra, "WikiLeaks Hints at CIA Access to Aadhaar Data, Officials Deny It", *The Times of India*, 26 de agosto de 2017. URL

97 A ello se suma que, al año siguiente, Cross Match fue adquirida por el fondo Francisco Partners, que no sólo absorbió sus operaciones, sino que en 2014 sumó también a NSO Group y a Blue Coat —esta última, una de las compañías responsables de sistemas de inspección profunda de paquetes (DPI) empleados tanto en Argentina como en muchos otros países.

98 Kasli, Shelley. "How CIA Spies Access India's Biometric Aadhaar Database," *Voltaire Network*, 25 de agosto de 2017. URL

proveedores donde las exigencias de transparencia permanecen en disputa y sus implementaciones quedan en el limbo entre lo público y lo privado.[99]

En 2014, un pedido de información parlamentaria reveló que Alemania había vendido tecnologías de vigilancia a varios países de la región, entre los que estaba Argentina.[100] Los documentos oficiales no detallaron los proveedores ni el tipo de licencias aprobadas para "sistemas de interceptación" y "centros de observación de vigilancia".[101] La información no pasó de allí. No se determinó cuáles fueron las tecnologías ni las empresas alemanas involucradas.

Es cierto que, en 2014, Paraguay había adquirido recientemente el *spyware* de origen alemán FinFisher; Argentina buscaba legalizar el uso de este tipo de tecnologías de intrusión y negociaba también con NSO Group de Israel y Hacking Team de Italia.

En general, no existen indicios que permitan especular sobre *spyware* ni es posible determinar con certeza qué fue lo que se adquirió de Alemania. En cambio, sí resulta posible esbozar algunas hipótesis basadas en la disponibilidad y las compras efectuadas en otros países. Al menos hay tres candidatas. ATIS y Utimaco producen plataformas de *Lawful Interception Management System*, con antecedentes de ventas a Colombia, México, Ecuador y Paraguay. Otra posibilidad es que se trate de la empresa alemana Rohde & Schwarz, que tiene una filial en Buenos Aires y, en el rubro de seguridad gubernamental, promueve una gran variedad de productos. R&S es históricamente uno de los proveedores globales de plataformas de *lawful interception* y dispositivos de interceptación de telefonía móvil, y además ofrece herramientas abocadas a la interceptación de señales, desde *IMSI catchers* y *Direction Finders* (DF) hasta otros productos de escaneo de frecuencias y monitoreo avanzado de redes con inspección de paquetes.[102]

En cualquier caso, desde el 2014, la habilitación legal del uso de software de intrusión se ha consolidado en Argentina a través de la figura de la "vigilancia remota sobre equipos informáticos", primero en el plano federal y luego en códigos provinciales que copian esa fórmula. El Código Procesal Penal Federal, aprobado por la Ley 27.063 en 2014 y publicado en 2019, incluye dentro del capítulo "Medidas de vigilancia sobre las comunicaciones y equipos informáticos" una categoría específica definida como: *la utilización no ostensible de un software que permita o facilite el acceso remoto al contenido de ordenadores y*

---

99 Entre ellas se encuentran 3M Electronic Monitoring (EE.UU./Israel), AnyVision/Oosto (Israel), BGH (con operaciones en varios países de América Latina), Clearview AI (EE. UU.), Haivision (EE. UU.), Hikvision y Dahua (China), Huawei y ZTE (China), Incode (EE. UU.), Jumio (EE. UU.), NEC (Japón), NtechLab (Rusia/Chipre), Veridas (España) e IDEMIA/Morpho (Países Bajos/Francia). Kiguel, Alejo. *Tecnologías de vigilancia en Argentina*. ADC, 2021. URL // Pisanu, Gaspar y Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*. 2021. URL

100 TEDIC. "La adquisición y el abuso de tecnologías de vigilancia en América Latina - Al Sur." *TEDIC*, 28 de marzo de 2019. URL

101 *Jahrbuch Netzpolitik 2014: Von der Überwachungsgesamtrechnung bis zur Netzneutralität* (Berlin: Netzpolitik.org, 2014). URL

102 Hoy en día, Rohde & Schwarz ipoque desarrolla tecnologías de análisis de tráfico que permiten identificar y clasificar comunicaciones en redes —incluso cuando están cifradas— mediante técnicas de aprendizaje automático. Sus motores, como R&S®PACE 2 y R&S®vPACE, brindan visibilidad en tiempo real sobre aplicaciones y usuarixs, lo que facilita la gestión de redes. "Ipoque | Encrypted Traffic Intelligence for Network Traffic Analysis.", 2025 . URL, URL , URL

dispositivos electrónicos; con autorización judicial y bajo el régimen de técnicas especiales de investigación, lo que abre la puerta al uso de malware estatal en investigaciones penales.[103]

Al menos existen dos casos en los que las provincias buscaron replicar estas capacidades, cabe suponer, para poder adquirir este tipo de software de manera directa y poder utilizarlo en procesos judiciales. En la Ciudad Autónoma de Buenos Aires, un proyecto de reforma al Código Procesal Penal presentado en 2018 incorporó un nuevo artículo que reiteraba esta redacción casi literalmente. A través de una carta pública y posicionamientos técnicos, Fundación Vía Libre, junto con otras organizaciones de la sociedad civil, lograron frenar en la Ciudad de Buenos Aires la incorporación explícita de facultades de "vigilancia remota sobre equipos informáticos". La presión conjunta llevó a que la Legislatura eliminara ese artículo del texto aprobado.[104] Por su parte, el Código Procesal Penal de Corrientes (Ley 6518) de 2019 constituye otro ejemplo claro y habilita a los jueces a autorizar el acceso remoto al contenido de ordenadores, dispositivos electrónicos y sistemas informáticos a través de un software.[105]

Si bien existe entonces una tendencia clara, según el análisis del Centro de Estudios Legales y Sociales (CELS), un punto de inflexión se produjo con el cambio de gobierno de diciembre de 2015. Por un lado, el Decreto 683/2018 modificó la reglamentación de la Ley de Defensa Nacional y amplió el papel de las Fuerzas Armadas. A este le siguió un nuevo decreto que formalizó una nueva configuración en todo lo que se refiere a la agencia de inteligencia. Y ante solicitudes de acceso a la información presentadas por el CELS, tanto el Poder Ejecutivo como la Agencia Federal de Inteligencia (AFI) respondieron que todo lo vinculado al sistema de inteligencia nacional había sido reclasificado como secreto por motivos de seguridad.[106] También la Policía Federal Argentina adquirió nuevas capacidades: la ministra de Seguridad Patricia Bullrich oficializó que esta fuerza iba a comenzar a utilizar nuevas herramientas de "*ciberpatrullaje*" como nueva función preventiva en entornos digitales.[107]

En este marco fue que, en noviembre de 2018, el Ministerio de Defensa firmó un acuerdo por 5,2 millones de dólares con Israel para la provisión de servicios de defensa y ciberseguridad, en vísperas de la cumbre del G20 celebrada en

---

103 Congreso de la Nación, *Ley 27.063. Código Procesal Penal Federal* (Boletín Oficial de la República Argentina, 10 de diciembre de 2014).

104 Access Now, Amnistía Internacional Argentina, Asociación Civil por la Igualdad y la Justicia (ACIJ), Asociación por los Derechos Civiles (ADC), Asociación Pensamiento Penal Capítulo Buenos Aires (APP), Centro de Estudios Legales y Sociales (CELS), Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Colectivo para la Diversidad (COPADI), Fundación Vía Libre, Instituto de Estudios Comparados en Ciencias Penales y Sociales (INECIP), Poder Ciudadano, "La Legislatura porteña debate una reforma penal que habilita la vigilancia y vulnera la intimidad personal," comunicado conjunto de organizaciones, 28 de septiembre de 2018. URL

105 Provincia de Corrientes, *Código Procesal Penal de la Provincia de Corrientes* (Ley 6518/2019), art. 217, "Vigilancia remota sobre equipos informáticos," texto disponible en el Sistema Argentino de Información Jurídica (SAIJ).

106 Litvachky, Paula, Margarita Trovato, Tomás Griffa, et al. "El secreto. La seguridad nacional como coartada para un Estado sin controles." En *Derechos humanos en la Argentina: Informe 2019,* CELS. 2019. URL

107 "Se relanzó la Policía Federal con su nueva función de 'ciberpatrullaje", *Clarín*, 18 de abril de 2017. URL

Buenos Aires. El contrato incluyó la adquisición de equipamiento de Rafael Advanced Defense Systems Ltd., una empresa de tecnología militar que también produce soluciones para el sector privado y que con frecuencia actúa como intermediaria de otras firmas israelíes proveedoras de capacidades SIGINT, COMINT y OSINT, como Verint o Elbit.[108]

Las hipótesis más sólidas sobre qué fue lo que concretamente se adquirió apuntan a: **(i)** una plataforma SOC (Security Operations Center) y CSIRT/CERT (Computer Security Incident Response Team); es decir, centros donde se monitorean redes críticas, se detectan ataques y se responden incidentes en tiempo real. Rafael ofrece este paquete como una plataforma orientada a ministerios de defensa, fuerzas armadas y agencias nacionales de ciberseguridad.[109]Se trata de capacidades estándar de seguridad informática no confirmadas oficialmente y que en principio no tienen relación directa con el tema de este informe. **(ii)** Herramientas de analítica y fusión de fuentes abiertas (OSINT) integradas al mencionado SOC. La prensa que investigó habló de "software de ciberdefensa y ciberseguridad con capacidad de recolectar y analizar redes sociales y acceder a bases públicas/privadas", lo que encaja tanto con módulos de Rafael como con paquetes típicos de Verint/Cognyte.[110]**(iii)** En paralelo al G20, aunque bajo partidas y organismos distintos, la protección física anti-drones (C-UAS) con Drone Dome de Rafael se reportó desplegada en Buenos Aires durante el G20 y los Juegos Olímpicos de la Juventud 2018.[111]

A fines de 2023, el nuevo gobierno de Javier Milei ubicó de nuevo como ministra de Seguridad a Patricia Bullrich, quien había ocupado este cargo también entre diciembre de 2015 y diciembre de 2019. Recién asumido, el ejecutivo impuso por decreto —y no por ley— un nuevo protocolo de seguridad. Junto a este decreto, existió la amenaza de identificar personas mediante la tarjeta de viajes SUBE —el sistema obligatorio de transporte público— para retirar subsidios estatales a quienes fueran identificados participando de manifestaciones sociales.[112] Además, la

---

108 Con la Decisión Administrativa 1658/2018 (04/10/2018), Argentina aprobó un gasto de US$ 5,245,000 para un proyecto "CORE iSOC & CSIRT/CERT de Ciberdefensa" firmado G2G con Israel. La compra se adjudicó a Rafael, con instalación y puesta en marcha del CSIRT/ISOC a mediados de noviembre de 2018 (días antes del G20) en el Edificio Cóndor y otros sitios (incluyó adecuaciones, fibra óptica, data center y despliegue de hardware/software). "InfoLEG - Ministerio de Justicia y Derechos Humanos - Argentina." URL

109 Rafael Advanced Defense Systems, *RAFAEL Cyber Defense Center (RCDC)*, 2021, URL // Rafael Advanced Defense Systems, "National SOC – Security Operation Center,". URL

110 "El Gobierno le pagará US$ 5 millones a Israel por un programa de ciberseguridad," *Convergencia*, 5 de octubre de 2018. URL // Sergio G. Eissa y Ana Albarracín Keticoglu, "La ciberdefensa en su laberinto. Cambio de rumbo en la concepción de ciberdefensa durante la gestión de Mauricio Macri (2015–2019)," *Revista Defensa Nacional* nº. 5 (Universidad de la Defensa Nacional, 2020), 26–28. (detalle de oferentes Rafael, Verint, IAI/ELTA y Elbit; adjudicación a Rafael; cronograma de instalación).

111 Rafael Advanced Defense Systems Ltd., *Drone Dome Counter-Unmanned Aerial System (C-UAS) Solution – Technical Data Sheet* (Haifa: Rafael Advanced Defense Systems, 2018), URL

112 "El Gobierno argentino quitará ayudas sociales a quienes asistan a protestas." *SWI swissinfo.ch*, 18 de diciembre de 2023. URL // Débora Rey, "Argentina: gobierno de Milei advierte con retirar ayudas sociales a los que salgan a manifestarse." *Los Angeles Times en Español*, 18 de diciembre de 2023. URL // Centenera, Mar. "Milei amenaza con quitar las ayudas sociales a quienes corten la calle para protestar., *El País*, 19 de diciembre de 2023. URL

ministra impulsó otras regulaciones y anunció que también se iba a emplear la información de la aplicación oficial "Mi Argentina" para monitorear la participación en huelgas y protestas. Más allá de esta amenaza, existe evidencia concreta del uso de registro de viajes de la tarjeta SUBE para vigilancia de personas, por fuera de los procesos judiciales que podrían ser esperables. Hasta el momento, no está claro qué tecnologías o capacidades de procesamiento de datos permitirían estas capacidades, ni si tales medidas son técnica o legalmente viables.[113]

Seis meses después, la Secretaría de Inteligencia del Estado (SIDE) fue colocada bajo la autoridad directa del Poder Ejecutivo y recibió una asignación récord de fondos reservados. También por decreto presidencial, se creó la Agencia Federal de Ciberseguridad (AFC), dentro de la órbita de la SIDE.[114] Asignar la ciberseguridad al ámbito de la inteligencia estatal constituye una declaración política inequívoca, con profundas implicaciones institucionales. En el nivel más básico, esta decisión otorga un manto de secreto sobre las capacidades, adquisiciones y prácticas regulatorias de un organismo que podría tener distinto tipo de funciones. Al mismo tiempo, limita la supervisión pública y la participación civil, trasladando el diseño y la implementación de la política de ciberseguridad a la estructura opaca de los servicios de inteligencia, un modelo que, hasta ahora, no tiene precedentes en la región.

Este proceso se inscribe en una reconfiguración más amplia de la política de seguridad e inteligencia iniciada en diciembre de 2023, marcada por un alineamiento geopolítico explícito con los gobiernos de Estados Unidos e Israel en los foros globales, y por incrementos significativos en las partidas reservadas destinadas a la modernización tecnológica de los servicios de inteligencia mediante compras directas. Esta orientación se refleja también en una intensa agenda de viajes internacionales del presidente y de la ministra de Seguridad en los que han señalado como objetivo la negociación de acuerdos de cooperación y la adquisición de capacidades de inteligencia digital más sofisticadas. En este mapa de vínculos debe destacarse a las empresas intermediarias OCP Tech y Tactic Global, compañías de soluciones IT y ciberseguridad, cuyo dueño es el ex agente de inteligencia Leonardo Scatturice, quien no sólo es contratista del Estado durante la actual gestión sino que, además, como investigó la prensa, es uno de los nexos políticos del presidente con los proveedores de seguridad de los Estados Unidos y el presidente de este país. En el vínculo con Israel, la figura central parece ser Mario Montoto, presidente de la Cámara de Comercio Argentino-Israelí, accionista de Global View —firma dedicada a sistemas de videovigilancia urbana— y editor de la revista y del canal DEF, especializados en defensa, seguridad e inteligencia.[115]

---

113 Para un pantallazo de las leyes de privacidad en Argentina, puede verse: Rodríguez, Katitza, Verdiana Alimonti, Leandro Ucciferri y Luiza Reheder. *Necessary & Proportionate*. EFF, 2020. URL

114 "Boletín Oficial República Argentina - Sistema de Inteligencia Nacional - Decreto 656/2024." URL

115 "Milei anunció que el Memorando con Israel implicará mejoras en Defensa. "Luego de décadas de desfalco del Estado y vaciamiento de las Fuerzas Armadas, la Argentina está francamente atrasada en capacidades militares, armamentísticas y de inteligencia. Cualquier país que se hace respetar necesita de estos recursos'", Russo, Emiliano. "Netanyahu destacó a Milei como un 'ejemplo para el mundo' y el presidente exigió la liberación 'inmediata' de los rehenes de Hamas." *Clarín*, 12 de junio de 2025. URL

Por esto último, en agosto de 2024 el diputado Juan Manuel López y la diputada Victoria Borrego presentaron un pedido de información al jefe de Gabinete preocupados por el aumento insólito de fondos reservados para la SIDE. En el documento señalaban que "el recientemente dictado DNU 656/2024, que incrementó en cien mil millones de pesos los fondos reservados de la Secretaría de Inteligencia del Estado (SIDE), enciende nuestras alarmas respecto del destino de estos recursos, que podrán ser utilizados de forma discrecional, secreta y sin ningún tipo de control o supervisión pública."[116]

Box 11: Algunos revendedores que conviene observar

- **Global Interactive Group** (a veces registrado como Digital Global Interactive Ltd.) figura como empresa constituida en Tel Aviv-Jaffa, Israel. En catálogos y programas de ferias como ISS World Latin America, aparece como socio comercial de Verint, Elbit y Rayzone Group, tres compañías israelíes que desarrollan herramientas SIGINT/COMINT/OSINT.[117] En los correos filtrados de Hacking Team de 2015, su CEO, Alejandro "Alex" Lawson fue quien firmó acuerdos de confidencialidad con la empresa italiana. Posteriormente, el 19 de enero de 2018, se realizó otra audiencia en el auditorio del Ministerio de Seguridad. En esa ocasión, la empresa Global Interactive Group (como Enforce One S.A) presentó los productos Galileo de Hacking Team y otro llamado Iron Man de la empresa "española In nova" (este último, un probable dato erróneo: muy posiblemente se trata de la conocida empresa italiana Innova SpA). En la reunión participaron representantes del ámbito de la seguridad y la inteligencia de Argentina, de la Prefectura Naval Argentina y la Secretaría de Fronteras.[118] Global Interactive Group comercializa, al menos en Argentina y México, elementos de seguimiento, contra-inteligencia, herramientas SIGINT y la herramienta OSINT española Minerva AI.
- Por su parte, la empresa **Assine S.A.**, de capital argentino, opera como representante e integradora regional de varias firmas europeas especializadas en tecnologías de inteligencia y defensa, con foco en soluciones de SIGINT, COMINT y OSINT para organismos de seguridad. En su sitio institucional, la compañía declara representar a Elettronica S.p.A. (ELT Group), líder italiano en sistemas de guerra electrónica (Electronic Warfare, EW), cuyas líneas incluyen sensores COMINT y plataformas de defensa electromagnética para

---

116 Juan Manuel López y Victoria Borrego, "Pedido de información sobre Pegasus - 4609-D-2024", 23/08/2024, *Trámite Parlamentario* n° 123. URL

117 "ISS World Latin America Brochures / Program: Presentaciones de interceptación judicial y productos de vigilancia electrónica," ISS World Latin America, catálogo de ferias, URL

118 Los participantes destacados incluyen a Martín Siracusa (Subsecretario de la Subsecretaría de Gestión Administrativa), Alejandro Lawson (CEO de Global Interactive Group / Enforce One S.A.), Luis Antonio Barreto (PFA), Luis Fernando Gallardo (Secretaría de Fronteras), Gonzalo Javier Alvarez (Global Interactive Group / Enforce One S.A.), Mario Gabriel Babijezuk (Dirección de Inteligencia de Prefectura), Rubén Sassone (Secretaría de Fronteras), Jorge Nicolás Occhionero (Global Interactive Group) y Crispín Ezequiel Ortigoza (Dirección de Inteligencia de Prefectura). "Registro Único de Audiencias." URL

fuerzas aéreas, navales y terrestres.[119] Asimismo, actúa como representante de CY4GATE S.p.A., empresa derivada del mismo grupo industrial, dedicada al desarrollo de herramientas de interceptación legal, *network intelligence* y *cyber-intelligence*, entre ellas la plataforma QUIPO, destinada a la explotación analítica de fuentes abiertas y redes de comunicación.[120] A su vez, Assine incorpora productos de Divitech S.r.l., firma italiana especializada en centros de comando y telemática para seguridad pública y gestión de operaciones[121]. De este modo, se posiciona como un nodo comercial y logístico que importa y distribuye software y equipamiento de inteligencia y defensa —principalmente desde Italia— para fuerzas y agencias estatales en el Cono Sur, funcionando como interfaz local de proveedores tecnológicos europeos en el ámbito de la seguridad estratégica.

- **TAMCE** (ex High Security) es una firma fundada en Buenos Aires en 1998 por Nicolás Ruggiero y renombrada en 2012; opera desde Argentina y México con presencia comercial en varios países de Latinoamérica y EE. UU. (Miami). Importa y comercializa, para fuerzas de seguridad, algunos armamentos, equipos de espionaje tácticos y contra medidas. Ofrece soluciones SIGINT/COMINT de venta restringida —por ejemplo, un "Interceptor Táctico PHOENIX" para captura de IMSI/IMEI—, además de sistemas de jamming (incluidos anti-drone y penitenciarios) y de análisis forense (UFED/Oxygen). En OSINT ofrece plataformas de ciberinteligencia como Medusa y Social Links (para monitoreo de redes sociales, web abierta, *deep web* y *dark web*, y análisis de CDR), orientadas a investigación criminal. En 2014 intentaron actuar como intermediarios del *spyware* producido tanto por NSO Group como por Hacking Team.
- **VEC SRL** es una empresa argentina que hoy opera como importadora, distribuidora e integradora de equipos de comunicaciones, radiofrecuencia, enlaces satelitales y vigilancia para fuerzas de seguridad y defensa. En su catálogo de "Investigaciones digitales" ofrece productos de marcas como Cellebrite, Inseyets, Chainalysis, Smart Search, Pathfinder, Clearview y Mollitiam Industries para análisis forense, monitoreo digital y OSINT. La empresa también representa a Mollitiam, con una suite de herramientas de OSINT, COMINT e interceptación electrónica destinadas exclusivamente a organismos de seguridad y fuerzas del orden. A esto se suma la distribución de Clearview AI, especializada en reconocimiento facial basado en fuentes abiertas, y de Chainalysis, enfocada en la analítica blockchain para rastrear transacciones en criptomonedas. VEC S.A., que se presenta como distribuidor oficial de Cellebrite en Argentina, concentra así un portafolio orientado al soporte tecnológico de investigaciones digitales y de inteligencia en el ámbito público y judicial.
- **HK Systems SRL** es una empresa argentina fundada en 2016 por Hugo Issel y Erik Kanter Snaider que actúa como representante local de la firma israelí PICSIX Ltd., especializada en tecnología SIGINT. Su catálogo y presentaciones públicas muestran que ofrece IMSI-catchers multibanda y sistemas de geolocalización por SS7/Diameter, además de soluciones de análisis y fo-

---

119 Elettronica S.p.A. (ELT Group), "Company Profile," acceso 16 de octubre de 2025, URL

120 CY4GATE S.p.A., "Law Enforcement & Security Agency Solutions," acceso 16 de octubre de 2025, URL

121 Divitech S.r.l., "Solutions," acceso 16 de octubre de 2025. URL

rense móvil. En 2018 se presentó en una licitación nacional con ese tipo de equipamiento y, según fuentes abiertas del sector seguridad, ha provisto o realizado demostraciones de equipos SIGINT para la Policía de Seguridad Aeroportuaria, la Policía Federal Argentina y la Gendarmería Nacional Argentina, además de otras fuerzas provinciales, con vínculos documentados en catálogos y ferias técnicas aunque los contratos no sean públicos por su carácter sensible. En conjunto, HK Systems opera como integrador argentino de tecnología de interceptación y geolocalización celular de origen israelí, con una cartera de clientes centrada en fuerzas de seguridad federales.

2.2. Demanda / Soluciones

2.2.1. *Spyware*

En 2015, las filtraciones de correos internos de la empresa italiana especializada en *spyware* Hacking Team revelaban que Argentina estaba negociando con dicha firma y con NSO Group de manera simultánea. Tanto la prensa como varias organizaciones de la sociedad civil comenzaron a expresar su preocupación por las implicancias de estas revelaciones.[122]

A través de estos correos, puede reconstruirse que, en marzo de 2012, tres miembros de Hacking Team organizaron una visita a Buenos Aires con el fin de mostrar Remote Control System (RCS) ante diversas agencias de seguridad. Las reuniones tuvieron lugar entre el 19 y el 23 de marzo en el Hotel Hilton de Puerto Madero, con la participación de representantes del Ministerio de Seguridad de la Nación (Dirección Nacional de Inteligencia Criminal), la Procuración General de la Nación (Unidad de Investigaciones Complejas), el Ministerio de Justicia y Seguridad de la Provincia de Buenos Aires y el prefecto nacional de la Prefectura Naval Argentina.

Los correos dejan claro que varias empresas locales pretendían actuar como intermediarias en el negocio. Si bien no indican que se haya concretado ninguna compra, sí mencionan la firma de dos acuerdos de confidencialidad destinados a continuar las negociaciones: uno con la empresa Nullcode Team y otro con Global Interactive Group. Nicolás Ruggiero, representante de la compañía argentino-mexicana Tamce, también quería vincular a la empresa con la agencia de inteligencia que, durante la presidencia de Cristina Fernández, dirigieron primero Héctor Icazuriaga y luego Oscar Parrilli. “Estoy seguro de que van a comprar a corto plazo (ojalá sea a nosotros)”, escribió Nicolás Ruggiero a su interlocutor de Hacking Team el 8 de julio de 2015.[123]

El optimismo resulta contundente. No obstante, la existencia de compras efectivas no pudo ser confirmada.[124] Esto plantea una pregunta crucial: ¿es posible que el software haya sido adquirido y utilizado durante algún tiempo sin conocimiento público? Se trata de un interrogante central.

---

122 Ucciferri, Leandro. “Hacking Team, software de interceptación y vulneración de derechos humanos”. *ADC Digital*, AGO 2015.

123 “WikiLeaks - The Hackingteam Archives”, 2015. URL

124 Aunque la plataforma Mobile Surveillance Monitor Network registró cuatro casos de Pegasus, del grupo NSO, en 2024, estos resultaron ser falsos positivos. URL

Dos años después, en 2017, Patricia Bullrich —quien, como señalamos, no sólo es la actual ministra de Seguridad, sino que también ocupó esta función entre diciembre de 2015 y diciembre de 2019— manifestó su interés en adquirir *spyware* para teléfonos móviles. De hecho, en el proceso de reforma del Código Penal, se intentó legalizar el uso de este tipo de programas por parte del Poder Ejecutivo para monitorear las actividades de los ciudadanos a través de sus teléfonos, computadoras y otros dispositivos, incluso sin orden judicial.[125]

Fue en este marco cuando en enero de 2018 hubo una nueva audiencia con Global Interactive Group, una de las revendedoras que había firmado el acuerdo de confidencialidad con Hacking Team, para hacer una nueva demostración de su *spyware* a los responsables de las principales fuerzas de seguridad del país.[126]

En esta ocasión, además, aprovecharon y también promocionaron otro producto. Su nombre en código era "Iron Man" y, según el legajo, era de una empresa "española" llamada "In Nova". Aquí se abren dos opciones. La más probable es que se trate de un error en el acta de la reunión y en verdad, como detallamos más adelante, la empresa en cuestión sea la italiana Innova SpA, dedicada a productos de inteligencia de redes. Si en cambio efectivamente se tratase de una empresa española, la principal candidata sería IN-NOVA, de Toledo, que participa de un programa de desarrollo de interceptador de drones. Pero no parece ser este el caso.[127]

En 2021, dos periodistas accedieron a los registros financieros de la empresa italiana Cy4gate, donde descubrieron la existencia de contratos con Argentina.[128] Para publicitar que su cartera de clientes se extendía más allá del mercado interno, la propia compañía destacó que contaba con permisos de exportación para productos de doble uso hacia Argentina —posiblemente a través de la empresa local Assine SA. A partir de los productos ofrecidos por Assine surgen dos posibilidades: que se tratara del denominado software espía Epeius, concebido como competidor de Pegasus de NSO, o bien de otros desarrollos de la empresa, como D-SINT (una herramienta de análisis pasivo tipo OSINT) o Hydra (orientada a la interceptación activa de tráfico IP).

---

125 Asociación por los Derechos Civiles (ADC), Asociación Civil por la Igualdad y la Justicia (ACIJ), Asociación Pensamiento Penal (APP) Instituto de Estudios Comparados en Ciencias Penales y Sociales (Inecip). "La reforma del Código Procesal amplía las facultades del Estado para vigilar." Políticas de Seguridad. CELS, 17 de abril de 2018. URL

126 Registro Único de Audiencias de Gestión de Intereses, Ministerio del Interior (Argentina), "Audiencia ID 9763," URL

127 La opción menos probable. Si efectivamente se tratase de una empresa española, la principal candidata sería IN-NOVA Programa de Innovación Internacional S.L.U., registrada en Toledo, que desarrolla proyectos de I+D+i y consultoría tecnológica —incluida la ciberseguridad— a través de su filial y de la Fundación In-Nova Castilla-La Mancha, vinculada al Instituto Nacional de Ciberseguridad (INCIBE). Documentos de la Plataforma de Contratación del Estado español confirman su participación en un contrato con el Instituto Nacional de Técnica Aeroespacial (INTA) para el desarrollo de un prototipo RPA interceptador, indicio de su trabajo en soluciones de seguridad y defensa. *Boletín Oficial del Registro Mercantil*, "IN-NOVA Programa de Innovación Internacional, S.L.U.," 27 de septiembre de 2024. URL // Plataforma de Contratación del Sector Público (España), *Adquisición de prototipo RPA interceptador – INTA*, 16 de octubre de 2019, URL

128 Bagnoli, Lorenzo, y Ricardo Coluccini. "Sorveglianza: l'azienda italiana che vuole sfidare i colossi NSO e Palantir." *IrpiMedia*, 17 de noviembre de 2021. URL

Otra sospecha gira en torno al software espía desarrollado por la empresa española Mollitiam Industries, cuyos productos más conocidos son *Invisible Man* y *Night Crawler*, utilizados en operaciones de vigilancia en Colombia. Diversas fuentes ubican a Mollitiam como proveedor de herramientas de ciberespionaje para fuerzas armadas y cuerpos de seguridad en América Latina, y en Argentina sus soluciones se ofrecen a través de la firma VEC SRL., que se presenta como especialista en inteligencia digital, comunicaciones críticas y defensa. Las tecnologías dirigidas a agencias de seguridad se describen bajo las etiquetas COMINT y OSINT, pero con una caracterización inusualmente ambigua: su línea COMINT se presenta como una

> **Plataforma de explotación y post-explotación. Las soluciones COMINT modulares de Mollitiam cubren todo el proceso de interceptación, mejorando los resultados operativos y optimizando los recursos. (SOLO para Agencias de Orden Público).** [129]

Indica, además, que es capaz de abarcar todo el proceso de interceptación, incluida la de comunicaciones cifradas, formulación que se aproxima más al lenguaje propio del *spyware* que al sentido clásico de la inteligencia de comunicaciones.

A esto se suma que el Informe Anual de Exportaciones de Material de Defensa y de Productos y Tecnologías de Doble Uso del Gobierno de España registra, para 2020, exportaciones hacia Argentina en la categoría 5 del anexo de doble uso —"Telecomunicaciones y seguridad de la información"—, donde se encuadran precisamente las herramientas de vigilancia e intrusión digital. Aunque los datos públicos no permiten identificar a los proveedores concretos ni los productos exportados, el hecho de que Mollitiam figure en los catálogos de la industria de defensa española y requiera licencias de exportación para parte de sus soluciones de ciberespionaje hace plausible la hipótesis de que estas tecnologías estén siendo comercializadas en el país a través de intermediarios locales como VEC, aun cuando no existan pruebas abiertas de contratos específicos con organismos federales o provinciales.[130]

En consecuencia, las sospechas persisten en distintos grados. Las empresas mencionadas —VEC S.A. (distribuidora de Mollitiam), Assine S.A. (canal de Cy4gate), Global Interactive Group (firmante del acuerdo de confidencialidad de Hacking Team en 2015 y otros contactos israelíes) y High Security / Tamce (que casi seguro fracasó como entusiasta intermediaria de Hacking Team)— figuran entre aquellas que ofrecieron soluciones de espionaje al Estado argentino.

---

129 "Mollitiam Industries soluciones de inteligencia | VEC." Acceso 25 de junio de 2025. URL

130 Secretaría de Estado de Comercio. *Informe estadístico de exportaciones de material de , otro material y productos y tecnologías de doble uso 2020*. Madrid: Ministerio de Industria, Comercio y Turismo, 2021, 55–56. URL

A pesar de no haberse probado compras concretas de *spyware*, hay que tener mucho cuidado con descartar esta posibilidad. Y no sólo porque se trata de un contexto legalizado, con elevados fondos discrecionales y múltiples canales de oferta. Como enfatizamos en el cierre del reporte, aún resta por explorar otros métodos de detección, como el análisis forense consensuado o el mapeo de infraestructura maliciosa.[131]

2.2.2. SIGINT

Argentina realizó varias licitaciones públicas para equipos *IMSI catcher* y otras tecnologías de interceptación de frecuencias, como *Direction Finder*[132]. Observarlas permite identificar empresas y equipos.[133]

HK Systems SRL ofrecía dos productos fabricados por la firma israelí Picsix: el P6 *IMSI Catcher* y el sistema de *Direction Finding* (usualmente incluido en equipos *IMSI catcher*). Este último proporciona una aplicación sencilla para Android utilizada para geolocalizar un dispositivo objetivo con cierta proximidad, ya que necesita estar dentro del rango de recepción del teléfono. Una vez que el *IMSI catcher* detecta un teléfono en la zona general, el sistema opera interceptando y analizando las señales de radiofrecuencia emitidas por el teléfono móvil en cuestión para lograr una localización más precisa.[134]

Por su parte, la empresa argentina Global Interactive Group ofrece a los países de la región dos productos bajo la marca TITAN. Se lo presenta como un localizador de celulares a gran distancia. En realidad, se trata de una estación base celular táctica portátil de alta potencia a la que los teléfonos móviles cercanos se conectan automáticamente para la captura de IMSI y la geolocalización precisa del dispositivo objetivo.[135] Resulta probable que TITAN sea el nombre

---

131 Solo se registró un caso aislado relacionado con Hermit, el software espía de la empresa italiana RCS Lab, identificado por el Monitor Network Research Workbook en 2022. Mobile Surveillance Monitor. "Surveillance Dashboard." URL

132 En Argentina, su uso debe estar amparado por orden judicial (Ley 25.520 y modificaciones).

133 Licitación Pública Nº 0006/2018, realizada en 2018. El dictamen que adjudica a Teclab LLC y desestima a HK Systems SRL Policía Federal Argentina, "Adquisición de 2 sistemas de localización IMSI Catcher y 1 sistema de consultas de geolocalización (LPU 30-0006-LPU18) — Acto de apertura," Boletín Oficial, 14 de septiembre de 2018. URL // Policía Federal Argentina, "LPU 30-0006-LPU18 — Dictamen de Evaluación (adjudicación a Teclab LLC; desestimación de HK Systems SRL y Tecoar SA)," Boletín Oficial, 18 de diciembre de 2018. URL // Ministerio de Seguridad, UAI, "Informe de Auditoría N.º 15/2024 (formulación PFA) — menciones a 'IMSI Catcher' y paquete de 2.000 consultas," 15 de octubre de 2024. URL

134 PICSIX, "P6-Catcher," Products, consultado 16 de octubre de 2025; "P6-MITM," Products, consultado 16 de octubre de 2025; "P6-Fi5," Products, consultado 16 de octubre de 2025. URL La plataforma de geolocalización de Picsix emplea una aplicación encriptada que consulta de forma pasiva las redes celulares (GSM, UMTS, LTE) para identificar las estaciones base transceptoras (BTS) a las que está conectado el dispositivo objetivo. Al determinar la ubicación de esas BTS y la dirección de la señal del dispositivo, el sistema puede inferir la posición del equipo.

135 "Localizador de celulares a gran distancia – Global Interactive Group." 15 de junio de 2025. URL

comercial del producto. Como no existe un nombre legal asociado a una firma desarrolladora, podría tratarse de una empresa sin presencia pública o de un equipo desarrollado por un ente gubernamental o industrial sin perfil comercial abierto. Algo similar ocurre con la oferta de la empresa argentino-mexicana TAMCE, que comercializa un *IMSI catcher* llamado Phoenix con capacidades de *Direction Finder*.[136]

Con respecto a estos dispositivos, es interesante destacar la existencia de los proyectos FADE (*Fake Antenna Detection Project*) de la Universidad de Washington y el proyecto Crocodile Hunter de la Electronic Frontier Foundation (EFF). Ambos proponen equipos simples de desarrollo casero para detectar el uso de *IMSI catchers* a través de una metodología estandarizada. No obstante, la evidencia recolectada por estos proyectos no prueba la existencia de *IMSI catchers*, sino que registra anomalías de red compatibles con su uso y advierte sobre posibles falsos positivos (por ejemplo, celdas mal configuradas o desactualizadas). Además, las mediciones que se realizaron en la región mediante estos dos proyectos tuvieron un alcance temporal acotado —entre abril y noviembre de 2020— y no se realizaron en momentos específicos, como marchas y huelgas, que es cuando suelen instalarse estos equipos. Dicho esto, estas mediciones reportaron en 2G un total de 17 casos (15 "network parameter outliers" y 2 "unknown tower") para el centro de Buenos Aires, mientras que en 4G no detectó anomalías.[137]

En lo que respecta a tecnologías de geolocalización mediante explotación del sistema de señalización SS7/Diameter, según su propio sitio web, la empresa israelí Kavit figura como proveedora de Argentina de este tipo de herramientas. En este punto, y más allá de quién ofrece esta tecnología, hay otra evidencia relevante. Según la plataforma Mobile Surveillance Monitor, Argentina está clasificada entre los países de mayor riesgo en términos de vigilancia mediante explotación de señales, debido a la alta presencia de infraestructura vulnerable en sus redes móviles. Es más, dentro de la región, Argentina es el país con mayor cantidad de infraestructura proclive a sufrir (y permitir) este tipo de ataques. La misma fuente informa que, desde 2022, Argentina ha registrado más de 60.000 instancias de actividad de vigilancia significativa basada en ataques de señalización —principalmente en redes 3G, con algunos incidentes sobre 4G.[138]

Sobre esto, existen además registros de demandas y licitaciones oficiales en Argentina para realizar "consultas" de geolocalización. Por ejemplo, se encuentra pública una auditoría interna de la Policía Federal Argentina donde se hace referencia a la voluntad de adquirir *IMSI catchers*, un sistema ruso de biometría de voz y "2000 consultas" de un sistema de geolocalización mediante SS7.[139]

---

136 TAMCE, "Interceptor Táctico PHOENIX (IMSI/IMEI; BTS falsa; 2G/3G/4G/LTE)," consultado 16 de octubre de 2025. URL

137 South Lighthouse, *FADe (Fake Antenna Detection Project)*, "Buenos Aires (2G)," URL; "Buenos Aires (4G)," accedido el 5 de noviembre de 2025, URL; "FAQs," accedido el 5 de noviembre de 2025, URL

138 Mobile Surveillance Monitor. "Mobile Surveillance Monitor: surveillance dashboard." Accedido el 12 de diciembre de 2025. URL

139 Ministerio de Seguridad, UAI, "Informe de Auditoría N.º 15/2024 (formulación PFA)", 15 de octubre de 2024. URL

2.2.3. Inteligencia de tráfico IP

Desde 2003, el marco normativo argentino obliga a que los operadores de telecomunicaciones implementen capacidades de interceptación legal (LI) compatibles con estándares ETSI y 3GPP.[140] Esto implica usar módulos obligatorios de LI en los core de red. Por eso hoy en día resulta posible acceder al número de pedidos de interceptación de este tipo que se solicitaron en los últimos años.[141] Además, desde entonces es posible encontrar registros de entrega de equipos de "interceptaciones" a la Dirección de Delitos Complejos por parte de la Agencia Federal de Inteligencia.[142]

Ericsson y Nokia son los fabricantes de la infraestructura de las empresas de telefonía más grandes del país —Claro, Movistar y Personal. Dado que depende de estos operadores proveer de capacidades de interceptación, resulta esperable que, a su vez, sean también Ericsson y Nokia los que provean sus propios módulos de *Lawful Interception* ya integrados.[143]

Existen además registros de productos comercializados por la empresa estadounidense Pat Systems.[144] Su suite Vortex AIT-Stack incorpora tanto *IMSI catchers* como un sistema de interceptación de comunicaciones IP que se integra directamente con las redes de telecomunicaciones para capturar metadatos y contenido de comunicaciones, en cumplimiento con las normas ETSI. A través de nodos desplegados dentro de la red del proveedor, el sistema intercepta llamadas, mensajes y tráfico IP, y luego transmite la información en forma cifrada a un centro de monitoreo, donde se procesa, analiza y almacena. Dependiendo del protocolo utilizado en cada caso, el sistema puede acceder a contenido no cifrado o interceptarlo antes o después de aplicarse el cifrado. Según uno de los folletos promocionales —ya antiguo— de la compañía, la plataforma incluye funciones avanzadas

---

140 Decreto 357/2002 y resoluciones de la Secretaría de Comunicaciones. Corte Suprema de Justicia de la Nación, "Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado (DAJuDeCO)." *Poder Judicial de la Nación*, URL

141 Entre 2016 y 2025, la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado (DAJuDeCO) consolidó un marcado incremento en la demanda de asistencia vinculada a interceptación y tratamiento de información de comunicaciones. El 79,4 % de las asistencias se originó en pedidos de los ministerios públicos fiscales, frente a un 20,6 % de los juzgados. En el mismo período se registraron 5.327 asistencias de adelanto de comunicaciones y 1.875 asistencias en materia de comunicaciones, mientras que los pedidos de información asociada ascendieron a 206.818, mayoritariamente dirigidos al Ministerio Público Fiscal. Entre 2019 y 2024, se tramitaron 160.232 solicitudes de datos procesados, que dieron lugar a 426.349 respuestas, lo que evidencia una fuerte intensificación en el uso de herramientas de investigación basadas en datos de tráfico y sus metadatos. "Crece la actividad de la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado con el sistema acusatorio." URL / URL

142 Argentina.gob.ar. "La AFI entregó equipos a la DAJUDECO." 17 de julio de 2020. July 17, 2020. URL

143 Nokia Corporation, "Lawful Intercept (LI) describes a process to intercept telecommunications... Nokia's implementation satisfies most national standards' requirements," *Nokia Infocenter*, URL // Ericsson AB, "Regulatory Products," URL

144 "PAT Systems | Surveillance Watch." Consultado 12 de diciembre de 2025. URL

como herramientas de búsqueda y geolocalización, asegurando trazabilidad y seguridad en las operaciones.[145]

También está disponible en el mercado local el equipo desarrollado por la italiana Cy4gate. Por la oferta, podría tratarse de su producto Hydra. Del mismo modo, este sistema se despliega dentro de la infraestructura del proveedor de servicios de Internet (por ejemplo, conectado a un punto de agregación, un router core o un switch de *backbone*), lo que le permite integrarse de forma pasiva en los flujos de tráfico de la red. Hydra recopila metadatos —como visitas a sitios web, uso de aplicaciones y frecuencias de comunicación— y genera perfiles digitales. El sistema no descifra contenido ni accede a mensajes privados; su foco es exclusivamente el análisis de metadatos y el comportamiento digital. No obstante, es capaz de perfilar categorías de contenido, identificar usuarixs y patrones de uso, mapear conexiones, inspeccionar paquetes y extraer metadatos visibles del tráfico de red. Cabe señalar que Cy4gate ofrece actualmente un producto integral denominado CEWIS (Cyber Electronic Warfare Integrated System), que integra distintos módulos, con tecnología de *IMSI catcher*, explotación del protocolo SS7/Diameter, interceptación de comunicaciones, *direction finding* y capacidades OSINT.[146]

Resulta muy probable que Global Interactive Group haya ofrecido, como intermediaria, los productos de Innova SpA en 2018. Se trata, de hecho, de otra empresa cuyos productos se han comercializado junto con los de Hacking Team en otras ocasiones y otros países de la región (por ejemplo, en Chile en el mismo año). Innova suele especializarse en sistemas de monitoreo IP de *Lawful Interception*, como EGO, y el nombre "Iron Man", que aparece mencionado en el registro de la audiencia con la empresa, sería un alias o derivado comercial para agencias argentinas.[147]

A esta lista de herramientas que probablemente fueron adquiridas en Argentina, podría agregarse también Cognyte (antes Verint), ya que Argentina figura como "cliente gubernamental regional" en el material de marketing de la empresa de 2021.

Como señalamos en el punto 1.1.3., si una agencia de seguridad conectara por su cuenta plataformas comerciales como Vortex (PAT Systems), Hydra/Cewis (Cy4gate) o EGO (de Innova) a puntos de acceso en la infraestructura, surge la duda sobre hasta qué punto esas herramientas podrían proporcionar visibilidad útil y sostenida al tráfico, sin colaboración con las empresas proveedoras de servicios; es decir, por fuera de los límites legales.

Algunos apuntes sobre esto. (i) El mencionado informe técnico de 2014 titulado *"Lawful Hacking: Using Existing Vulnerabilities for Wiretapping"* ya había analizado cómo, con el auge de comunicaciones cifradas extremo-a-extremo, las capacidades de interceptación requieren combinarse con técnicas que apunten directamente a los dispositivos para obtener los datos antes de que sean cifra-

---

145 PAT Systems, *VORTEX AIR-STACK V4 — IMSI CATCHER* (folleto/PDF), consultado el 16 de octubre de 2025. URL // "Pat Systems - Centros de Monitoreo.", URL / "Pat Systems | Vortex-Stack." URL

146 "HOMELAND SECURITY MOBILE ASSETS | CY4GATE S.p.A.". URL

147 Una posibilidad es que se trate de EGO (también comercializado en Chile durante los mismos años) u otra plataforma centralizada para interceptación de tráfico IP desarrollada por Innova S.p.A.. "Innova_Product List, Specifications_MicroIP, EGO, Internet Interception and Probes, Gps Innova, RB800.", 2011. URL

dos.[148] (2) Más recientemente, Amnesty Tech documentó cómo la suite de Intelexxa integra herramientas de inteligencia de red con otras técnicas adicionales de discutible legalidad. En este caso, Predator está diseñada para operar en cooperación con los proveedores de Internet para inyectar enlaces de infección mientras la víctima navega por la web.[149] (iii) En la investigación ya citada, CIPER documentó la capacidad operativa de módulos de interceptación legal fuera del circuito formal.[150]

A partir de estas investigaciones, podemos pensar que, al menos técnicamente, podrían efectuarse copias de tráfico y metadatos para su almacenamiento y análisis, pero su alcance práctico dependería críticamente de factores como el punto exacto de conexión y la escala del despliegue. Plataformas como Hydra, Vortex o EGO pueden operar legítimamente como sistemas LI dentro del cauce estandarizado. Sin embargo, pueden funcionar junto a otras tecnologías para interceptar fuera del marco legal si reciben copias de tráfico o se combinan con otras herramientas de modo que cambien por completo la validez jurídica, la trazabilidad y los riesgos de abuso.

2.2.4 Monitoreo de red

Al menos desde el 2010, dentro de esta categoría debe incluirse a Blue Coat, uno de los principales proveedores de la NSA y desarrolladora de PacketShaper, equipos que pueden emplearse tanto para asegurar y administrar redes como para restringir el acceso a la información y vigilar las comunicaciones y el tráfico de Internet[151].

También con alcance regional, la empresa Sandvine reportó el despliegue de sus soluciones de gestión de tráfico en múltiples países de América Latina, sin detallar específicamente si estos incluyen a Argentina, Chile o Uruguay.[152] Algo similar ocurre con Allot. Esta última ofrece a los operadores de telecomunicaciones una plataforma de "network intelligence & traffic management" que incluye

---

148 En el 2014, este paper explicaba "the viability and implications of an alternative method for addressing law enforcement's need to access communications: legalized hacking of target devices through existing vulnerabilities in end-user software and platforms. The FBI already uses this approach on a small scale; we expect that its use will increase, especially as centralized wiretapping capabilities become less viable". Bellovin, Steven M., Matt Blaze, Sandy Clark, and Susan Landau. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet." *Northwestern Journal of Technology and Intellectual Property* 12, n.º 1 (2014): 66. URL

149 Amnesty International Security Lab, "To Catch a Predator: Leak Exposes the Internal Operations of Intellexa's Mercenary Spyware". URL

150 Peña, Cristóbal y Sebastián Minay, "Así se hacen los cuestionados 'pinchazos' telefónicos legales." Investigación. *CIPER Chile*, 29 de octubre de 2008. URL

151 Marquis-Boire, Morgan, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton. *Some Devices Wander by Mistake: Planet Blue Coat Redux. Citizen Lab and Canada Centre for Global Security Studies,* Munk School of Global Affairs, University of Toronto, 2013. URL

152 Sandvine, "Network Intelligence Solutions for Telecom Operators", reporte de despliegue, consultado 16 de octubre de 2025. "Sandvine Expands Multi-Country Deployments Across Latin America," Sandvine Press Release, 2023, URL // BNamericas, "Sandvine Seals US$ 3 mn Contract with Tier 1 LatAm Telco," *BNamericas*, 15 de julio de 2022, URL

inspección profunda de paquetes (DPI), visibilidad de aplicaciones y usuarixs, control de políticas y gateway de servicio de alta capacidad. La empresa anunció que "un operador fijo de nivel 1 en América Latina, con millones de suscriptores, selecciona Allot HomeSecure para ofrecer servicios de ciberprotección", lo que sugiere un contrato comercial regional.[153]

En 2021, Telecom Argentina implementó junto a Cisco y Qwilt una plataforma de *Open Caching* integrada en su infraestructura, orientada a mejorar la distribución de contenidos de video mediante análisis avanzado de tráfico.[154] Aunque esta tecnología no constituye un sistema de inspección profunda de paquetes (DPI) en sentido estricto, comparte mecanismos de análisis y optimización del flujo de datos a nivel de red, otorga un nivel significativo de visibilidad sobre los flujos de datos del operador.[155]

Como este reporte ha enfatizado desde la introducción, conocer las capacidades de intrusión y monitoreo de herramientas como estas subraya la relevancia de discutir sus alcances y aplicaciones.

2.2.5. OSINT/WEBINT

Argentina también ha emergido como un comprador destacado de herramientas de análisis de contenidos web.[156] Poco después del anuncio del Ministerio de Seguridad, ya en 2018 la Asociación por los Derechos Civiles (ADC) alertó sobre los riesgos en materia de derechos humanos vinculados al monitoreo estatal de publicaciones en redes sociales.[157] Ese fue el año, de hecho, en que, probablemente mediante la empresa israelí Rafael, se adquirieron soluciones OSINT de Verint y Cognyte, compatibles con sus opciones de monitoreo IP.[158]

En el mercado local se ofrece, además, D-SINT de la empresa italiana Cy4gate, que posee una licencia de exportación para tecnologías de doble uso en el país. Diseñada para competir con Palantir, recopila, procesa y analiza plataformas digitales —como redes sociales, foros y bases de datos públicas o semiabiertas— mediante técnicas de *scraping*, *text mining* y análisis de patrones comunicacio-

---

153 Allot, *Allot Solutions for Service Providers* (ca. 2021), folleto técnico, URL // Allot, "Tier-1 Fixed Broadband Operator, with Millions of Subscribers in Latin America, Selects Allot HomeSecure to Provide Cyber Protection Services," *Press Release*, 11 de mayo de 2023, URL

154 Qwilt, "*Open Caching and Edge Delivery for Telecom Operators*", URL // Cisco Systems, "Telecom Argentina Launching New Cisco, Qwilt and Digital Alpha CDN Solution to Improve Streaming Experience for Its Customers in Argentina," *Cisco Newsroom*, 5 de febrero de 2021, URL

155 *"Telecom Argentina Adopts Open Caching CDN Solution from Cisco and Qwilt,"* Cisco Newsroom, 2021, URL // Telecom Argentina, *"Plataforma Open Caching CDN 'as-a-service'"*, comunicado de prensa, 2021.

156 Ucciferri, Leandro. *Seguidores que no vemos – Una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence (SOCMINT)*. ADC, 2018. URL

157 Asociación por los Derechos Civiles (ADC), *Seguidores que no vemos: prácticas estatales de monitoreo en redes sociales y sus impactos en los derechos humanos*, Buenos Aires, 2018, URL

158 "InfoLEG - Ministerio de Justicia y Derechos Humanos - Argentina." URL

nales. El sistema está concebido para funcionar conjuntamente con Phoenix o Hydra —desarrollados también por la misma empresa— de modo que opere como una plataforma de fusión de datos que integra múltiples fuentes. Según la información disponible, incluye funciones de reconocimiento facial y de objetos, lo que permite realizar búsquedas de información sobre personas y elementos en textos, bases de datos de imágenes y redes sociales.[159]

A esta oferta y disponibilidad se suma otra pista: la licitación realizada por la Policía de Seguridad Aeroportuaria (PSA) en 2024. El pliego oficial para la adquisición de una "Plataforma integral de fusión de datos, geolocalización y WEBINT" detalla requerimientos compatibles, sobre todo, con esta herramienta, ya que menciona capacidades de fusión, análisis y visualización de datos heterogéneos en tiempo real —con funciones de gestión de casos, geolocalización celular, perfilado OSINT/social media, análisis de gráficos/IA, exportación de informes y análisis predictivos.[160] Ninguna de las otras plataformas OSINT mencionadas más adelante cubre simultáneamente el análisis WEBINT con AI y la geolocalización exigida por el pliego (MSISDN/IMSI (2G/3G/4G), mientras que, en cambio, el pack completo de Cy4gate (D-SINT/QUIPO) con herramientas de LI es el único que podría cumplir todos estos requerimientos.[161] Por lo tanto, resulta convincente pensar que la licitación fue armada para esta compra.

En esta categoría también puede incluirse el sistema de i2 Limited, adquirido al menos tanto por el Ministerio de Seguridad como por la ciudad de Buenos Aires y por la provincia de Río Negro en 2019. Se trata más bien de un motor de análisis diseñado para compatibilizarse con otras herramientas de minería a las cuales las contrataciones públicas dicen vincularlo.[162] En base a la información disponible, i2 Limited —filial de IBM desde 2008— ofrece una plataforma avanzada de análisis y visualización de datos de redes y relaciones, para identificar patrones y predecir eventos futuros mediante inteligencia artificial.[163]

También es muy probable que algunas agencias de seguridad del país utilicen Medusa, el sistema OSINT de la empresa italiana IPS Intelligence (Intelligence Positioning Solutions), dedicada además al análisis, inteligencia e intercepta-

---

159 Bagnoli, Lorenzo, and Ricardo Coluccini. "Sorveglianza: l'azienda italiana che vuole sfidare i colossi NSO e Palantir." *IrpiMedia*, 17 de noviembre de 2021. URL

160 *"Plataforma integral de fusión de datos, geolocalización y WEBINT" (pliego oficial)*, Gobierno de la República Argentina, 2023, URL

161 "Products | CY4GATE S.p.A." Accessed December 12, 2025. URL

162 "I2 Analyst's Notebook - Discover and Deliver Actionable Intelligence | I2." Accedido 1 de agosto de 2025. URL // IBM. "IBM -Integrated Law Enforcement: A Holistic Approach to Solving Crime." IBM, 2014. URL

163 Hubo una contratación directa del Ministerio de Seguridad (2016) titulada "Software avanzado para el análisis criminal con la firma Unitech S.A." (Proc. 347-0066-CDI16), y apunta a analítica e inteligencia criminal (link-analysis, minería de datos, visualización de redes). Organizaciones que auditaron ese proceso citan el mismo expediente y lo vinculan con la suite IBM i2 (Analyst's Notebook / Enterprise Insight Analysis), una familia de herramientas usada por ministerios de seguridad y fiscalías para descubrir patrones, relaciones entre personas/llamadas/casos, líneas de tiempo y grafos. Además, en 2018 el MPF CABA adjudicó un "paquete de análisis criminal i2"; en esa actuación, IBM informó que Unitech S.A. era su reseller autorizado, lo que encaja con el rol de integrador/distribuidor de software analítico. URL

ción de redes IP.[164] Medusa permite recopilar y analizar grandes volúmenes de datos provenientes de redes sociales, la *Deep* y *Dark Web*, con el fin de transformar esta información pública en inteligencia accionable. Según su prospecto, aplicada en ámbitos de seguridad nacional y defensa, utiliza algoritmos avanzados de inteligencia artificial para identificar tendencias en tiempo real, monitorear sentimientos y opinión pública, y analizar la difusión de mensajes. Además, automatiza el perfilado de objetivos en línea, facilita operaciones encubiertas mediante la gestión de avatares y permite interacciones proactivas en redes sociales, como la difusión de contranarrativas o la respuesta a publicaciones clave, incrementando la capacidad de reacción y prevención frente a amenazas digitales. Una de sus particularidades es que afirma poder acceder incluso a navegación cifrada en TOR.[165]

Minerva AI es otra herramienta OSINT/WEBINT española ofrecida por TAMCE en el mercado latinoamericano. Sus capacidades van más allá de una simple herramienta de *scraping* y análisis. Más bien se ofrece como una suite de soluciones de ciberseguridad, ciberinteligencia y ciberdefensa que se basa en modelos propios de inteligencia artificial, *machine learning, deep learning* y *big data* para detectar, analizar y anticipar amenazas complejas, especialmente en entornos con grandes volúmenes de datos. Si bien es difícil ver más allá del marketing, ofrece desde servicios de ciberseguridad de infraestructuras y sistemas hasta análisis de información y narrativas digitales con apoyo de analistas humanos, consultoría y peritaje informático forense, para organismos civiles, militares y gubernamentales.

TAMCE ofrece además al mercado regional otra solución OSINT orientada tanto a agencias de seguridad como a empresas: Social Links CrimeWall, que permite hacer investigaciones que reconozcan objetos, biometría facial y sentimientos a través de distintas redes sociales y fuentes abiertas.[166]

Queda claro que, en los últimos años, Argentina ha avanzado de manera sostenida en la implementación de sistemas de inteligencia basados en análisis de datos y monitoreo digital, mediante herramientas de WEBINT, geolocalización y análisis automatizado mediante inteligencia artificial. En 2024, obtuvo de hecho un nuevo marco. La Unidad de Inteligencia Artificial del Ministerio de Seguridad formalizó su infraestructura mediante la Resolución 710/2024 para autorizar el uso de software de análisis de actividades en redes sociales, anticipar disturbios y seguir movimientos delictivos.[167] Una vez más, resulta conveniente mencionar que esta "unidad" fue creada por resolución ministerial, como parte de una dependencia creada también por resolución ministerial, reportando directamente al jefe del gabinete de asesores de la Ministra Patricia Bullrich; es decir: por fuera de todo organigrama formal y por fuera del alcance de la Ley de Inteligencia (que prohíbe expresamente que cualquier otra dependencia que no figure en la ley realice tareas de inteligencia).

---

164 Además de la oferta de TAMCE, sabemos que IPS S.p.A. aparece como proveedor global de inteligencia de fuentes abiertas que opera, entre otras regiones, en América Latina, con subsegmentos que incluyen a Argentina. URL

165 "MEDUSA - Plataforma de Inteligencia Activa | TAMCE. URL

166 "CrimeWall." *TAMCE*, Consultado el 19 de octubre de 2025. URL

167 *Resolución 710/2024*, Boletín Oficial de la República Argentina, 29 de julio de 2024, URL

Tabla 2: Resumen Argentina

ARGENTINA				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Spyware	**Hacking Team (Italia)**	Global Interactive Group / Nullcode Team / TAMCE.	Remote Control System (RCS) ofrecido bajo distintos nombres, entre ellos Galileo.	Probable. Hizo demostraciones en Argentina al menos en 2012 y 2018.
	NSO Group (Israel)		Pegasus	Probable. Mantuvo negociaciones al menos durante 2014.
	Mollitiam (España)	VEC S.A.	*Invisible Man / Night Crawler*	Probable. La empresa VEC ofrece sus productos como "plataforma de explotación" y tiene permisos de exportación de productos de doble uso en ciberseguridad a Argentina.
	Cy4gate (Italia)	Assine S.A.	Epeius	Probable. Tiene una revendedora local y permisos de exportación de productos de doble uso en ciberseguridad a Argentina

ARGENTINA				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
SIGINT	**PICSIX (Israel)**	HK Systems SRL	*IMSI catcher* / *Direction Finder* / SS7 exploitation	Muy probable. Fue ofrecida en licitaciones nacionales y provinciales.
	TITAN (EE.UU.)	Global Interactive Group	*IMSI catcher*	Muy probable.
	Kavit (Israel)		SS7-Diameter exploitation	Muy probable. Confirmado por la propia empresa.
	Pat Systems (EE. UU.)		*IMSI catcher* / SS7 exploitation	Muy probable. Publicitada por la compañía.
	Phoenix	TAMCE	*IMSI catcher* / *Direction Finder*	Confirmada.
	Cy4gate (Italia)	Assine S.A.	*IMSI catcher* / SS7-Diameter exploitation	Muy probable. Tiene una revendedora local y permisos de exportación de productos de doble uso en ciberseguridad a Argentina.
	Rohde & Schwarz (Alemania)	Rohde & Schwarz Argentina SRL	*IMSI catcher* / *Direction Finder*	Muy probable. Tiene una filial local y numerosos acuerdos nacionales y provinciales.

ARGENTINA				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Inteligencia de red / *Lawful interception*	**Pat Systems (EE. UU.)**			Probable
	Cy4gate (Italia)	Assine S.A.	Hydra / CEWIS	Probable
	Rohde & Schwarz (Alemania)	Rohde & Schwarz Argentina SRL		Muy probable. Tiene una filial local y numerosos acuerdos nacionales y provinciales.
	Ericsson (Suecia)	Movistar, Personal, Claro	Ericsson *Lawful Interception* (LI-IMS/LMISF)	Confirmada
	Nokia (Finlandia)	Movistar, Personal, Claro	Nokia LI	Confirmada
	Innova S.p.A. (Italia)	Global Interactive Group	Algún sistema de *Lawful Interception*	Probable
Monitoreo de red	**Blue Coat (EE. UU.)**		PacketShaper	Confirmada
	Sandvine / Procera (Canadá)	Ingram Micro / Datco / Cablevisión–Fibertel	Active Network Intelligence, PacketLogic	Muy probable
	Allot (Israel)	Telefónica	Service Gateway Tera (SG-Tera) (DPI para CSP e ISP)	Confirmada

ARGENTINA				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
OSINT / WEBINT	**Cy4gate (Italia)**	Assine S.A.	D-SINT / QUIPO	Probable
	I2 Technologies / IBM (EE. UU.)	Unitech S.A.	i2 Analyst's Notebook: motor de búsqueda y visualización integrable con otras tecnologías de minería de datos	Confirmada
	Minerva IA (España)	Global Interactive Group		Probable
	Rafael - Verint / Cognyte (Israel)		SOC (Security Operations Center) + herramientas OSINT	Confirmada
	IPS Intelligence Spa (Italia)	TAMCE	Medusa	Probable

ARGENTINA				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Extracción forense	**Cellebrite (Israel)**	Security Team Network S.A. / IAFIS Argentina S.A., ARSEC	UFED	Confirmada
	Digital Intelligence (EE. UU.)	Estudio de Informática Forense	Forensic Recovery of Evidence Device (FRED)	Confirmada
	EnCase Forensic (EE. UU.)			Confirmada
	MOBILedit Forensic (República Checa)			Confirmada
	MSAB (Suecia)	VEC S.A.		Confirmada
	Oxygen Forensics (EE. UU.)			Confirmada
	Silicon Forensics (EE.UU.)	HOZ S.A		Confirmada

ARGENTINA				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Videovigilancia / Biometría / Reconocimiento facial	**3M Electronics Monitoring Inc. (EE.UU.)**		Biometría	Confirmada
	AnyVision / Oosto (Israel)		Better Tomorrow	Confirmada
	BGH Tech Partner (Argentina)		Videovigilancia - reconocimiento facial	Confirmada
	Clearview AI (EE.UU.)		Reconocimiento facial (fuentes abiertas)	Confirmada
	Haivision (Canadá)	Danaide SA		Confirmada
	Hikvision y Dahua (China)		Cámaras y análisis biométrico de video	Confirmada
	Huawei y ZTE (China)			Confirmada

ARGENTINA				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
	IDEMIA (ex Morpho) (Francia)			Confirmada
Videovigilancia / Biometría / Reconocimiento facial	**Incode (EE. UU.)**		Identidad digital y biometría	Confirmada
	Jumio (EE.UU.)		Verificación de identidad	Confirmada
	NEC (Japón)		Biometría y reconocimiento facial.	Confirmada
	NtechLab (Rusia)		Find Face, UltralP	Confirmada
	Veridas (España)		Biometría de voz y facial.	Confirmada
	Speech Technology Center (STC Group) / Speech Pro (Rusia)		Biometría de voz (herramientas de análisis acústico)	Confirmada

3. Chile
3.1. Contexto

Chile también estuvo en el listado de países hacia los cuales se reveló que Alemania había exportado herramientas de doble uso para cibervigilancia.[168] En 2014 esto constituyó un hito regional. Con esto, también las hipótesis señaladas en el apartado anterior pueden aplicarse a este caso. Además, al año siguiente, el país tuvo un lugar central en la filtración de correos de Hacking Team, con la diferencia de que en este caso se mencionaba a la Policía de Investigación de Chile como uno de sus clientes directos.[169]

En 2017 otros dos eventos atrajeron la atención mediática. Global Systems Chile —una afiliada de la compañía israelí Rebrisa Ltd.— vendió globos de vigilancia a la municipalidad de Las Condes. Esto marcó el inicio de distintas investigaciones sobre videovigilancia y biometría. En esta misma secuencia, el portal América Transparente reveló más adelante una inversión millonaria en un sistema de reconocimiento facial provisto por la empresa francesa IDEMIA, que funcionaba en secreto en Santiago de Chile.

También en 2017 se difundió la llamada *Operación Huracán.* En el contexto de conflicto social en el sur del país, una fabricación policial de pruebas falsas fue utilizada para incriminar a activistas mapuches en actos de violencia. Los datos falsos para la "investigación" de Carabineros surgían de una supuesta interceptación de mensajes encriptados de WhatsApp. Para justificar haber accedido a estos mensajes, afirmaron que Carabineros poseía una herramienta de software espía desarrollada localmente llamada "Antorcha". Los informes posteriores no sólo mostraron que se trataba de pruebas falsas, sino que incluso pusieron en duda la existencia de dicha herramienta.[170]

El 18 de octubre de 2019 comenzó un importante ciclo de movilizaciones sociales que se extendió hasta marzo de 2020. Durante estos meses, la organización civil especializada Derechos Digitales recibió una importante cantidad de denuncias sobre investigaciones policiales y acciones de intimidación basadas en información obtenida mediante el monitoreo de redes sociales.[171] En este contexto convulsionado, las filtraciones de documentos internos de Carabineros conocidas como "Pacoleaks" revelaron casos de espionaje policial contra activistas, sindicatos y grupos estudiantiles.[172]

---

168 TEDIC. "La adquisición y el abuso de tecnologías de vigilancia en América Latina - Al Sur." *TEDIC*, 28 de marzo de 2019. URL

169 "WikiLeaks - The Hackingteam Archives." 2015. URL

170 Garay, Vladimir, y Zack Rogoff. *Tecnología y vigilancia en la operación Huracán: Una revisión del trabajo periodístico realizado en torno al caso.* Derechos Digitales, 2018. URL

171 Derechos Digitales, "Situación de derechos humanos y el uso de tecnología en el contexto de la protesta social en Chile 2019", Santiago de Chile, noviembre 2019; URL ; Datos Protegidos. "Informe 2020 - Libertad de expresión en Chile." *Fundación Datos Protegidos*, 30 de junio de 2021. URL

172 Fossa, Lissette. "PacoLeaks: Estos son los nombres y organizaciones que han sido vigiladas por Carabineros en los últimos meses." *Interferencia*, 1 de noviembre de 2019. URL

A raíz de estos episodios de alto perfil, la Comisión Interamericana de Derechos Humanos condenó ese mismo año la vigilancia a periodistas que investigaban casos de corrupción, así como también la fabricación de pruebas policiales y el monitoreo de sindicatos y organizaciones sociales. Las investigaciones realizadas por organizaciones como Amnistía Internacional, la Comisión Interamericana de Derechos Humanos, Human Rights Watch y la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos determinaron la ocurrencia de graves violaciones cometidas por funcionarios del Estado chileno.[173]

En los años posteriores, el debate sobre las capacidades estatales de vigilancia se trasladó del plano mediático al normativo. A partir de 2018, distintas resoluciones técnicas comenzaron a incorporar un marco habilitante para la retención y el cruce de datos de tráfico. Este proceso culminó en 2025 con una reforma más amplia del reglamento que regula la interceptación y grabación de comunicaciones (DS 142/2005), la cual actualizó los procedimientos para órdenes judiciales y el tratamiento de registros de tráfico.[174] Ese mismo año, una norma complementaria introdujo la facultad de intervenir redes mediante "tecnologías que simulen sistemas de transmisión de telecomunicaciones"; es decir, simuladores de celdas o *IMSI catchers*. El nuevo texto menciona expresamente los identificadores IMSI, IMEI, MSISDN e IP, ampliando la cobertura de los regímenes de datos de localización y autenticación. Con ello, Chile pasó de episodios puntuales de vigilancia irregular a un entorno regulatorio más formalizado, aunque aún cuestionado por organizaciones civiles por la falta de transparencia en la aplicación de estas tecnologías y la ausencia de controles democráticos efectivos.

Box 12: Algunos revendedores que conviene observar

- **Tecnodata**. proveedor histórico en el circuito tecnológico de Carabineros, ligado especialmente a la infraestructura de interceptación y soporte técnico. En particular, investigaciones periodísticas señalan que el sistema danés ETI (operativo desde 2001 para interceptaciones) fue adquirido a través de Tecnodata —asociada públicamente a Alfredo Giacoman—, quedando Tecnodata posicionada como un actor recurrente en el ecosistema de compras y soporte de tecnologías sensibles para la institución.
- **Mipoltec / Milpotec** fue creada en 2013 por Jorge Patricio Lorca Rivera (ex empleado de Tecnodata), quien pasó a operar como proveedor e integrador de equipamiento de uso policial con foco en capacidades de interceptación. Mipoltec se adjudicó por licitación privada la provisión del sistema de interceptación EGO de Innova SpA para Carabineros (adjudicado a fines de 2013 y contratado en 2014) y, en paralelo, obtuvo contratos asociados a monitoreo e intervenciones telefónicas para otras agencias. Lorca/Mipoltec fue también el intermediario local de Hacking Team en la venta del RCS Galileo (rebautizado "Phantom") a la Policía de Investigaciones, y los

173 Montes, Rocío. "La ONU denuncia 'violaciones graves de los derechos humanos' durante el estallido social en Chile." *El País* (Madrid), 13 de diciembre de 2019. URL

174 *Diario oficial de la República de Chile* - Núm. 42.096, sábado 30 de junio de 2018 - Núm. 44.063, viernes 31 de enero de 2025 - Núm. 44.073, miércoles 12 de febrero de 2025. URL // URL // URL

correos filtrados publicados por Wikileaks muestran intercambios directos entre ejecutivos de Hacking Team y Lorca bajo el asunto “Propuesta a DEMTEL” (Departamento de Monitoreo Telefónico), además de referencias a presentaciones comerciales para Carabineros en carácter de prospecto.

- **SAT Internacional S.A.** es una empresa chilena constituida en 1990, fundada por el ex coronel Jaime Vicencio Serre. Su representante legal, lobbista y accionista es su hijo, Jaime Vicencio Silva. En el campo de inteligencia/OSINT, SAT Internacional aparece en registros oficiales de la Ley del Lobby como gestor de intereses para presentar en Chile a Prelysis (Israel) y su plataforma Tucán, descrita allí como un software OSINT para monitorear mensajería instantánea y redes sociales (incluyendo la narrativa de “desanonimizar” usuarios y mensajes) y también para búsquedas en “data leaks”. Como parte de su perfil de intermediación y representación de proveedores extranjeros (no sólo de vigilancia), SAT Internacional también figura en un registro institucional chileno de “proveedores especiales extranjeros con representación en Chile” como representante en Chile de Israel Weapon Industries (IWI). Y en el mismo ecosistema de audiencias por Ley del Lobby, SAT Internacional aparece gestionando presentaciones vinculadas a Israel Aerospace Industries (IAI), consignada como su “representada” .
- **DYMEQ Ltda.** (DYM Equipos e Ingeniería Limitada) aparece como un integrador y proveedor chileno con foco en seguridad y telecomunicaciones que declara entregar soluciones a las FF.AA. y al gobierno para el monitoreo de señales terrestres y satelitales, incluyendo “sistemas de radio inteligencia” dentro de su oferta en defensa. En registros administrativos, su rol se conecta con capacidades típicas de radiomonitoreo del espectro radioeléctrico para transmitir información al centro de monitoreo de la Subsecretaría de Telecomunicaciones SUBTEL, incluyendo componentes y licencias de Rohde & Schwarz, lo que refuerza el perfil de proveedor recurrente en infraestructura de señales. Complementariamente, en audiencias registradas bajo la Ley del Lobby, DYMEQ figura presentando “equipamiento de comunicaciones y Guerra Electrónica” y, en esa instancia, se presenta como representante en Chile de Rohde & Schwarz, lo que encaja con un patrón de intermediación y representación local para tecnologías sensibles.
- **DTS** (Desarrollo de Tecnologías y Sistemas SpA) se perfila como un actor del sector defensa–electrónica insertado en ámbito del SIGINT y adyacentes. Su origen está formalmente ligado al Estado. La Empresa Nacional de Aeronáutica de Chile (ENAER) consigna que en 1991 se creó la filial DTS como sociedad con ELTA Systems Limited en el marco de la diversificación hacia electrónica aeronáutica. En la prensa especializada, DTS aparece brindando capacidades para defensa —guerra electrónica y soporte/modernización— y la articulación industrial, lo que la posiciona como proveedor tecnológico recurrente del ecosistema militar chileno. En su propia oferta pública, DTS explícita trabajo en guerra electrónica “utilizando el espectro electromagnético” y muestra un catálogo de productos y soluciones. Complementariamente, la empresa y terceros han visibilizado alianzas técnicas con proveedores internacionales del rubro (por ejemplo, capacitación y equipamiento de Rohde & Schwarz para pruebas EMC bajo estándares militares), señal típica de integradores que operan en cadenas de suministro de tecnologías sensibles. Cabe destacar su acuerdo como importadora regional de la empresa italiana ELT Group / Cy4gate SpA.

- **Grupo Zeuz / RightCom** (ecosistema Verint/Intelligence/Cognyte). Grupo Zeuz se presenta como representante oficial de Verint en Chile, y en registros de la Ley del Lobby hay entradas donde figuran como representantes para el Cono Sur de Verint/Cognyte ante instituciones del ámbito de defensa y seguridad.
- **Innova Chile SpA** es la única filial regional de la empresa italiana de interceptación legal Innova S.p.A., empresa que figura desde su constitución en 2019 como accionista única y es representada por Daniele Traunero. Define un objeto social explícito de "suministro de productos y servicios en el campo de la seguridad y la interceptación", junto con el comercio de material electrónico, diseño y mantención de redes y sistemas de videovigilancia, y formación y capacitación asociada. Mercado Público registra una orden de compra de Gendarmería para "Mantenimiento, soporte y actualización del Servicio de Monitoreo EGO". En paralelo, la prensa especializada reportó que la Policía de Investigaciones adjudicó a Innova Chile el arriendo del sistema EGO como plataforma de interceptación, grabación y monitoreo (con detalles de capacidades técnicas y de implementación), reforzando su rol como canal local de provisión y soporte para tecnología de interceptación legal.

3.2. Demanda / Soluciones

3.2.1. *Spyware*

En julio de 2015, la mencionada filtración de emails de Hacking Team reveló que la Policía de Investigaciones (PDI) adquirió su *spyware* bajo el nombre de Phantom.[175] Hasta el día de hoy se desconocen los términos bajo los cuales esta tecnología fue utilizada, así como también las identidades de las personas infectadas que estuvieron bajo vigilancia con este *spyware*. Como en toda la región, tampoco existen análisis de muestras forenses de dispositivos específicos en Chile. En uno de los correos electrónicos filtrados, el jefe del Departamento de Monitoreo Telefónico (Demtel) señala que el propósito real del software era "utilizarlo como herramienta de apoyo para obtener datos de IP de los clientes y acceder a información que no podrían conseguir mediante una orden judicial".[176] Esta afirmación sobre sus objetivos de uso resulta contundente.

La figura central en los intercambios de correos electrónicos de Hacking Team fue Jorge Lorca Rivera, quien en ese momento operaba a través de Mipoltec, identificada como proveedora clave de este tipo de tecnología en Chile.[177] En los correos se hace evidente que Rivera también oficiaba como intermediario de otra empresa italiana, Innova SpA, más dedicada a soluciones para la inteligen-

---

175 "WikiLeaks - The Hackingteam Archives." 2015. URL

176 Partarrieu, Bárbara, y Matías Jara. "Los correos que alertaron sobre la compra del poderoso programa espía de la PDI." Actualidad. CIPER Chile, 11 de julio de 2015. URL

177 Pérez de Acha, Gisela. *Hacking Team: malware para la vigilancia en América Latina.* Derechos Digitales, 2016. URL

cia de redes.[178] Como vimos en el caso de Argentina, parece que fue una práctica habitual que estas dos empresas italianas presenten sus herramientas de manera conjunta.

El segundo *spyware* descubierto en Chile fue nada menos que Pegasus de NSO Group. Según el dataset utilizado por el CyberPeace Institute para su informe, en 2023 se documentaron tres casos de uso contra periodistas por parte de la Policía de Investigaciones de Chile.[179] Al año siguiente también se registró una nueva infección identificada a través del Mobile Surveillance Monitor.[180] Estos hallazgos se suman al historial previo de la institución con la empresa, ya que dos años antes habían surgido reportes sobre el uso de la herramienta Circles de NSO para explotar el protocolo SS7/Diameter.[181]

3.2.2. SIGINT

Las adquisiciones públicas registradas en Chile a partir del mencionado reporte al Parlamento alemán en 2014 confirman la presencia de equipamiento de Rohde & Schwarz, integrado por la firma local DYMEQ Ltda., destinado al control técnico del espectro radioeléctrico. Los contratos de la Subsecretaría de Telecomunicaciones (SUBTEL) y las fichas en Mercado Público incluyen estaciones de monitoreo y radiolocalización instaladas en dependencias de Santiago y La Reina. Se trata de herramientas diseñadas para la inspección y geolocalización de emisiones, utilizadas en tareas de radiomonitoreo, detección de interferencias y control del uso del espectro; en principio, sin capacidades intrusivas de interceptación legal (*Lawful Interception*), captura IMSI o explotación SS7/Diameter.[182]

Del mismo modo, en el caso de la empresa alemana de *Lawful Interception* Utimaco, las bases de licitación municipal refieren a su producto HSM Utimaco para equipos de encriptación y firma electrónica avanzada, lo que prueba la presencia de la marca, pero, en principio, no así de plataformas de interceptación.

---

178 Dentro de los correos de Hacking Team para el caso Chile, aparecen, además, mencionados Eduardo Pardo Carvajal, por su rol técnico-comercial dentro de Hacking Team, quien figura como "Field Application Engineer" para la región. También Sergio Rodríguez-Solís aparece en Chile como personal técnico del proveedor italiano Hacking Team. "WikiLeaks - The Hacking Team Archives." 2015. URL

179 Kreke, Aditi, Maira Cardillo, and Sina Fisher. *Targeting, Infecting, Surveilling, Harming. A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People.* CyberPeace Institute, 2023. URL

180 Monitor, Mobile Surveillance, 2025 Workbook, URL

181 Fossa, Lissette. "Prensa internacional revela espionaje con software Pegasus a dirigentes sociales, políticos y periodistas." *Interferencia*, 20 de julio de 2021. URL

182 La línea ARGUS de R & S pertenece a la categoría de sistemas de monitoreo de espectro empleados por organismos reguladores de telecomunicaciones en diversos países y forma parte de un marco técnico más amplio de vigilancia del aire radioeléctrico, distinto al espionaje de redes móviles o de Internet. Subsecretaría de Telecomunicaciones de Chile, *Resolución Exenta N° 470/2024*, Transparencia Activa (Santiago: SUBTEL, 2024). URL // URL

Según un informe de Privacy International, en el caso de Chile, los equipos *IMSI catcher* podrían haber sido provistos por la empresa estadounidense Almenta.[183] Si esto es así, Almenta comercializa la línea CAPTUR. Según sus folletos, mientras que CAPTUR C funciona como un IMSI/IMEI catcher con menos capacidades, CAPTUR A posee funcionalidades ampliadas. Se trata de una herramienta de interceptación activa que actúa como una antena falsa, pero que, además de capturar IMSI/IMEI, puede forzar conexiones y decodificar tráfico multi-banda para interceptar llamadas e incluso analizar tráfico de datos, por lo que funciona como un sistema activo con capacidades *man-in-the-middle*.[184].Los testimonios recopilados por medio de investigación periodística CIPER sobre los usos de los dispositivos utilizados parecen coincidir bastante bien con este equipo.[185]

Al mirar los resultados del mencionado proyecto de detección de antenas falsas para Santiago de Chile, con las mismas limitaciones metodológicas (a modo de recordatorio: las anomalías no equivalen a una prueba concluyente y se trata de un estudio restringido como muestra entre abril y noviembre de 2020), FADe documenta señales compatibles con operación de simuladores de celda. Para 2G consigna 21 casos y para 4G, 11 casos. De nuevo: las mediciones no se realizaron en momentos de conflicto social específico que podrían delatar la instalación de celdas falsas móviles.[186]

En relación a los equipos de geolocalización mediante explotación del protocolo SS7, como mencionamos, el laboratorio canadiense Citizen Lab publicó un informe en 2020 en el que señalaba que la Policía de Investigaciones de Chile (PDI) figuraba como cliente de la empresa Circles vinculada a NSO.[187] A pesar de que la Policía negó esta adquisición, queda claro que las agencias de seguridad cuentan con herramientas de este tipo. La plataforma Mobile Surveillance Monitor Network registró más de 37.000 eventos compatibles en redes de telecomunicaciones chilenas desde noviembre de 2022.[188]

En 2024, la empresa local DTS (Desarrollo de Tecnologías y Sistemas) anunció una alianza con la italiana ELT Group (una empresa *partner* de Cy4gate). Dentro de las "áreas de negocios" en las que se define DTS incluye "Guerra Electrónica" y el acuerdo mutuo habla de "mejorar la interoperabilidad de los sistemas de defensa, optimizar sus capacidades de detección y respuesta, y ofrecer apoyo técnico y operativo de alto nivel". El comunicado señala que ambas empresas

---

183 Privacy International, and Derechos Digitales. *State of Privacy Chile. Privacy International,* 2019. URL

184 Almenta Group, "CAPTUR — Tactical Interceptions," Almenta Group, archivada el 20 de agosto de 2016, URL

185 Peña, Cristóbal y Sebastián Minay, "Así se hacen los cuestionados 'pinchazos' telefónicos legales.". *CIPER Chile*, 29 de octubre de 2008. URL

186 South Lighthouse, *FADe (Fake Antenna Detection Project)*, "Santiago de Chile (2G)," accedido el 5 de noviembre de 2025, URL; "Santiago de Chile (4G)," accedido el 5 de noviembre de 2025, URL; "FAQs," accedido el 5 de noviembre de 2025, URL

187 Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert. *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles.* Citizen Lab Research Report n.º 133. University of Toronto, 2020. URL

188 Mobile Surveillance Monitor. "Mobile Surveillance Monitor: Research Workbook." URL

"agrupan sus conocimientos y experiencia" para ofrecer "soluciones innovadoras adaptadas a los mercados chileno y latinoamericano" en el sector de defensa electrónica.[189] Por su parte, ELT Group tiene capacidades para "Homeland Security & Law Enforcement", cuya descripción general parece ofrecer varios tipos de soluciones SIGINT.[190] Pero además, su empresa hermana Cy4gate SpA se define explícitamente como proveedora de "***Lawful Interception*** & Network Intelligence" para fuerzas de seguridad, ofreciendo herramientas de interceptación legal de redes móviles y fijas, *IMSI catchers* y OSINT.[191]. Por lo tanto, se puede estimar una probabilidad media-alta de que la alianza incluya también soluciones con capacidad de interceptación de comunicaciones móviles o de red. Como dice el anuncio, esa sociedad cooperativa podría habilitar que ELT ofrezca sus productos en países sudamericanos. Sobre todo, porque DTS se declara una "empresa chilena, creada en 1991, líder en la provisión de servicios y en el desarrollo de integración de tecnologías y sistemas para Defensa" con negocios probados con el Estado chileno y agencias de seguridad.[192]

3.2.3. Inteligencia de red

El artículo 222 del Código Procesal Penal obliga a las empresas telefónicas y de comunicaciones a mantener a disposición del Ministerio Público un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. Por una investigación del medio CIPER, sabemos que al menos desde el 2008 Chile cuenta con mecanismos de interceptación legal.[193]

Desde 2017, la organización Derechos Digitales evalúa de manera periódica la transparencia de los proveedores de Internet en Chile respecto al tratamiento de datos de usuarixs y a la forma en que responden a solicitudes de información gubernamental. El último informe realizado data de 2022. En general, constatan avances graduales en las políticas de privacidad y transparencia de las empre-

---

189 *ELT Group y DTS firmaron un acuerdo de cooperación en el sector de defensa electrónica en Chile y Sudamérica. - DTS® | Desarrollo de Tecnologías y Sistemas SpA*. Noticias DTS. 20 de diciembre de 2024. URL

190 *ELT Group*, "Company Profile". URL

191 ELT Group (antes Elettronica S.p.A.) mantiene una relación societaria estrecha con CY4GATE S.p.A., de la cual posee el 38,38 % del capital social y se declara como su accionista principal, lo que consolida a CY4GATE como parte del grupo especializado en ciberinteligencia e interceptación legal. En los materiales institucionales de ELT Group se afirma que CY4GATE "forma parte del Grupo ELT, especializada en ciberseguridad e inteligencia cibernética", y ambas empresas mantienen contratos de colaboración interna, incluido un acuerdo de I+D de más de 6,5 millones de euros en el que CY4GATE identifica a ELT Group como su accionista mayoritario. "Shareholding Structure and Share Capital," *CY4GATE S.p.A.*, consultado 22 de octubre de 2025. URL

192 Uno de ellos, de "industria de la defensa de Chile", indica que DTS "desarrolla, fabrica y soporta sistemas para las Fuerzas Armadas y de Orden en las áreas de Mando y Control, Guerra Electrónica y Comunicaciones". Zona Militar. "Industria de la Defensa de Chile - Empresas Autónomas del Estado, Filiales y Privados." 21 de enero de 2019. URL

193 Peña, Cristóbal y Sebastián Minay. "Así se hacen los cuestionados 'pinchazos' telefónicos legales." Investigación. *CIPER Chile,* 29 de octubre de 2008. URL

sas de telecomunicaciones chilenas (Claro, Entel, Movistar, VTR, WOM y GTD Manquehue), aunque ninguna cumple plenamente los estándares internacionales de protección de datos ni demuestra una defensa activa y sostenida de los derechos digitales de sus usuarixs. Destacan que aún en 2022 el marco normativo chileno sigue siendo insuficiente —en especial por la demora en actualizar la Ley 19.628 de Protección de Datos Personales—, lo que deja amplios márgenes de discrecionalidad tanto para las compañías como para las autoridades que solicitan información. Algunas empresas, como Claro y Movistar, mejoraron la calidad y estructura de sus informes de transparencia, incorporando más detalles sobre solicitudes de información y rechazos. Sin embargo, otras mantienen formatos ambiguos o parciales. La mayoría de las compañías no notifica a las personas afectadas cuando sus datos son requeridos por autoridades, salvo casos excepcionales. Esta ausencia de notificación sigue siendo una de las mayores debilidades detectadas.[194]

Mediante Tecnodata-Mipoltec, en 2014, Carabineros de Chile adquirió el sistema de interceptación de comunicaciones EGO, desarrollado por la empresa italiana Innova SpA. La adquisición se produjo en el mismo momento que la del *spyware* de Hacking Team. Sin embargo, debido a aparentes problemas vinculados con el diseño del contrato y el proceso de adquisición del distribuidor Mipoltec, el sistema nunca llegó a operar en ese momento.[195]

Quizás por las propias torpezas de esta empresa, la compañía italiana abrió una filial propia en Chile, lo que habla de una presencia comercial permanente. Innova Chile inició sus actividades en 2019 y funcionó también como nodo para ofrecer sus productos de interceptación a otros países de la región. En una licitación realizada en el año siguiente, Innova volvió a adjudicarse el contrato, esta vez compitiendo con otra empresa italiana, RCS Lab,[196] lo que permite suponer que el sistema está funcionando al menos desde el año posterior. En 2021 también *Infodefensa* reportó que la PDI adjudicó a "Innova Chile" un nuevo arriendo del sistema EGO, que vuelve a actualizarse como "Mantenimiento, soporte y actualización del Servicio de Monitoreo EGO" también para Gendarmería en el 2023.[197]

Según un antiguo folleto promocional de 2011, ya en este año EGO de Innova era un sistema avanzado de interceptación legal de comunicaciones (*Lawful Interception*), diseñado para capturar, decodificar, reconstruir y analizar todo tipo de comunicaciones IP —como videollamadas, mensajes MMS y correos electrónicos—, en cumplimiento con los estándares del ETSI (European Telecommunications Standards Institute) para interceptación legal. El sistema se despliega en puntos estratégicos de la red —como *switches, routers,* nodos de acceso o *gateways*— y recibe copias del tráfico seleccionado por sus operadores (por ejemplo, el tráfico asociado a un número telefónico o una dirección

---

194 Michelle Bordachar, *¿Quién defiende tus datos?*, Santiago, Derechos Digitales - EFF, 2022. URL

195 Miranda, Ida, y Bárbara Partarrieu. "Carabineros pagó US$3,3 millones por equipo para 'pinchar' teléfonos: lo instaló y no funcionó." Investigación. *CIPER Chile*, 12 de febrero de 2015. URL

196 García, Nicolás. "Innova arrendará a la PDI de Chile el sistema de interceptación y monitoreo telefónico Ego." *Infodefensa - Noticias de defensa, industria, seguridad, armamento, ejércitos y tecnología de la defensa*, 26 de enero de 2020. URL

197 Orden de compra N°634-748-SE23 "Mantenimiento soporte actualización Monitoreo EGO", URL

IP específica). Funciona como un analizador de paquetes con capacidades extendidas: puede reconstruir sesiones completas de comunicación (en lugar de mostrar solo paquetes individuales), clasificar automáticamente los datos —como llamadas entrantes y salientes, ubicaciones o correos enviados— y proporcionar análisis interpretativos. El sistema incorpora algoritmos propietarios que firman digitalmente la información adquirida, garantizando su integridad y preservación mediante soluciones combinadas de software, hardware y arquitectura. Finalmente, el folleto destaca que EGO permite análisis avanzados de datos, localización y seguimiento de objetivos, gestión de directorios que muestran relaciones entre interlocutores y herramientas optimizadas de investigación para operadores de fuerzas de seguridad.[198]

En 2018, el Ministerio Público adquirió una versión denominada *Vigía Elite* o *Vigía Elite Advanced*, con un costo aproximado de un millón de dólares, con el objetivo de modernizar sus capacidades de interceptación.[199] Sin embargo, la implementación del sistema fue fallida, nunca llegó a operar plenamente y derivó en una investigación por irregularidades y fraude.[200] El software Vigía es una plataforma de interceptación, análisis y geolocalización de comunicaciones adquirida en Chile por la Policía de Investigaciones (PDI) y el Ministerio Público (MP) para labores de investigación criminal.[201] Su desarrollo y provisión corresponden a la empresa Cognyte —anteriormente parte del conglomerado israelí-estadounidense Verint Systems—, especializada en soluciones de vigilancia y análisis de datos.[202] De acuerdo con diversas fuentes, el sistema permite capturar llamadas telefónicas y mensajes SMS y MMS, así como el tráfico de datos asociado a un número interceptado y geolocalizar dispositivos mediante el uso de información proveniente de antenas de telefonía móvil.[203] Asimismo, registra y organiza metadatos como hora, ubicación y participantes de las comunicaciones.[204]

---

198 "Innova_Product List, Specifications_MicroIP, EGO, Internet Interception and Probes, Gps Innova, RB800", 2011. URL

199 *La Tercera Sábado,* "Vigía Elite: El software del millón de dólares que complica a la Fiscalía," 2023, URL

200 *BioBioChile,* "La trama del Vigía: Cómo la Fiscalía tiró 1 000 millones a la basura en el proyecto estrella de Abbott," 3 de julio de 2025. URL

201 *Interferencia,* "Vigía: El software con que la PDI trató de situar a Llaitul en atentados durante dos años," 2022. URL

202 Vigía es el nombre en código local de alguno de los productos de Cognyte de interceptación legal. Cognyte Software Ltd., *"Cognyte Software Ltd."* (Oslo: The Council on Ethics for the Norwegian Government Pension Fund Global, diciembre de 2022). URL

203 Verint reconoce sus productos RELIANT / VANTAGE como líneas de interceptación. En un documento corporativo, Verint describe sus líneas RELIANT y VANTAGE como suites de "intelligent recording and analysis solutions for communications interception activities for law enforcement" (soluciones inteligentes de grabación y análisis para actividades de interceptación de comunicaciones) que se ofrecen a agencias de seguridad. URL También en la enciclopedia de información corporativa se menciona que Reliant y Vantage son vendidos a cuerpos policiales y agencias gubernamentales, también en Sudamérica. URL

204 Fiscalía de Chile, "Fiscalía se capacita en software que analiza información derivada de interceptaciones telefónicas," 2020, URL

Por el problema señalado en relación a los usos del sistema de interceptación legal, este caso resulta particularmente relevante, ya que evidencia un uso concreto de equipamientos instalados de manera legal, pero con prácticas excesivas derivadas de su propia configuración y de las posibilidades técnicas que ofrece. Aunque probablemente la instalación del sistema haya requerido la colaboración del proveedor de internet bajo los procesos esperables, la investigación de Nicolás Sepúlveda recoge testimonios que certifican su uso discrecional.[205]

Además, productos comercializados por la firma estadounidense Pat Systems —en particular la suite Vortex AIT-Stack— integran tanto *IMSI catchers* como un sistema de interceptación de comunicaciones a través de la red IP. Este último, el sistema de monitoreo judicial de Pat Systems, es una plataforma de interceptación que se conecta directamente con las redes de telecomunicaciones para capturar tanto metadatos como contenido de las comunicaciones, conforme a los estándares ETSI y CALEA.[206]

Para cerrar esta sección, vale la pena mencionar dos casos de probable adquisición e implementación no corroborados.

Al parecer, RCS Lab, otra empresa italiana que en su momento actuaba como revendedora de Hacking Team, también intervino como intermediaria. Esta empresa, especializada en tecnologías de interceptación legal de comunicaciones y análisis forense digital, ha sido señalada en informes internacionales por mantener vínculos o actividades comerciales en Chile, aunque no existen evidencias públicas de implementaciones operativas confirmadas en el país.[207] Su portafolio incluye plataformas de *lawful interception*, monitoreo de redes móviles y fijas, y soluciones de extracción de datos desde dispositivos electrónicos, comercializadas para agencias de seguridad y operadores de telecomunicaciones. Su presencia en Chile debe considerarse posible pero no comprobada, limitada —según la información disponible— a contactos y negociaciones comerciales.[208]

Por último, aunque tampoco existan registros públicos que confirmen la implementación en Chile de sistemas de interceptación o vigilancia desarrollados por SearchInform Ltd., la empresa rusa sí mantiene presencia comercial en el país a través de su socio local Techlaw, con sede en Santiago. Su oferta se centra en soluciones corporativas de Data Loss Prevention (DLP), monitoreo de usuarixs internos y gestión de riesgos informáticos, más que en plataformas de intercep-

---

205 La investigación de Nicolás Sepúlveda sostiene que Carabineros habría tenido acceso a Vigía, una plataforma usada para organizar y analizar información vinculada a interceptaciones y registros de comunicaciones (como números, llamadas entrantes y salientes, duración y, en algunos casos, datos asociados a antenas). Aunque el acceso a este tipo de información tiene una vía legal y regulada, en el caso investigado ese acceso no habría contado con la autorización correspondiente y habría circulado por canales informales. "Miembros de Inteligencia reconocieron a CIPER que esas escuchas muchas veces eran ilegales." Sepúlveda, Nicolás. "'Operación Huracán': la secreta casa donde se hacían centenares de escuchas telefónicas ilegales." Investigación. *CIPER Chile*, 5 de abril de 2018. URL

206 Surveillance Watch, "PAT Systems" Accedido el 12 de diciembre de 2025, 2025. URL

207 Feldstein, Steven, and Brian Kot. *Global Inventory of Commercial Spyware & Digital Forensics*. 2023. DOI

208 Lookout Threat Intelligence, *"Hermit Spyware Discovery,"* Lookout Inc., 2022, URL

tación de comunicaciones. En consecuencia, la posibilidad de que SearchInform haya desplegado en Chile tecnologías de vigilancia estatal SORM parece remota, aunque la existencia de contactos comerciales y representación local sugiere al menos un vínculo potencial con el mercado de la seguridad y análisis de datos ruso.[209]

3.2.4. Monitoreo de red

En el ámbito de los operadores de telecomunicaciones, al menos desde 2008 la canadiense Sandvine reportó contratos con proveedores de servicios de Internet (ISP) en Brasil, Chile y Colombia para su plataforma Policy Traffic Switch, orientada a Deep Packet Inspection (DPI), gestión de congestión y analítica de aplicaciones a escala de *backbone*.[210]

VTR Chile SA, una de las principales compañías de Internet y televisión por cable, introdujo desde mediados de la década de 2000 una infraestructura de nueva generación (IP NGN) con equipos Cisco CRS-1 en el núcleo de su red. Esa arquitectura de nivel operador permite medir, analizar y administrar el tráfico mediante sistemas de control que regulan el uso de la red y mejoran la calidad del servicio.[211]

Más recientemente, en 2022, la firma VAS Experts informó que un gran proveedor de internet chileno había incorporado su sistema de traducción masiva de direcciones IP (CGNAT). Este tipo de software permite que muchos clientes compartan una misma dirección pública y, al mismo tiempo, registra cómo circula el tráfico por la red, ofreciendo a la empresa una visión detallada del uso y del rendimiento de sus conexiones.[212]

Por su parte, Entel —uno de los mayores proveedores del país— estandarizó su portafolio en torno a Palo Alto Networks, integrando firewalls de nueva generación (NGFW), detección de intrusiones (IDS/IPS) y coordinación en su Network Operations Center / Security Operations Center (NOC/SOC) corporativo. Aunque diseñadas como soluciones de seguridad, estas herramientas también aportan monitoreo continuo de tráfico y constituyen el núcleo técnico de la observabilidad y el control de red en los proveedores chilenos de gran escala.[213]

Como mencionamos, el despliegue de tecnologías de monitoreo y gestión de red por parte de los ISP chilenos —como inspección profunda de paquetes (DPI), control de políticas de filtrado, traducción masiva de direcciones (CGNAT) y firewalls de nueva generación (NGFW) integrados en la operación de los operado-

---

209 SearchInform, "Partners – Latin America," consultado 23 de octubre de 2025, URL // International Coalition Against Illicit Economies (ICAIE), "How Russian Surveillance Tech Is Reshaping Latin America," 12 de septiembre de 2024, URL

210 Light Reading, "Sandvine Touts LatAm Success," 2008. URL

211 Cisco Newsroom, "Chile's VTR First in Latin America to Deploy IP NGN with Cisco CRS-1," 17 de julio de 2006

212 VAS Experts, "CG-NAT Solution for Saving IPv4 Address Space — A Case Study," 6 de abril de 2022.

213 Palo Alto Networks, "Modern Managed Cybersecurity Services in Chile: Entel Case Study," 2024; *ANDA Chile*, "Palo Alto Networks eleva a Entel Ocean a su máxima categoría de partner," 8 de noviembre de 2022.

res— se justifica por necesidades de gestión de tráfico, eficiencia del espectro IP y seguridad de red; al mismo tiempo, estos sistemas también habilitan una observabilidad granular del comportamiento de lxs usuarixs. Esa capacidad, que permite distinguir aplicaciones, priorizar flujos o identificar patrones de consumo, es la misma que podría emplearse —sin controles adecuados— para prácticas de vigilancia comercial o estatal. Por esto, abre importantes preguntas respecto a la privacidad y la transparencia.

Por ejemplo, en Chile la Ley 20.453 consagra el principio de neutralidad en la red para usuarios de Internet: los proveedores no pueden "bloquear, interferir, discriminar, entorpecer ni restringir arbitrariamente" el uso legal de contenidos, servicios o aplicaciones. Esto establece un marco regulatorio destinado a proteger el acceso igualitario y la privacidad de los usuarios frente a decisiones arbitrarias de los proveedores.[214] Sin embargo, la normativa —tal como está redactada y aplicada hasta ahora— no impone una obligación pública general que exija a los proveedores de servicios de Internet (ISP) revelar con detalle técnico qué mecanismos de gestión emplean, cómo configuran eventuales sistemas de inspección o priorización de tráfico , qué tipos de metadatos retienen, ni por cuánto tiempo conservan registros de tráfico. Esa carencia normativa deja una zona de opacidad respecto de las prácticas reales de gestión de redes. De ese modo, aunque la neutralidad de red establece límites —prohibiendo bloqueos y discriminación arbitraria—, existen riesgos estructurales de que las tecnologías de gestión de tráfico, concebidas para el mantenimiento de la calidad, puedan ser usadas de forma extensiva o indebida para monitoreo, priorización o filtrado, sin que las y los usuarios tengan medios confiables de saberlo. Ese vacío regulatorio y de supervisión legítima la preocupación sobre posibles violaciones de derechos de privacidad, libertad de comunicación y transparencia en el ecosistema de telecomunicaciones.[215]

Asimismo, los controles institucionales son todavía débiles. Aunque la ley de protección de datos personales en Chile brinda derechos a lxs usuarixs (Ley 19.628), no existe todavía —o al menos no de manera plenamente operativa— una autoridad especializada con facultades de supervisión y sanción fuertes respecto del tratamiento de datos por ISP. Esto implica que incluso cuando se adquirieron herramientas corporativas de monitoreo de red, no siempre hay evidencia pública de auditorías independientes, informes de transparencia de los operadores o mecanismos de queja de lxs usuarixs sobre el uso que se les da estos sistemas.

---

214 Ley 20.453, "Consagra el principio de neutralidad en la red para los consumidores y usuarios de Internet", modificatoria de la Ley General de Telecomunicaciones, artículos 24 H, 24 I y 24 J. Ver: Biblioteca del Congreso Nacional de Chile, texto de la ley. URL

215 Veridiana Alimonti, *Who Defends Your Data in Latin America & Spain? A Comparative View of Telecom Companies' Commitments to User Privacy* (San Francisco: EFF, marzo de 2023), URL

3.2.5. OSINT

Una investigación realizada por el diario *Haaretz* reveló que la empresa israelí Cognyte vendió al Ejército de Chile equipos activos de inteligencia de fuentes abiertas OSINT. Además, Cognyte fue mencionada en el informe de Meta sobre la industria de la vigilancia publicado en diciembre de 2021 por su uso de avatares falsos como parte de su fase OSINT activa, ofensiva y dirigida (targetizada). Según la compañía, estos avatares habrían sido utilizados para vigilar y recopilar información sobre periodistas en diversos países, entre ellos Chile. La investigación sugiere que el sistema funciona mediante la creación de perfiles que recogen datos en redes sociales asociados a un número telefónico. Una vez obtenida, esta información puede ser empleada para diseñar estrategias de *phishing* de precisión. Por lo tanto, no se trataría de una recolección pasiva de OSINT, sino de una operación activa de obtención de datos.[216]

En 2024, la Policía de Investigaciones de Chile (PDI) adjudicó la "Adquisición de software tipo OSINT con búsqueda a través de imágenes" a la empresa Servicios Profesionales UP SpA, por un monto cercano a 252 millones de pesos chilenos (unos 267 mil dólares). El contrato corresponde a la adquisición de licencias equivalentes a Clearview AI y tiene como propósito fortalecer las capacidades operativas de la institución en búsqueda inversa y reconocimiento facial mediante análisis de fuentes abiertas. Esta compra representa una de las primeras evidencias documentadas de adopción explícita de tecnologías OSINT por parte de una fuerza de seguridad chilena orientada a labores de investigación criminal y ciberinteligencia.[217]

Por su parte, cabe destacar que, según consigna el diario *La Tercera*, Carabineros cuenta con OS-9, un equipo especializado en "*ciberpatrullajes*" para detectar amenazas en las redes sociales." La vocera del OS-9, la teniente Javiera García, explicó que este equipo "constantemente mantiene monitoreos o patrullajes virtuales revisando muchas redes sociales. Cuando hay algún comentario que indica directamente la intención de agredir gravemente a una persona, como, por ejemplo, un *te voy a matar*, se enciende la alerta que la configura como una amenaza a considerar y a investigar junto al Ministerio Público". Además, a través de las interacciones en redes sociales, Carabineros determina con quiénes se comunica y se relaciona la persona que está siendo investigada. Esta información es analizada a la luz de otros datos, como los antecedentes penales de las personas que se comunican con la persona que está siendo monitoreada, y en base a eso se decide (o no) incluirlas en la investigación. Además de perfiles personales, desde el OS-9 explican que también monitorean agrupaciones o colectivos, como es el caso de barras de fútbol, colectivos "anarquistas" o agrupaciones feministas.[218]

De manera más reciente, en registros oficiales de audiencias de la Plataforma Ley del Lobby, la empresa chilena SAT Internacional presentó Tucán, de la compañía israelí Prelysis como una plataforma OSINT que centraliza en un solo entorno el

---

216 Benjakob, Omer, and Phineas Rueckert. "Fake Friends: Leak Reveals Israeli Firms Turning Social Media into Spy Tech." National Security & Cyber. *Haaretz*, 28 de febrero de 2023. URL

217 "Adquisición de software tipo OSINT con búsqueda a través de imágenes (5890-36-LQ24)," *todolicitaciones*.cl, consultado el 30 de octubre de 2025, URL

218 Rivera, Victor. "El desconocido 'ciberpatrullaje' de Carabineros en las redes sociales". *La Tercera* (Santiago de Chile), 28 de agosto de 2018. URL

monitoreo de redes sociales y mensajería instantánea, y que se promociona con capacidades de "desanonimizar" usuarios y mensajes (mencionando, entre otras, Telegram, Threema, WhatsApp, Zalo e Imo), además de módulos de detección de huella digital, análisis de imágenes con IA y reconocimiento facial, monitoreo de foros y *darknet*, análisis de enlaces y operaciones de big data. En una audiencia adicional se incorpora explícitamente la función de búsquedas específicas en "data leaks".[219]

También la empresa chilena Black up Spa ofrece en el país Babel Street, una plataforma de inteligencia de riesgos para entidades estatales y privadas que combina recolección y análisis de información digital para detección de amenazas, evaluación de riesgos e identificación y resolución de identidades. Su suite incluye capacidades tipo OSINT/SOCMINT, con analítica de textos, además de módulos para mapeo de entidades y relaciones y herramientas de investigación.[220]

Por fuera del sector de inteligencia, seguridad y defensa, también se han adoptado capacidades de monitoreo abierto. El Servicio Electoral (SERVEL) licitó una plataforma de administración y monitoreo de redes sociales destinada a mejorar la percepción ciudadana sobre su gestión y fortalecer la comunicación institucional. Según su propio portal, el organismo utiliza software de inteligencia del consumidor y análisis de redes sociales para recolectar y sistematizar información pública, orientada a detectar desinformación electoral.[221] También la Comisión para el Mercado Financiero (CMF) licitó el monitoreo de redes sociales, sitios web y medios online y, en un proceso separado pidió servicios especializados de ciberseguridad que incluyen cibervigilancia, ciberinteligencia y *threat hunting*. Esto sugiere un enfoque de gestión de riesgos y respuesta a incidentes con insumos de inteligencia de amenazas. En este caso, el objetivo de la CMF es emplear herramientas de *social listening* basadas en inteligencia artificial y procesamiento de lenguaje natural para monitorear conversaciones públicas en redes sociales y medios digitales, con el fin de identificar tendencias, percepciones y eventuales riesgos comunicacionales que puedan afectar al sistema financiero o a la propia institución.[222]

---

219 Plataforma Ley del Lobby (Chile), Armada de Chile, "Audiencias - Año 2024 - Marco Villegas Zanón," Identificador AD007AW1685110 (22 de octubre de 2024), URL / Plataforma Ley del Lobby (Chile), Fuerza Aérea de Chile, "Audiencias - Año 2025 - César Pineda," Identificador AD008AW1742130 (12 de marzo de 2025), URL / Buitrago, Leonardo. "Empresa israelí ofreció 'Tucán' a Armada y FACh: actas consignan promesa de 'eliminar el anonimato' en WhatsApp y Telegram." *El Ciudadano*, 27 de agosto de 2025. URL

220 Babel Street, "Text Analytics and Identity Intelligence Solutions (Modules)", en URL

221 Servicio Electoral de Chile, "Servicio de plataforma de administración y monitoreo de redes sociales del Servicio Electoral," ficha de licitación (Santiago, 2025), ID 5155-14-LE25. URL

222 Comisión para el Mercado Financiero (CMF), "Servicio de monitoreo de redes sociales, sitios web y medios online," ficha de licitación (Santiago, 2023/2025). URL // CMF, "Contratación de herramientas y servicios especializados de ciberseguridad (incluye monitoreo de ciberseguridad, threat hunting, cibervigilancia y ciberinteligencia)," ficha de licitación ID 1005498-21-LR25 (Santiago, 2025). URL

Tabla 3: Resumen Chile

CHILE				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Spyware	**Hacking Team (Italia)**	Tecnodata - Mipoltec / RCS Lab	Remote Control System (Phantom / Galileo)	Confirmada en las filtraciones de 2015.
	NSO Group (Israel)		Pegasus	Documentado en la base de datos del CyberPeace Institute (supuesto uso).
SIGINT	**Almenta Group (EE. UU.)**		Dominator - Captur (*IMSI catcher*) / Observer (SS7-Diameter Signaling Interception)	Probable
	NSO / Circles (Israel)		Explotación SS7/ Diameter	Confirmada
	ELT Group / Cy4gate (Italia)	DTS	*IMSI catcher*	Probabilidad media-alta
	RCS Lab (Italia)		*IMSI catcher* / Explotación SS7	Poco probable
	Pat Systems (EE. UU.)		*IMSI catchers* / Explotación SS7	Muy probable
	Rohde & Schwarz (Alemania)	DYMEQ Ltda.	*IMSI catcher* / *Direction Finder*	Probable

CHILE				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Inteligencia de red / *Lawful interception*	**Innova S.p.A. (Italia)**	Mipoltec / Innova Chile	EGO	Confirmada
	Verint / Cognyte (Israel)	Grupo Zeuz / RightCom	Vigía	Muy probable. Adquisición documentada (implementación cuestionada o parcialmente fallida).
	Pat Systems (EE.UU)		Interceptación de red IP	Muy probable
	ELT group / Cy4gate (Italia)	DTS	Cy4gate LI	Probabilidad media alta
Monitoreo de red	**Blue Coat (EE. UU.)**		PacketShaper	Confirmada
	Sandvine / Procera (Canadá)		Policy Traffic Switch, PacketLogic	Confirmada
	CISCO (EE.UU.)		Arquitectura IP NGN	Confirmada
	Allot (Israel)	ENTEL	ContentSecure, MailSecure, WebFilter, Service Gateway, Deep Packet Inspection (DPI)	Confirmada. Aparece en el Annual Report 2014 de Allot Communications.
	VAS Experts (Países Bajos)		Stingray Service Gateway (solución DPI avanzada)	Confirmada. En 2022 afirmó tener “instalaciones” en Chile.
	Palo Alto Networks (EE. UU.)		NGFW / Orquestación SOC	Confirmada

CHILE				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
OSINT	**Prelysis (Israel)**	SAT Internacional S.A	Tucán	Muy probable
	Verint / Cognyte (Israel)	Grupo Zeuz / RightCom	Active OSINT surveillance / Analítica / fusión de datos para investigación	Confirmada
	ELT group / Cy4gate (Italia)	DTS	Cy4gate OSINT	Probable
	BabelStreet (EE. UU.)	Black-up SpA	Inteligencia de riesgos / SOCMINT	Muy probable
	IBM (EE. UU.)	Xmartlab	IBM i2 Analyst's Notebook y también de i2 iBridge	Confirmada
	Clearview	Black-up SpA / Servicios Profesionales UP SpA	Reconocimiento facial OSINT	Confirmada

CHILE				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Extracción y análisis forense	**Cellebrite (Israel)**	IAFIS group (IAFIS Chile) / Black-up SpA	UFED	Confirmada
	Toka Group (México)		Extracción forense	Probable
	Oxygen (EE. UU.)	Xmartlab / Digitoforense SpA.	Oxygen Forensic Rugged Kit	Confirmada
	MSAB (Suecia)	Digitoforense SpA.	Extracción de dispositivos	Confirmada

CHILE				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Videovigilancia / Biometría / Reconocimiento facial	**Clearview AI (EE. UU.)**	Black-up SpA / Servicios Profesionales UP SpA	Reconocimiento facial	Confirmada
	Verint / Cognyte / Intellicene (Israel)	Grupo Zeuz y RightCom	Reconocimiento facial / "FaceDetect" / Nextiva Video management / VMS (CCTV IP)	Confirmada
	NEC (Japón)	NEC Chile S.A.	Biometría facial	Confirmada
	Dahua Technology (China)	SSTT SpA (Chile) / Dahua Technology Chile SpA		Confirmada
	Luxriot / VisionLabs (Rusia)	Rustec (Chile)		Confirmada
	AnyVision / Oosto (Israel)		Better Tomorrow	Confirmada
	Hikvision (China)			Confirmada
	Huawei / ZTE (China)		Infraestructura de videovigilancia	Confirmada
	Veridas (España)		Identidad digital	Confirmada
	Jumio (EE. UU.)		Verificación de identidad	Confirmada
	IDEMIA / Morpho (Francia)		Sistemas de identificación	Confirmada

4. Uruguay
4.1. Contexto

Al pasar a Uruguay puede pensarse en un escenario menos conflictivo que el de Argentina y Chile, fuera de los grandes escándalos de compras a proveedores internacionales, con gobiernos menos proclives a la espectacularización de la seguridad y más instancias participativas de la sociedad civil en la definición de políticas públicas. En términos de protesta social, el panorama también luce más tenue. Se trata, además, de un país con menos de tres millones y medio de habitantes, frente a los casi veinte millones de Chile y los cuarenta y cinco millones de Argentina, lo que obliga a ajustar las escalas. Sin embargo, aunque las dimensiones y el origen del paquete tecnológico incorporado difieran de manera considerable, las prácticas concretas no distan tanto de las del vecindario.

Uruguay llega, además, a la discusión contemporánea sobre vigilancia con instituciones relativamente sólidas y protección constitucional de la privacidad y la libertad de expresión, apuntaladas por la Ley 18.331 de Protección de Datos Personales y la Ley 18.381 de Acceso a la Información Pública.[223] A partir de 2016, no obstante, diversos análisis ya advertían que, aunque ese andamiaje habilita controles y transparencia, su funcionamiento real resultaba desigual y opaco. Un primer reporte realizado ese año subraya que no existe obligación legal de retención masiva de datos, pero que algunas operadoras los conservan voluntariamente sin reglas de notificación a usuarixs.[224]

El nuevo Código del Proceso Penal (Ley 19.293) y, sobre todo, la Ley 19.696, que regula el Sistema Nacional de Inteligencia de Estado, redefinieron el ecosistema institucional.[225] Lecturas críticas —como las de Datysoc— señalan que la definición de "inteligencia policial" y las fronteras entre prevención, instrucción penal e inteligencia difuminan límites y favorecen el trasvasamiento de técnicas de vigilancia hacia ámbitos donde deberían exigirse mayores garantías. También advierten que la ley no distingue con claridad entre "fuentes abiertas" y el análisis de redes sociales (SOCMINT), con implicancias para las expectativas de privacidad.

Cabe seguir los diagnósticos de Datysoc, la organización civil pionera en estos temas dentro del país. Desde 2020 gana peso el mal llamado ***"ciberpatrullaje"*** —monitoreo preventivo de espacios digitales— como práctica policial. En su reporte, documenta que no hay regulación específica ni protocolos públicos para OSINT/SOCMINT; que la Fiscalía reconoce usos puntuales (incluso la

---

223 República Oriental del Uruguay, *Ley Nº 18.331, Protección de Datos Personales y Acción de Habeas Data* (publicada D.O. 18 de agosto de 2008), IMPO. URL // República Oriental del Uruguay, *Ley Nº 18.381, Derecho de Acceso a la Información Pública* (publicada D.O. 7 de noviembre de 2008), IMPO/URCDP. URL

224 Scrollini, Fabrizio, Ana Tuduri y Katitza Rodríguez. *Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay (2016)*. EFF, 2016. URL

225 República Oriental del Uruguay, *Ley Nº 19.293, Código del Proceso Penal* (promulgación 2014), IMPO. // República Oriental del Uruguay, *Ley Nº 19.696, Aprobación y regulación del Sistema Nacional de Inteligencia de Estado* (promulgación 29 de octubre de 2018), IMPO/SIEE. URL

posible creación de perfiles encubiertos); y que faltan reglas sobre necesidad, proporcionalidad, cadena de custodia y rendición de cuentas a nivel judicial.[226]

La opacidad agrava el cuadro. El Ministerio del Interior ha sido objetado por negar o demorar información amparada por la Ley 18.381. La Unidad de Acceso a la Información Pública (UAIP) dictó resoluciones recientes reconociendo incumplimientos de plazos por parte de este Ministerio; y Datysoc obtuvo, por sentencia, datos sobre *ciberpatrullaje* que el Ministerio había reservado.[227] Incluso cuando la propia Memoria 2020 del Ministerio admite la incorporación de un software de análisis de redes (UCINET) para el Observatorio Nacional sobre Violencia y Criminalidad, la cartera declaró "reservados" los fines y protocolos de uso.[228] En paralelo, este Ministerio avanzó en una reorganización de su área de datos: en julio de 2025 presentó el Área de Estadística y Criminología Aplicada (AECA) y su Consejo Asesor, con la promesa de profesionalizar la producción y el uso de evidencia en seguridad pública.[229] El resultado: fue imposible determinar de forma cierta el alcance del ***ciberpatrullaje*** o qué herramientas se emplean.

El Ministerio del Interior se destaca entre los organismos con mayores niveles de incumplimiento de la Ley de Acceso a la Información Pública. Registra uno de los puntajes más bajos en el ranking de transparencia de Uruguay y recibe la mayor cantidad de demandas de la sociedad civil en esta materia. Dos ejemplos recientes de estas acciones judiciales se dieron a raíz de la negativa a responder sobre el registro de distintos procedimientos policiales, así como de la negativa a brindar información sobre el software de reconocimiento facial adquirido. Del mismo modo, la implementación del sistema de reconocimiento facial para uso policial ya está en marcha, aunque no existen normativas específicas ni protocolos públicos que otorguen garantías para su utilización.

Los hitos resultan así, en comparación, de menor escala mediática, pero no triviales: adopción de leyes de datos y acceso, incorporación y operación de un sistema de interceptación con funcionalidades OSINT, reordenamientos legales del proceso penal, expansión de prácticas de ***ciberpatrullaje*** sin reglas específicas y creación de unidades internas de análisis.

Con todo, la tradición participativa, junto con una oscilación política menos radical que la de sus vecinos, abre iniciativas que funcionan como salvoconducto. En el marco del Sexto Plan de Gobierno Abierto 2025–2029, el Ministerio del Interior convocó a organismos de la sociedad civil para avanzar en la creación de un "Espacio de diálogo multisectorial sobre regulación de tecnologías de vigilancia policial y prueba digital". Se trata de un compromiso en elaboración cuyo objetivo es establecer reglas claras, criterios de necesidad y proporcionalidad, y mecanismos de control democrático sobre OSINT/SOCMINT, reconocimiento

---

226 Díaz Charquero, Patricia, y Jorge Gemetto. *Ciberpatrullaje: Los límites borrosos de la vigilancia policial en Uruguay*. Montevideo, Datysoc, 2022. URL

227 Díaz Charquero, Patricia, y Jorge Gemetto. *Ciberpatrullaje: Los límites borrosos de la vigilancia policial en Uruguay*. Montevideo, Datysoc, 2022. URL // Unidad de Acceso a la Información Pública (UAIP), Resolución 2521/2025. URL

228 Ministerio del Interior, *Memoria 2020* (citado por Datysoc): incorporación de UCINET para el Observatorio; declaración de "reserva" sobre fines/protocolos.

229 Ministerio del Interior, "Ministerio del Interior presenta el Área de Estadística y Criminología Aplicada (AECA)", 1 de julio de 2025. URL // Presidencia – Uruguay, "Ministerio del Interior diseñará política pública en seguridad basada en evidencia" , 1 de julio de 2025. URL

facial e interceptación de comunicaciones. El compromiso —en estado de borrador al 4 de noviembre de 2025— formaliza una mesa de trabajo multiactor para producir lineamientos y protocolos públicos.

BOX 13: Algunas empresas a tener en cuenta

- **Teleimpresores S.A.** (Uruguay) es una empresa uruguaya de tecnología y seguridad que ofrece desde cámaras de seguridad, alarmas, control de acceso y telefonía hasta planificaciones de sistemas de seguridad.. Al menos entre 2010 y 2011 también vendió equipos de interceptación telefónica adquiridos desde el Portal de Compras Estatales. También en las primeras compras operó como intermediaria para la adquisición del sistema brasileño Intellotum - El Guardián.
- **Aeromarine S.A.** Figura en la normativa oficial (URSEC) como representante exclusivo en Uruguay de equipos Rohde & Schwarz, marca que cubre instrumentación y soluciones de radiomonitoring y radiolocalización.

4.2. Demanda / Soluciones

4.2.1. *Spyware*

Como en el resto de los países de la región, en mayo de 2014, ejecutivos de la firma italiana Hacking Team —Alex Velazco y Sergio Solis— viajaron a Montevideo para presentar su Remote Control System (RCS) —también conocido, según el caso, como *Da Vinci, Galileo, Phantom,* etc.— ante autoridades de seguridad uruguayas. Según los correos internos filtrados en 2015, mantuvieron reuniones separadas con el entonces director nacional de Policía, Julio Guarteche, y con el coordinador de Inteligencia del Estado, Ramón Bonilla.[230] Los reportes de los propios ejecutivos consignan demostraciones con "dispositivos infectados", una recepción "muy bien impresionada" y la promesa de interlocutores locales de "presionar" políticamente para su adquisición. El RCS es descrito en esos documentos como capaz de infectar sigilosamente equipos objetivo, extraer contenidos y activar micrófono y cámara.[231]

En paralelo, un informe de 2016 preparado para la Electronic Frontier Foundation documentó que el intermediario provenía de Paraguay y resaltó la ausencia de reglas específicas para herramientas de infección de dispositivos, un vacío que dificulta evaluar legalidad, necesidad y proporcionalidad frente a estándares internacionales.[232]

---

230 "WikiLeaks - The Hacking Team Archives." 2015. URL // Solis, Sergio, "Paraguay-Uruguay Report". 8 de julio de 2015. Wikileaks. URL

231 Gonzalo Terra, "Gobierno de Mujica sondeó compra de más equipos de espionaje", *El País* (Montevideo), 10 de julio de 2015, URL

232 Fabrizio Scrollini, Ana Tudurí y Katitza Rodríguez, *Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Uruguay,* Electronic Frontier Foundation, 2016, URL

Tras la filtración, el entonces ministro del Interior, Eduardo Bonomi, confirmó que la cartera había analizado el *spyware* Galileo, pero que lo descartó por "invasivo". En la misma intervención defendió la plataforma de interceptación recién adquirida de inteligencia de red, "El Guardián", como una herramienta de vigilancia "con garantías", diferenciándola del uso de malware intrusivo. La línea oficial añadió que, luego de la presentación de Hacking Team, no se activó ninguna negociación por Galileo.[233]

Años más tarde, el semanario *Búsqueda* informó que el Ministerio del Interior recibió una propuesta para obtener Pegasus de NSO Group, entre otras ofertas internacionales orientadas a "reemplazar" o "mejorar" capacidades existentes.[234].La nota precisó que, a esa fecha, no había una decisión tomada y que la evaluación continuaba. Poco después, la Unidad Reguladora y de Control de Datos Personales (URCDP) publicó la Resolución Nº 30/021 (12 de agosto de 2021) sobre un pedido de acceso a información que solicitaba documentos donde se mencionara a NSO Group, Pegasus y la posible adquisición de *spyware*. En su respuesta sólo remitió que no poseía esa información.[235] En términos de trazabilidad pública, esto constituye un indicio de negociación y evaluación de *spyware* mercenario de grado estatal, sin evidencia abierta de compra o despliegue efectivo.[236] Cabe destacar que el actual encargado de ventas de NSO Group, Martin Berenstein, es de nacionalidad uruguaya y es quien ofrece pruebas y demostraciones en los países de la región. Sobre esto, sólo queda mencionar la existencia de un interés declarado de algunos funcionarios de seguridad en los últimos años, que llaman la atención sobre la necesidad de adquirir este tipo de herramientas.

4.2.2. SIGINT

No hay evidencia pública (leyes, compras, fallos, prensa o reportes técnicos) que confirme la adquisición o la operación de *IMSI catchers* por parte de agencias uruguayas. Referencias periodísticas locales describen *IMSI catchers* como tecnologías "posibles", pero no acreditan compras.[237]

Las empresas mencionadas que funcionan en la región —Pat Systems, Almenta Group, Titan/Titan-Geo y otros— publicitan *IMSI catchers* y ofrecen sus productos a todos los gobiernos de la región. Sin embargo, no se identifican contratos o entregas en Uruguay.

Sobre los pedidos concretos de geolocalización mediante explotación del proto-

---

233 "Bonomi: 'Descartamos la compra de El Galileo porque es invasivo'," *El País* (Montevideo), 16 de julio de 2015. URL

234 "Ministerio del Interior recibió oferta para adquirir software espía Pegasus," *Caras y Caretas*, 23 de julio de 2021, URL

235 Unidad Reguladora y de Control de Datos Personales, Resolución Nº 30/021 (2 de agosto de 2021). URL

236 Juan Francisco Pittaluga, "El Ministerio del Interior recibió propuesta para obtener Pegasus, el software israelí usado en presunto espionaje ilegal," *Búsqueda*, 21 de julio de 2021, consultado el 3 de noviembre de 2025, URL

237 Marina González, "Secretos a la luz", *La Diaria*, 15 de abril de 2025, URL

colo SS7, la plataforma Mobile Surveillance Monitor reporta más de 8000 incidentes del tipo "IMSI Identity Disclosure / sendRoutingInfoForSM (SRI-SM) / 3G" atribuidos a CTI/AM Wireless Uruguay (razón social de Claro Uruguay). Esto indica que existe actividad de señalización SS7 orientada a obtener el IMSI de abonados uruguayos mediante SRI-SM, una operación legítima del núcleo 2G/3G que —mal usada— filtra el IMSI y el MSC del objetivo. Sin poder confirmarlo, con esto, puede inferirse un riesgo real de exposición de explotación al protocolo SS7-Diameter por el alto volumen de SRI-SM anómalos contra la red de Claro, usados por actores privados o estatales en otros países de la región.[238]

El sistema disponible en Uruguay con estas capacidades es, de nuevo, EGO de Innova SpA, que funciona también en Chile. Esta suite fue adquirida en 2024 y es utilizada en la Dirección General de Represión al Tráfico Ilícito de Drogas. Las herramientas EGO de Innova permiten monitorear comunicaciones telefónicas e integran diversas tecnologías de vigilancia en tiempo real. Sus capacidades de geolocalización mediante la utilización del protocolo SS7/Diameter fueron descritas por los propios funcionarios involucrados en la compra: "Entre sus principales funciones se destacan la localización geográfica de dispositivos móviles —con visualización en mapas—, el envío de mensajes SMS invisibles para rastrear objetivos sin que estos lo perciban, y la generación de alertas sonoras ante eventos previamente definidos", sostiene un documento del Ministerio Público italiano al que accedió el medio *Búsqueda*.[239]

4.2.3. Inteligencia de red

Gracias a un pedido de información legislativa, la Corte de Justicia informó que entre 2009 y marzo de 2014 los jueces penales habían ordenado más de 6.000 interceptaciones telefónicas —un promedio cercano a tres por día, sin estándares uniformes de transparencia sobre su uso.[240] Por el sistema público de licitaciones, sabemos que una de las empresas proveedoras de este tipo de servicios fue Teleimpresores SA.

Al menos en una primera instancia, también esta empresa funcionó como mediadora en la adquisición del sistema brasileño "Intellotum - El Guardián" de Dígitro Tecnología Ltda. En 2014, esta compra fue entonces capitalizada como solución para unificar interceptaciones que en la práctica funcionaban de manera desorganizada. El Ministerio del Interior defendió de hecho la herramienta por su capacidad de control, y en diciembre de ese año la Suprema Corte habilitó su operación.[241]

---

238 M. Cappellari, *Detecting SS7 Attacks in the Telecommunication Networks*, Aalborg University, 2025. URL

239 Pittaluga, Juan Francisco. "Carlos Negro sobre la necesidad de comprar nueva tecnología de interceptación: 'El Guardián pasó de moda.'" *Búsqueda*, 10 de julio de 2025. URL

240 Fabrizio Scrollini, Ana Tuduri y Katitza Rodríguez, "Vigilancia de las Comunicaciones del Estado y la Protección de los Derechos Fundamentales en el Uruguay (2016)", *Necessary and Proportionate*, marzo de 2016.

241 "El Guardián: el nuevo vigilante que compró el gobierno", *El Observador*, 4 de marzo de 2015. URL / "El sistema 'El Guardián' quedó habilitado; protocolo firmado por Fiscalía, Interior y SCJ", *En Perspectiva*, 2 de diciembre de 2015. URL

En paralelo, se licitaron múltiples procesos para el desarrollo y mantenimiento del Sistema de Administración de Interceptaciones Legales (SAIL). Pliegos y anexos técnicos de compras públicas describen a SAIL como un sistema que automatiza la generación, firma y envío de órdenes judiciales a las operadoras y centraliza el flujo de aprobaciones, rechazos y tipos de medidas (intervención, información, datos históricos, tráfico, etc.).

De este modo, el funcionamiento de El Guardián con el SAIL está regulado por un memorando entre la Fiscalía, el Poder Judicial y el Ministerio del Interior: la policía solicita la medida, Fiscalía la analiza y el juez autoriza o rechaza; la orden viaja por SAIL a la operadora telefónica, que valida la firma digital del juez y entrega el tráfico a El Guardián, donde queda almacenado y disponible para la investigación.[242]

Según la cobertura de ese momento, "Intellotum - El Guardián" era capaz de intervenir hasta 800 celulares y 200 teléfonos fijos en simultáneo, crear hasta 100 cuentas espejo de e-mail y monitorear redes sociales.[243] Estas capacidades se potenciaron con el tiempo.

El Ministerio del Interior, de hecho, sostuvo y expandió la plataforma. En 2019, utilizó unos 65.000 dólares para ampliar sus capacidades y subrayó que su desarrollo exclusivo estaba hecho por Digitro "a medida" de la Secretaría de Estado.[244] En 2022, el Tribunal de Cuentas autorizó el uso de más de un millón de dólares —por compra directa y en carácter "secreto"— para nuevas funcionalidades de El Guardián, y en noviembre de 2024, Presidencia registró una misión oficial para visitar a Dígitro, identificada allí como "proveedora del Sistema Guardián On-line", confirmando la continuidad tecnológica.[245]

El Guardián era, ante todo, un sistema centralizado de interceptación legal (LI) bajo autorización judicial que articula a la policía, la fiscalía, los jueces y las operadoras para intervenir comunicaciones (telefonía fija, telefonía móvil, mensajería) dentro del proceso penal; el propio gobierno lo presentó así y detalló que "sólo el juez competente tiene la llave digital" para habilitar su uso.[246]

Dicho esto, con el tiempo las distintas capacidades lo transformaron en un sistema más abarcativo con capacidades ampliadas (p. ej., creación de cuentas espejo de e-mail y monitoreo de publicaciones en redes sociales) que, aunque se encuadren en causas con orden judicial, desbordan la interceptación legal y se introducen en el terreno de OSINT/vigilancia digital sobre información abierta.

---

242 "'El Guardián': así funciona el sistema de escuchas telefónicas del Ministerio del Interior", *Subrayado*, 21 de noviembre de 2022. URL

243 "Justicia avaló cerrojo en torno a 'El Guardián'; apelarán el fallo", *El País*, 14 de marzo de 2015; "Gobierno compró 'El Guardián' para espiar llamadas y redes sociales", *Subrayado*, 26 de julio de 2013.

244 "Compra por Excepción 17/2019. Proveedor Digitro Tecnología Ltda. para 12 unidades". URL

245 "Tribunal de Cuentas autorizó compra secreta de nuevas funcionalidades de El Guardián", *Montevideo Portal*, 14 de noviembre de 2022. // Presidencia — Gub.uy, "Resolución S/N/024: participación de Hugo Darío Imas Charlin en la visita a la empresa DIGITRO TECNOLOGÍA (TELEIMPRESORES S.A.), proveedora del Sistema Guardián On-line", 1 de noviembre de 2024.

246 Presidencia de la República (Uruguay), "Solo el juez competente tiene la llave digital para autorizar uso del sistema Guardián," 13 de marzo de 2015.

Parecería que su núcleo funcional es de interceptación legal, pero integra módulos que posibilitan tareas afines a OSINT cuando se trata de observar y analizar contenidos públicos en línea.[247]

En efecto, según el gráfico de la Plataforma Guardião de Dígitro (ver arriba), no se trata sólo de interceptación telefónica y reconocimiento o transcripción de voz: el fabricante la presenta como un ecosistema modular de inteligencia e investigación que integra gestión de operaciones y captura de múltiples fuentes, análisis y fusión de datos, monitoreo de información pública , inteligencia financiera, banco de rostros/biometría, georreferenciación y colaboración segura. Si bien las implementaciones reales pueden remitirse a un subconjunto de módulos según el cliente, el marketing del proveedor deja claro que Guardião es una suite amplia en continuo desarrollo.[248]

La cronología muestra así un pasaje desde un régimen de interceptaciones fragmentado hacia uno centralizado, seguido de ampliaciones persistentes de capacidades, pero todavía con un nivel de opacidad relevante en la divulgación de datos de uso y control.

Investigaciones periodísticas registraron algunos riesgos de abuso, desde el uso político de información de interceptaciones y la venta de información hasta problemas de control interno, como el uso compartido de usuarios y contraseñas entre la Dirección de Inteligencia y el Departamento de Antiterrorismo.[249]

---

247 *El Observador*, "Ministerio del Interior afirma que pondrá en marcha los controles de El Guardián," 9 de julio de 2019. URL // *Necessary & Proportionate*, "Vigilancia de las comunicaciones del Estado y la protección de los derechos fundamentales en el Uruguay," marzo de 2016. URL // *UyPress*, "¿Qué es el Guardián?," 9 de marzo de 2015. URL

248 "Plataforma Guardião: Solução para Segurança Pública | Dígitro." *Dígitro Tecnologia*, Consultado, 1 octubre 2025. URL

249 Garat, Guillermo. "Escándalo Uruguay: de pasaportes rusos a espiar opositores." *AP News*, 30 de noviembre de 2022. URL

Sobre esto, los dos operadores privados móviles están integrados en la misma arquitectura de interceptación legal que Antel. Movistar Uruguay publica un "Protocolo de Entrega de Datos a Autoridades Competentes", donde explica que la mayoría de los pedidos judiciales llegan a través del SAIL (Sistema Automatizado de Interceptaciones Legales), que se integra con el sistema "El Guardián", ambos provistos por el Ministerio del Interior, "y que se encuentran interconectados con infraestructuras de las tres empresas de comunicaciones de Uruguay".[250]

Además, en 2024, Uruguay adquirió el sistema EGO de la empresa italiana Innova SpA mediante su distribuidora en Chile.[251] El costo fue de 250.000 euros y también se trata de un sistema modular escalable, por lo que también resulta difícil determinar cuáles de sus capacidades fueron adquiridas. En un principio, se trataba de una herramienta de interceptación legal que con el tiempo integró interfaces para telefonía fija y móvil, datos IP, email, MMS y comunicaciones de vídeo, grabación de conversaciones, metadatos y localización. Dispone de un repositorio con marca temporal y firma digital para asegurar integridad, maneja casos, usuarixs y auditorías centralizadas, y se adapta mediante APIs a nuevos formatos de red OSINT.[252] La información disponible no permite saber si EGO también funciona a través de SAIL.

4.2.4. Monitoreo de red

Uruguay es el único caso analizado donde documentos públicos aluden de forma relativamente directa a la existencia de inspección profunda de paquetes (DPI) en la operadora estatal.[253] Un documento programático menciona de manera explícita la necesidad de "legislar sobre el correcto empleo de los dispositivos que hoy posee ya Antel para la inspección de comunicaciones entre ciudadanos", y subraya a la "tecnología de inspección profunda de paquetes de datos (DPI)" como un riesgo para la protección de datos personales. Al menos aparece en la formulación política de un senador y un candidato provincial en el

---

250 Una investigación de la revista *Sudestada* sobre el SAIL detalla que el sistema fue diseñado para procesar digitalmente las interceptaciones y que el protocolo de 2015 obligaba al Ministerio del Interior y a las tres operadoras telefónicas (Antel, Movistar y Claro) a reportar trimestralmente las interceptaciones efectuadas, justamente porque estas se implementan desde sus redes. *Sudestada*. "Ministerio del Interior omitió informar a SCJ por casi cuatro años sobre intervenciones telefónica." 31 de agosto de 2019. URL

251 Pittaluga, Juan Francisco. "Carlos Negro sobre la necesidad de comprar nueva tecnología de interceptación: 'El Guardián pasó de moda.'" *Búsqueda*, 10 de julio de 2025. URL

252 Según el manual técnico de Innova (2011) y seguimiento de fuentes secundarias que describen que EGO "enables to intercept, decode and restore on the same interface all types of IP communication, such as Video-communications, MMS..." URL

253 Hay, de hecho, evidencia antigua –pero muy clara– de gestión de tráfico tipo DPI en un ISP. A mediados de los 2000, usuarios de Dedicado (ISP inalámbrico/fijo) reportaban filtrado fuerte del tráfico P2P. Un análisis técnico publicado en 2006 describe que el tráfico P2P se filtraba mediante equipos Packeteer ("PAKETEERS") instalados en el router central de la red, que identificaban y limitaban P2P por horarios para no saturar el enlace internacional. Packeteer era, precisamente, una de las soluciones comerciales de DPI/traffic shaping más populares de esa época, luego absorbida por Blue Coat. URL

2015: “Perfeccionar la ley de protección de datos personales, protegiéndolos de la tecnología de inspección profunda de paquetes de datos (DPI). Legislar sobre el correcto empleo de los dispositivos que hoy posee ya Antel para la inspección de comunicaciones entre ciudadanos”.[254]

Los documentos oficiales de Antel de 2010 establecen que la operadora estatal se apoya en el DPI ya presente en su core móvil, evitando “sondas adicionales”.[255] El dato no identifica fabricante, pero deja claro que la inspección profunda se ubica dentro del núcleo donde se aplican políticas de tráfico, clasificación de aplicaciones y gestión.

Documentos de planificación del sector móvil uruguayo y la propia evolución tecnológica de Antel permiten inferir una continuidad tecnológica con Alcatel-Lucent (hoy Nokia). En 2011, Antel lanzó la primera red 4G comercial de la región con solución completa de Alcatel-Lucent; en 2019, Nokia y ANTEL anunciaron la primera conexión 5G en una red comercial de América Latina. Con ese historial, es razonable inferir que Nokia sea un proveedor central del equipamiento actual de Antel. Además, la documentación pública de Nokia describe módulos de “Application Assurance” que identifican aplicaciones y aplican políticas sobre el tráfico (funciones equivalentes a DPI) en sus plataformas de red, lo que haría plausible que el mismo proveedor que arma la red pueda ofrecer también la capacidad de inspección.[256]

También Huawei tiene presencia fuerte de infraestructura 5G con Antel, lo que implica que, como cualquier proveedor de red, sus equipos pueden integrar módulos de DPI e interceptación legal.

4.2.5. OSINT / WEBINT

Como señalamos, en Uruguay, el uso policial de OSINT existe, pero el Ministerio del Interior no brinda información sobre protocolos, áreas responsables o herramientas concretas de ***“ciberpatrullaje”***.[257]

Según lo analizado, las dos plataformas adquiridas desde las agencias de seguridad uruguayas, El Guardián y EGO, tienen módulos con capacidades OSINT. Sin embargo, aunque resulte probable, se desconoce si fueron adquiridos dentro del paquete de soluciones contratado.

En 2022, el Estado actualizó la plataforma a Guardián Online (del proveedor brasileño Dígitro), mediante una compra autorizada en régimen reservado. La propia documentación oficial confirma a Dígitro/Teleimpresores como proveedor del “Sistema Guardián On-line” y la literatura comercial de la empresa describe módulos para “datos de redes sociales y fuentes abiertas” con un “catálogo de

---

254 “Tecnología de la Información y las Comunicaciones - Senador Dr. Pedro Bordaberry”, URL
255 Administración Nacional de Telecomunicaciones (ANTEL), “Archivo adjunto de la aclaración Nº 4”, Portal de Compras Estatales (Uruguay), 3 de julio de 2024. URL

256 Alcatel-Lucent. “Antel and Alcatel-Lucent Launch 4G/LTE Services in Uruguay and Establish the First Commercial 4G/LTE Wireless Network in a Latin American Country”. URL

257 Díaz Charquero, Patricia, y Jorge Gemetto. *Ciberpatrullaje: Los límites borrosos de la vigilancia policial en Uruguay*. Montevideo, Datysoc, 2022. URL

más de 200 fuentes OSINT"—es decir, funcionalidades de WEBINT/OSINT integradas al ecosistema de investigación.[258] Algo similar sucede con EGO: cuenta con capacidades OSINT cuya adquisición no ha sido confirmada.

Por otro lado, la Secretaría Nacional para la Lucha contra el Lavado de Activos y Financiamiento del Terrorismo (SENACLAFT) de Uruguay recibió formación internacional que incluye el uso de "inteligencia" para convertirla en evidencia —lo cual sugiere que emplean herramientas de análisis de fuentes abiertas o datos públicos.[259]

Asimismo, el Observatorio Nacional sobre Violencia y Criminalidad declaró que ha incorporado "un software para el análisis de redes sociales (UCINET)" para profundizar en "aspectos vinculares o relacionales de la criminalidad". En organismos de seguridad, UCINET puede emplearse para analizar redes delictivas, relaciones entre individuos, estructuras de apoyo, mapas de actores, flujos de comunicación o colaboración, lo cual la convierte en una herramienta relevante para la inteligencia basada en redes.[260]

Más allá de las agencias de seguridad, hay contrataciones estatales uruguayas de organismos públicos que compran "servicios de vigilancia digital" o "monitoreo de redes/medios" con cláusulas de alerta sobre menciones y perfiles. El Banco Hipotecario del Uruguay , por ejemplo, licitó un servicio de vigilancia digital con monitoreo de redes sociales y detección temprana de amenazas reputacionales; otras dependencias licitan monitoreo de redes y medios para gestión de crisis y comunicación. Aunque no son adquisiciones policiales, muestran capacidad instalada de rastreo y alerta sobre contenidos abiertos dentro del aparato estatal.

---

258 Prosecretaría de la Presidencia de la República, Expte. N° 2024-4-1-0006320, 1 de noviembre de 2024. URL

259 "First joint training on Intelligence into Evidence to Paraguay, Uruguay" URL

260 Nicolás Zara, *"Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay,"* Buenos Aires, CELE, 2023. URL

Tabla 4: Resumen Uruguay

URUGUAY				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Spyware	**Hacking Team (Italia)**	OMNI S.A.–RADAR (Paraguay)	RCS	Poco probable
	NSO Group (Israel)		Pegasus	Poco probable
SIGINT	**Innova S.p.A. (Italia)**	Tecnodata / Mipoltec (Chile) / Innova S.p.A. (Chile)	EGO (capacidades de explotación SS7-Diameter)	Muy probable
Inteligencia de red / *Lawful interception*	**Teleimpresores SA (Uruguay)**	Teleimpresores SA (Uruguay)	Equipo para interceptación telefónica	Confirmada
	Digitro Tecnologia Ltda (Brasil)	Teleimpresores SA (Uruguay)	Intellotum - El Guardián	Confirmada
	Innova S.p.A. (Italia)	Innova S.p.A. (Chile)	EGO	Confirmada
	Nokia (Finlandia)	Antel	Módulos de LI	Muy probable
	Ericsson (Suecia)	Antel	*Lawful Interception* System	Confirmada
	Huawei (China)	Antel	Módulos de LI	Muy probable
Monitoreo de red	**Nokia (Finlandia)**	Antel	Módulos DPI	Muy probable
	Huawei (China)	Antel	Módulos DPI	Muy probable

URUGUAY				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
OSINT	**Innova S.p.A. (Italia)**	Innova S.p.A. (Chile)	EGO	Muy probable
	Digitro Tecnologia Ltda (Brasil)	Teleimpresores SA (Uruguay)	Intellotum - El Guardián	Confirmada
	Analytic Technologies (EE. UU.)		UCINET	Confirmada
	Social Links (EE. UU.)	TAMCE (Argentina-México)	Crimewall	Probable
Extracción forense	**Cellebrite (Israel)**	Softron Uruguay S.A. (SoftronIT) / IAFIS Uruguay	UFED	Confirmada
	Magnet AXIOM (Canadá)	Softron Uruguay S.A. (SoftronIT)	Axiom / Axiom Cloud add-on	Confirmada
	Oxygen Forensics		OnRetrieval	Confirmada
	Belkasoft Evidence Center X (EE. UU.)			Confirmada

URUGUAY				
Herramienta	Empresa	Distribuidora local	Tecnología / Producto	Adquisición
Videovigilancia / Biometría / Reconocimiento facial	Hikvision (China)			Confirmada
	Dahua (China)			Confirmada
	Huawei (China)			Confirmada
	ZTE (China)			Confirmada
	IDEMIA (Francia)			Confirmada
	NEC (Japón)			Confirmada
	Clearview AI (EE. UU.)			Confirmada
	M Electronics Monitoring Inc. (EE. UU.)			Confirmada

5. Algunas conclusiones

5.1. Un contexto común

Como señalamos al comienzo, PRISM y Pegasus ilustran dos escenarios narrativos distintos: dos extremos sólo aparentemente inaceptables. Ambos muestran distintos límites de lo que puede tomarse por legítimo y, a la vez, las mismas condiciones para su aceptación. Las características generales de PRISM no desaparecieron. Más bien se establecieron. NSO Group y otras empresas similares siguen existiendo. Los discursos sobre el tema determinan la forma misma del debate, brindan las variables en discusión y legitiman o cuestionan herramientas de interceptación y monitoreo.

En este marco, Argentina, Uruguay y Chile no suelen aparecer entre los países con un fuerte control de la información. Según los parámetros de Freedom House, Internet Society o AccessNow, no registran bloqueos significativos de tráfico web, apagones de internet, aplicaciones prohibidas u obstáculos sistemáticos al acceso de contenidos.[261] Tampoco ocuparon las primeras planas en las noticias que cubrieron el comercio de las más resonantes tecnologías de vigilancia. Podemos considerarlos, entonces, escenarios que se mantienen dentro de cierto promedio.

Sin embargo, hay que tener cuidado con semejante conclusión. Nos referimos a un ámbito poco explorado. Las compras estatales en materia de seguridad se encuentran veladas. Tampoco se han realizado análisis forenses consensuados de dispositivos para descartar indicadores de amenazas, ni investigaciones sobre infraestructura maliciosa. Más bien podemos concluir lo contrario. No hubo suficiente investigación sobre el tema. Existió un interés constante en la adquisición de este tipo de herramientas. Y en rigor sólo es cuestión de tiempo: o bien para que se confirme su adquisición, o bien porque ya están por ser compradas. Por esto, lo que se conoce de la trama ya vuelve urgente su discusión.

Las *soluciones* implementadas muestran que no existen suficientes instancias de visibilización y debate sobre procesos que se dan de manera continua y acelerada. Según el recorrido realizado, el marco regional muestra características compartidas a tener en cuenta para llevar a cabo estas discusiones.

Convergencia hacia arquitecturas de vigilancia completas. Las tablas confeccionadas muestran que los tres países incorporaron, con distintos niveles de intensidad, prácticamente todo el espectro de tecnologías de vigilancia. Esto muestra una tendencia no sólo regional hacia arquitecturas integradas, donde las capacidades no se adquieren de forma aislada, sino más bien como sistemas complementarios o de integración por módulos.

Sin embargo, las tablas muestran diferencias relevantes en el modo de adopción. Uruguay parece presentar un perfil diferenciado dentro de la región. Parece haber una baja probabilidad de adopción de *spyware* comercial, pero sí un desarrollo sostenido de capacidades integradas directamente en la infraestructura estatal, en particular a través del operador público de telecomunicaciones. El énfasis está puesto en la interceptación legal, el monitoreo de red mediante

261 Freedom House. “Countries and Territories”, 2025. URL // Internet Society, “Internet Society - Pulse.”,URL // Access Now. “Access Now.” URL

DPI, el uso de OSINT y el análisis forense, lo que configura un modelo más centralizado, estructural y regulado, antes que basado en operaciones encubiertas puntuales. En contraposición, en Argentina predomina un ecosistema fragmentado, con múltiples intermediarios locales, adquisiciones probables o parciales y una acumulación progresiva de capacidades entre distintas agencias y niveles del Estado, lo que configura un modelo flexible, opaco y difícil de auditar. En Chile, se observa una adopción más amplia y permanente: varias tecnologías altamente intrusivas —incluido *spyware* comercial— figuran como adquisiciones conocidas de agentes más reconocidos en el medio.

Cambios políticos y capacidades tecnológicas. A pesar de los —a veces radicales— cambios políticos de los países de la región, existe una tendencia común. De Piñera y Bachelet a Boric; de Cristina Fernández y Macri a Alberto Fernández y Milei; de Mujica y Vázquez a Lacalle Pou y Orsi —del progresismo a la derecha y de la extrema derecha a la centro-izquierda— el interés por los mismos productos permanece constante. Es cierto: con mayor o menor intensidad. Con distintos niveles de espectacularización. Con diferentes modos de capitalizar la adquisición de estos productos. Con otros discursos sobre su justificación. Y con, para nada menores, espacios que funcionen como salvaguardas.

Desde ya, esto último es central: el dispositivo político-institucional sobre el cual se asientan estas herramientas resulta crucial, ya que determina sus instancias de control. No obstante, esto constituye al mismo tiempo un riesgo a la vez mayor. Las herramientas pueden aceptarse bajo ciertas condiciones políticas. Esas condiciones pueden cambiar y las tecnologías ya están implementadas. Nunca las capacidades descritas van a dejar de ser un peligro político y social latente.

Implementaciones en un marco concreto suman un riesgo estructural. Muchas formulaciones clásicas plantearon este tipo de desafíos políticos en seguridad. Vale la pena pensar que el problema no son las tecnologías en sí, sino sus usos ya documentados contra periodistas, activistas y políticxs. Pero la aceptación racional condicional contiene un peligro incondicional. En el caso de tecnologías como estas, el poder otorgado bajo ciertas condiciones no desaparece cuando cambian esas condiciones. La implementación de tecnologías encarna decisiones políticas que siguen operando incluso cuando el contexto político cambia. Su adopción, además, con seguridad, resulta difícilmente reversible. Eso sí: sean estos Milei-Bullrich, Cristina Fernández-Parrilli, Piñera, Maduro o Bolsonaro, seguro que no queremos que nuestros rivales políticos tengan acceso discrecional a estas tecnologías. Casi seguro tampoco queremos que existan agencias de inteligencia autonomizadas con acceso a ellas.

Ahora bien, a nivel macro, sea cual sea el signo político del gobierno, la cantidad de adquisiciones mantiene un aumento constante.

Fuerzas de seguridad y agencias de inteligencia. De hecho, en paralelo al despliegue de capacidades de vigilancia digital, en Argentina, Chile y Uruguay persisten prácticas de espionaje "old school" —seguimientos físicos, infiltración, escuchas e inteligencia política— realizadas por servicios de inteligencia y fuerzas de seguridad con márgenes significativos de autonomía y débil supervisión civil. Los casos de espionaje ilegal atribuidos a la AFI en Argentina, las irregularidades y montajes revelados en la Operación Huracán en Chile y las investigaciones parlamentarias sobre espionaje militar y policial en democracia en Uruguay muestran cómo recursos y tecnologías estatales pueden emplearse de forma

discrecional o incluso cuentapropista, con fronteras difusas entre funciones de inteligencia y tareas policiales, sin controles efectivos sobre el uso real de las herramientas disponibles. Actualmente, estas tareas las realizan servicios de inteligencia con pocas garantías legales, sin la debida autorización política y con límites difusos con respecto a las fuerzas del orden. Por esto, es probable que haya que dar por sentado que las fuerzas de seguridad disponen de estas herramientas a su libre discreción, más allá de sus potenciales usos legales.

Los cambios geopolíticos y los alineamientos internacionales configuran un cuadro que, aunque a veces resulta opaco o fragmentario, sugiere que los países productores de herramientas de interceptación pueden contarse con los dedos de una mano y que las adquisiciones responden a alianzas internacionales evidentes. Es importante entender cuáles gobiernos impulsaron ciertas propuestas y cuáles las rechazaron. El *spyware* y las capacidades de interceptación se han convertido en herramientas geopolíticas. No solo buscan disponer de esas capacidades para sus propios fines, sino también regularlas en beneficio propio o en perjuicio de Estados competidores. En este marco, el interés declarado por los derechos humanos, o los derechos digitales, suele operar más como una ficha de negociación ética, dentro de un debate que tiene a la competencia geopolítica como motor principal.

Si Israel, Italia e India toman la delantera cuando se trata de *spyware*, entre estos, Latinoamérica sólo parece consumir los producidos por Israel e Italia.

En el plano de las herramientas SIGINT, Israel, Estados Unidos y Alemania ocupan el podio. Y de estos, Israel y Estados Unidos son sobre todo quienes nos venden *IMSI catchers* y tecnología de localización mediante el protocolo SS7-Diameter.

La "interceptación legal" con inteligencia de datos de red parece estar a cargo de productores europeos, con Italia y Alemania a la cabeza. Pero es Italia en donde se radican las empresas que parecen copar con éxito nuestro mercado.

Esto deja un panorama claro. Mientras la mayoría de los países de América del Sur adquieren este tipo de tecnologías de Occidente, las herramientas de otros grandes productores mundiales (como Rusia y China) sólo pudieron ser confirmadas en Cuba, Venezuela y Nicaragua.[262]

La investigación de Insikt Group siembra la duda sobre la posible adquisición de productos del conglomerado ruso Citadel —que agrupa a las empresas MFI Soft, Vas Experts y Protei. En conjunto, estas compañías desarrollan tanto soluciones de seguridad de la información, con inspección de paquetes, protección de bases de datos, filtrado de tráfico en Internet, como sistemas de interceptación legal (SORM). Diversos medios rusos informaron que las compras de productos de MFI Soft se habrían iniciado ya en 2017 en la región, a lo que cabe sumar el acercamiento de Argentina a Rusia y los BRICS entre 2019 y 2023, junto con el peso de Brasil en la región.

En síntesis: existen gobiernos que estrechan sus relaciones de seguridad con Estados Unidos e Israel y gobiernos que se abren también a contratos con China y Rusia.

Expertxs. Argentina, Uruguay y Chile conforman un polo regional de ciberseguridad con profesionales técnicxs altamente capacitadxs que resultan competitivxs

---

262 Insikt Group. *Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America.* Recorded Future, 2025. URL

en términos de experiencia técnica en relación con los costos, lo que ha impulsado la instalación de oficinas regionales, equipos remotos y operaciones avanzadas de múltiples empresas del sector. Casos como Core Security, surgida en Argentina en los años noventa, y el entramado local de firmas entre las que se encuentra Onapsis, evidencian la capacidad de producir investigación, herramientas y servicios de alcance global. Este ecosistema se ve reforzado por conferencias especializadas —como EkoParty en Buenos Aires y 8.8 Matrix en Chile— que atraen actores internacionales, funcionan como espacios de capacitación intensiva y operan como plataformas de reclutamiento.[263] Por este motivo, compañías extranjeras, entre ellas la suiza Dreamlab —vinculada a la estructura inicial de funcionamiento de FinFisher—, han establecido equipos en el Cono Sur aprovechando la disponibilidad de talento especializado. A esto se suma la incorporación sistemática de técnicxs de la región en equipos de investigación de empresas multinacionales (*vendors* de antivirus, consultoras y proveedores de seguridad digital), favorecida por el alto nivel técnico, el manejo de inglés, el huso horario compatible con Europa y Estados Unidos y la mano de obra relativamente barata. Así, los países del Cono Sur latinoamericano proveen especialistas capacitados a empresas que participan en alguna parte de la cadena del circuito; si bien no como productores directos de herramientas digitales de vigilancia, sí como desarrolladores de infraestructura, vulnerabilidades y *exploits*.

Legislaciones y vacancias. No es el tema de este reporte, pero es claro que constituye un eje central. Como en el resto de la región, leyes de seguridad ya caducas siguen vigentes y provocan una vacancia legislativa en mucho de lo que refiere a herramientas de vigilancia digital. En materia normativa, tanto Argentina (Ley 25.520 de Inteligencia Nacional y marco general de protección de datos), como Chile (Ley 19.974 sobre el Sistema de Inteligencia del Estado y Ley 19.628) y Uruguay (Ley 19.696 del Sistema Nacional de Inteligencia de Estado y Ley 18.331 de protección de datos personales) conservan esquemas concebidos para la interceptación clásica de comunicaciones y el tratamiento genérico de datos personales, sin reglas específicas, detalladas y transparentes sobre adquisición, uso, control democrático y rendición de cuentas en torno a *spyware*, explotación de vulnerabilidades, monitoreo masivo en línea u otras herramientas de vigilancia digital avanzada. Esto configura, en los tres países, una vacancia regulatoria que habilita amplios márgenes de discrecionalidad para fuerzas de seguridad e inteligencia y mantiene zonas grises significativas en la protección efectiva de derechos fundamentales frente a la vigilancia digital contemporánea. Como dijimos, en un marco global en el que Estados Unidos protege a sus propios ciudadanos con leyes específicas y Europa ha logrado imponer su Reglamento General de Protección de Datos (GDPR), lxs ciudadanxs de América del Sur carecen de mayores amparos legales frente a grandes, medianas y pequeñas compañías que acumulan y comercializan datos.

Dependencia estructural de proveedores extranjeros. Esto último cobra relevancia porque en los tres casos se repite un patrón: las tecnologías críticas provienen mayoritariamente de empresas de Israel, Italia y Estados Unidos. Los actores locales aparecen casi exclusivamente como distribuidores, integradores o socios comerciales. Esto refuerza una dependencia tecnológica que limita

---

263 Sobre esto último puede verse: Perlroth, Nicole. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race.* Bloomsbury Publishing, 2020.

la transparencia y la auditoría sobre herramientas de alto impacto en derechos fundamentales. Esta dependencia tecnológica introduce riesgos estructurales: pérdida de soberanía tecnológica, dificultades de auditoría y una relación asimétrica en la que los Estados incorporan capacidades de vigilancia avanzadas sin control efectivo sobre sus alcances y límites.

Importadoras intermediarias. Existe entonces un conglomerado de empresas intermediarias y representantes locales que comercializan tecnologías de vigilancia avanzada de forma reservada, con escasa transparencia y, en muchos casos, con niveles de profesionalismo discutibles. Los correos filtrados de Hacking Team mostraron negociaciones con revendedores y agencias de la región marcadas por improvisación, escaso soporte técnico y licencias costosas que quedaban obsoletas o inutilizadas, así como márgenes para usos personales o discrecionales de las herramientas. Muchas de estas firmas ofrecen simultáneamente servicios al sector privado, organismos públicos y fuerzas de seguridad, combinando catálogos abiertos con portafolios más opacos; adoptan nombres genéricos anodinos difíciles de rastrear —Infotech, Teleinformaciones, Automation Systems, Business Solutions Group, etc.— y sitios web mínimos con formularios de contacto como único canal visible, lo que suele permitir verificar la relación comercial, pero no el tipo específico de producto adquirido ni sus capacidades efectivas, reforzando las zonas grises en materia de control y rendición de cuentas.

En contrapartida, **el ecosistema** de instituciones de la sociedad civil que desarrollan investigación sobre las herramientas disponibles y sus usos lleva a cabo tareas fundamentales. El Security Lab de Amnesty Internacional junto al Citizen Lab de la Universidad de Toronto llevan la delantera en todo lo que se refiere a investigación técnica y el desarrollo de métodos novedosos para descubrir estas herramientas. Sus reportes técnicos, muchas veces publicados en colaboración con agencias periodísticas de prestigio, sientan los hitos del campo.

Por su parte, a nivel regional, Access Now combina varias líneas de acción en el llamado sur global; entre otras, brinda asistencia mediante su Digital Security Helpline e impulsa campañas globales (por ejemplo, contra los apagones de internet, #KeepItOn) para frenar la censura, la vigilancia masiva y el abuso de poder estatal y corporativo. Además, existen organizaciones de alcance regional con un foco en la difusión de discusiones, pedidos de información pública y análisis legal. Por su trayectoria, entre estas se destacan Fundación Vía Libre de Argentina, Derechos Digitales de Chile, Datysoc de Uruguay, Social TIC de México, Fundación Karisma de Colombia, MarIA Lab de Brasil, ODIA de Argentina y 0xche (Latinoamérica). Entre ellas, sólo Social TIC y 0xche poseen capacidad de análisis técnico.

Spyware. El mercado latinoamericano está cooptado por dispositivos Android obsoletos. Muchas veces, aunque se hagan públicos parches de seguridad para el sistema operativo, los proveedores no incluyen esos parches en sus equipos. Al comprarlos bajo sus términos y condiciones, definen cuánto tiempo sus dispositivos recibirán esas actualizaciones. Por esto, no solo se trata de países en los que no se han realizado ejercicios de análisis forense consensuado, sino que además no existen indicadores de compromiso o información válida donde identificar infecciones de *spyware* específicas. En este contexto, identificar ofertas, compras y contrataciones se ha mostrado como el método más efectivo para determinar la presencia de *spyware* en la región.

SIGINT. En el Cono Sur, las capacidades de SIGINT asociadas a la vigilancia móvil combinan al menos el uso de *IMSI catchers* con plataformas de geolocalización remota basadas en vulnerabilidades del sistema de señalización. En el caso de la interceptación mediante la señalización del protocolo SS7/Diameter, muchas veces se adquieren los servicios directamente desde el exterior, sobre infraestructuras donde siguen operativas redes inseguras. Estas herramientas habilitan rastreo continuo y, en algunos casos, interceptación selectiva de comunicaciones con escasa trazabilidad, marcos legales desactualizados y mecanismos de control débiles.

Como fuimos señalando, se destacan dos proyectos de investigación. El primero, dedicado a descubrir antenas falsas o *IMSI catchers*, llamado FADE (*Fake Antenna Detection Project*), se desarrolló exclusivamente durante 2022 en Buenos Aires y Santiago de Chile.[264] El segundo, el Mobile Security Monitor, registra tanto la persistencia de infraestructura insegura como eventos de mal funcionamiento y errores de la red de telefonía compatible con ataques sobre la señalización SS7/Diameter.[265]

Inteligencia de red, interceptación legal y alrededores. Existe un punto central: desconocemos las capacidades concretas de estas herramientas. En el terreno de la inteligencia de red y la interceptación legal en América Latina persiste una brecha estructural de transparencia y control sobre las capacidades efectivas disponibles para Estados y operadores. Lo que se conoce proviene principalmente de análisis técnicos independientes, trabajos académicos y reportes de organizaciones como EFF, ADC, Derechos Digitales y Access Now, que muestran un escenario mixto: algunos proveedores de telecomunicaciones han incorporado mejores políticas de privacidad, pero siguen sin publicar de forma sistemática estadísticas de requerimientos estatales, criterios de entrega de datos, uso de herramientas de gestión de tráfico ni detalles sobre retención y generación de metadatos. A la vez, muchas evaluaciones de las políticas de privacidad de datos llevadas a cabo por organizaciones independientes brindan en general un resultado pobre. Empresas como Personal, Telecentro, Arlink, Direct TV y Claro obtienen, de hecho, una performance preocupante.[266] En paralelo, se documenta la existencia de soluciones de monitoreo activo y pasivo —incluyendo DPI e interfaces de interceptación integradas en la red—, adquiridas bajo fuertes reservas y con escasos mecanismos públicos de auditoría, lo que impide evaluar con precisión el alcance real de las capacidades de vigilancia y refuerza las zonas grises en materia de garantías procesales y control democrático.[267]

Extracción y análisis forense, videovigilancia y biometría. Estas tecnologías no han sido objeto de este reporte y presentan problemáticas propias. Los equipos de videovigilancia son en general provistos por empresas chinas(ZTE, Huawei, Dahua,

---

264 https://fadeproject.org

265 Mobile Surveillance Monitor. "Mobile Surveillance Monitor: dashboard". URL

266 Penas, Victoria. *¿Quién defiende tus datos? Argentina – 3ra. edición.* ADC, 2023. URL

267 Veridiana Alimonti, *Eight Years Holding ISPs to Account in Latin America: A Comparative Outlook of Victories and Challenges for User Privacy.* San Francisco, EFF, 2023. URL

Hikvision) y los de biometría provienen mayoritariamente de Estados Unidos. El mercado de extracción y análisis forense para fuerzas de seguridad es hegemonizado a nivel regional por la tecnología UFED de Cellebrite. Aunque hasta ahora no se han detectado abusos en América del Sur, los riesgos asociados a estas tecnologías han sido ampliamente discutidos. Diversos informes internacionales señalan que estas mismas empresas comercializan sus productos en países donde se violan los derechos humanos.[268] En la práctica, en Estados Unidos estas extracciones suelen realizarse sin la autorización judicial correspondiente.[269] En Brasil, se ha documentado un uso indiscriminado,[270] y en Serbia existen registros del empleo de estas herramientas para desbloquear dispositivos con el fin de instalar *spyware* —desde ya, sin consentimiento— para lograr persistencia en el monitoreo.[271]

Por estos motivos, las discusiones en torno a estas tecnologías son muchas. Las herramientas forenses comerciales no poseen auditorías independientes y no permiten establecer estándares de fiabilidad, transparencia y admisibilidad. Las agencias de seguridad simplemente depositan allí su confianza sin mayores garantías. Además, puede plantearse que el uso de *exploits* no parcheados sobre vulnerabilidades no publicadas ejerce cambios radicales sobre el dispositivo, compromete la cadena de custodia de información y así, en consecuencia, la validez de la prueba digital presentada ante un tribunal.[272] A esto se suma que las propias herramientas tienen vulnerabilidades de seguridad que podrían ser explotadas con datos alojados en los teléfonos a propósito y, en consecuencia, alterar la prueba o el correcto funcionamiento de las herramientas forenses.[273]

Finalmente, como en el mencionado caso de Serbia, el hecho de que puedan operar sin dejar rastros en el dispositivo habilita su uso espurio con fines ilegales. Como está documentado, en contextos donde el Estado actúa contra disidentes, periodistas, activistas o minorías, estas herramientas pueden convertirse fácilmente en instrumentos de represión.

5.2. Problemas - Tensiones - Aporías

Cada una de estas herramientas trae distintas discusiones políticas, sociales y legales, al tiempo que plantean una serie de problemas comunes. A continuación, presentamos un punteo parcial a modo de cierre.

---

268 Pisanu, Gaspar, y Verónica Arroyo. *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*. Access Now, 2021. URL

269 Koepke, Logan, Emma Weil, Urmila Janardan, Tinuola Dada y Harlan Yu. *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones.* Upturn, 2020. URL

270 Ramiro, André, Amaral, Pedro, Canto, Mariana, and Pereira, Marcos César. *Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasi.* Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2022. URL

271 Amnesty Tech. *Serbia: "A Digital Prison": Surveillance and the Suppression of Civil Society in Serbia.* Amnesty International, 2024. URL

272 P. Dimpe, "Impact of Using Unreliable Digital Forensic Tools," *Proceedings of the World Congress on Engineering and Computer Science*. San Francisco: IAENG, 2017, 118–125. URL

273 Existen casos documentados de vulnerabilidades explotables en UFED y EnCase. URL

- **Privatización y opacidad de la capacidad estatal de seguridad y vigilancia.** La expansión comercial de estas herramientas produce una privatización de funciones clásicamente soberanas. Las decisiones sobre quién puede *vigilar* a quién quedan desplazadas a directorios corporativos y esquemas contractuales opacos. Desde el punto de vista teórico y político, esto configura un complejo industrial con capacidad de condicionar políticas públicas sin un control democrático proporcional.[274]
- **Producción deliberada de inseguridad estructural.** El modelo de negocio del *spyware*, los ataques de señalización SS7/Diameter y otras de las tecnologías mencionadas dependen de que existan agujeros de seguridad no corregidos. Empresas investigan vulnerabilidades, desarrollan y comercializan *exploits* y *suites* de intrusión. Los incentivos económicos favorecen la expansión del mercado, el secretismo técnico y el mantenimiento de vulnerabilidades abiertas. Cada exploit no reportado mantiene expuestos no sólo a supuestos "objetivos legítimos", sino a poblaciones enteras. Se subvierte el principio básico de seguridad digital: en lugar de fortalecer sistemas para todxs, se preservan debilidades para usos selectivos. Esto implica un problema social: la seguridad de millones queda subordinada a la necesidad estratégica de algunos actores de acceder a información que debería estar resguardada.[275]
- **Soberanía, geopolítica y colonialismo de vigilancia.** El *spyware*, los ataques mediante explotación de protocolos de señalización, muchas herramientas de inteligencia IP u OSINT permiten operaciones transnacionales silenciosas. Dispositivos ubicados en cualquier país pueden ser intervenidos remotamente. Empresas y gobiernos del mal llamado Norte global proveen herramientas utilizadas para vigilar opositores, periodistas y comunidades en el mal llamado Sur global. Estados con menos capacidades técnicas se vuelven dependientes de proveedores externos. Este esquema reproduce lógicas de dependencia tecnológica y modelos extraccionistas de datos: la capacidad de ver, mapear y anticipar se concentra en pocos nodos, mientras la exposición se distribuye asimétricamente.
- **Seguridad / privacidad / control político**. Muy brevemente: el desplazamiento del límite entre seguridad y control político se apoya en que el discurso legitimador de muchas de estas herramientas apela a la lucha contra el terrorismo, la pornografía ilegal y el crimen organizado. Sin embargo, investigaciones internacionales muestran su uso recurrente contra periodistas, defensores de derechos humanos, opositores y agrupaciones políticas. Este corrimiento tiene consecuencias políticas específicas: la frontera entre seguridad nacional y vigilancia política se vuelve opaca, la categoría de "amenaza" se expande hasta incluir voces críticas y el control sobre la discusión pública se ejerce por vías tácitas.[276]
- **Riesgo estructural.** Aceptar estas herramientas involucra aceptar un ries-

---

274 Amnesty Tech, *Operating in the Shadows: Investor Risk from the Private Surveillance Industry*. Londres, Amnesty International, 2021. URL

275 Lookout Mobile Security, *Technical Analysis of Pegasus Spyware*, 2016.URL
276 Forbidden Stories, "Pegasus: The New Global Weapon for Silencing Journalists," 18 de julio de 2021.URL

go político estructural, antes no conocido ni considerado. Como mencionamos, el dispositivo político-institucional sobre el cual se asientan estas herramientas resulta crucial, ya que determina sus instancias de control. Así, algunas herramientas pueden aceptarse bajo ciertas condiciones políticas. Pero esas condiciones pueden cambiar y las tecnologías ya están implementadas. Vale la pena pensar que el problema no son las tecnologías en sí, sino sus usos ya documentados contra periodistas, activistas y políticxs. Pero el poder otorgado bajo ciertas condiciones no desaparece cuando cambian esas condiciones. Nunca las capacidades descritas van a dejar de ser un peligro político y social latente.

- **Normalización de la vigilancia.** El riesgo radica en que la vigilancia se perciba como aceptada de hecho, funcionando como mecanismo de despolitización. Estas herramientas operan en un entorno donde la extracción de datos por plataformas, anunciantes y aplicaciones ya es considerada moneda corriente. Se diluye la diferencia entre (i) rastreo comercial, (ii) aceptación de términos y condiciones puntuales en plataformas concretas, (iii) vigilancia estatal y (iv) control total del dispositivo. No se trata solo de privacidad individual, sino de un ataque estructural a la confianza como recurso político y social.
- **Impacto sobre el periodismo y la deliberación pública.** Organismos internacionales y relatorías especializadas han documentado cómo esta vigilancia altamente intrusiva erosiona las condiciones materiales para el trabajo periodístico independiente, aun cuando no se concrete una represalia directa.[277] Según este argumento, estas herramientas introducen un efecto paralizante sobre la libertad de expresión y la producción de información. Periodistas y editorxs no pueden garantizar confidencialidad a sus fuentes. Las organizaciones y las redacciones comienzan a asumir un estado permanente de compromiso de dispositivos. De modo que esta percepción general alimenta una autocensura preventiva: reducción de temas investigados, moderación del lenguaje, renuncia a fuentes críticas. Al mismo tiempo, quienes asumen que "todo queda registrado digitalmente" tienden al cinismo o a la autocorrección constante. Ambos movimientos reducen la disposición al disenso abierto y a la organización social contra los límites de estas tecnologías. En este sentido, muchas de estas herramientas operan sobre las conductas políticas más que como meros dispositivos de obtención criminal de pruebas.
- **Límites de la noción de vigilancia.** Por todo esto, el concepto de "vigilancia" no resulta satisfactorio para abordar el uso de estas tecnologías. Lo utilizamos, pero presenta varios problemas. (i) Tiende a centrar el análisis en las agencias estatales de seguridad y opaca el rol decisivo de las empresas privadas y redes transnacionales con sus propias lógicas. (ii) Sugiere una continuidad con prácticas de persecución clásicas y no capta el salto cualitativo y cuantitativo. (iii) Presupone que el problema principal radica en su mal uso, en "ver demasiado" o recolectar datos en exceso, cuando

---

277 United Nations, Human Rights Council, *A/HRC/41/35: Surveillance and Human Rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (Ginebra: OHCHR, 2019). URL; Council of Europe, Commissioner for Human Rights, "Highly Intrusive Spyware Threatens the Essence of Human Rights," 27 de enero de 2023. URL; Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, *El impacto de la vigilancia digital en la libertad de expresión en las Américas*(OEA, 2025). URL

además la discusión incluye la capacidad de, al menos, mantener una inseguridad estructural, modelar conductas y producir cambios políticos. (iv) Mantiene el foco en la dicotomía uso legítimo/ilegítimo según la ley, lo que puede encubrir cómo estas tecnologías reconfiguran relaciones de poder aun cuando operen dentro de marcos formales.

***

Concluimos: son tecnologías que se expanden sin control ni debate. En buena medida, desconocemos las capacidades finales de estas herramientas y de su combinación, y las consecuencias políticas y sociales de su implementación a gran escala. Esperamos que este paneo permita al menos conocer, como un estado de la cuestión, cuáles son las herramientas y buena parte de las empresas que las producen y comercializan.

5.3. Límites, líneas de continuación

- **Inteligencia prospectiva.** Diversos informes de organizaciones de la sociedad civil han identificado una tendencia a desarrollar actividades de inteligencia prospectiva vinculadas a la prevención del delito. Esto implica la adquisición y acumulación de datos digitales sin una hipótesis criminal definida, un tipo de práctica que confunde de manera riesgosa las tareas de inteligencia policial con funciones de prevención del delito y conlleva controles y acopios de información ilegítimos.
- **Análisis forense consensuado.** Hasta el momento, no ha habido campañas de recolección de muestras de dispositivos móviles de activistas y dirigentes sociales en búsqueda de indicadores de infección para descubrir rastros de *spyware* en la región, como suele hacer Amnistía Internacional en otros países del globo.
- **Rastreo de infraestructura maliciosa.** Organizaciones como el Security Lab de Amnistía Internacional o Citizen Lab realizan monitoreo continuo de dominios y análisis del tráfico de red para identificar el despliegue de servidores de ataque y otras infraestructuras vinculadas a programas *spyware*. Las infraestructuras de los distintos proveedores de software de intrusión tienen huellas distintivas en cuanto a la forma en que se habilitan los servidores web, los lugares donde se adquieren los dominios de internet y la configuración de los servidores intermedios. Esto ha permitido, por ejemplo, a Amnistía Internacional obtener visibilidad sobre las pruebas y el despliegue de *spyware* en múltiples países de todo el mundo. Tampoco han existido análisis de este tipo en el ámbito local.
- **Análisis de información histórica de dominios y DNS.** El examen sistemático de historiales de dominios, cambios de DNS, registros de propiedad y movimientos de infraestructura vinculada a dominios ya identificados como indicadores de compromiso (IOC) sigue siendo una línea de investigación inexplorada para descubrir la presencia de campañas de *spyware* en la región.
- **Análisis legal preciso del alcance de cada herramienta.** Hasta donde se sabe, tampoco existe, en general, una práctica consolidada de evaluación jurídica detallada de las capacidades específicas de cada solución de vi-

gilancia. En ausencia de dictámenes técnicos-legales que crucen funcionalidades (geolocalización, interceptación, intrusión, retención de datos, etc.) con normas constitucionales y procesales, se consolidan zonas grises donde tecnologías altamente intrusivas se normalizan mediante contratos administrativos genéricos.

- **Pedidos de información pública.** Los mecanismos de acceso a la información constituyen una herramienta clave, pero subutilizada, para auditar la compra y uso de tecnologías de vigilancia. Allí donde se han presentado solicitudes, las respuestas suelen ser parciales, fragmentarias o amparadas en reservas de seguridad nacional, lo que refuerza la necesidad de estrategias más sistemáticas, litigios estratégicos y articulación regional para abrir estos datos y someterlos a escrutinio democrático.

Glosario

0-DAY EXPLOIT	*Exploit* que aprovecha una vulnerabilidad cuyo conocimiento no es de acceso público y carece de un parche oficial disponible.
0-CLICK EXPLOIT	*Exploit* que no requiere interacción alguna del usuarix para ejecutarse.
1-CLICK EXPLOIT	*Exploit* que requiere una única interacción del usuarix (por ejemplo, clickear un enlace).
3G / 4G / 5G	Tecnologías de telecomunicaciones móviles de tercera, cuarta y quinta generación, respectivamente.
3GPP (3RD GENERATION PARTNERSHIP PROJECT)	Consorcio que establece las especificaciones técnicas para sistemas móviles (GSM/3G/4G/5G).
ANSI (AMERICAN NATIONAL STANDARDS INSTITUTE - ANSI)	Organismo que supervisa el desarrollo de estándares para productos y servicios en EE. UU.
APT (ADVANCED PERSISTENT THREAT)	Ataques digitales dirigidos y persistentes cuyo objetivo es recopilar datos y monitorizar comunicaciones durante períodos prolongados.
ATTACK VECTOR	Vector de ataque; camino o método por el que un atacante accede a un sistema (email, web, mensajería, etc.).
BACKDOOR	Puerta trasera; defectos de seguridad incorporados de fábrica para mantener acceso persistente a un sistema de software o hardware.
CALEA (COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT)	Ley de EE. UU. que obliga a facilitar interceptaciones legales en redes.
CIFRADO DE EXTREMO A EXTREMO	Esquema criptográfico en el que los datos se cifran en el dispositivo del emisor y solo se descifran en el dispositivo del destinatario, de modo que los intermediarios (p. ej., servidores de transporte) no pueden acceder al contenido.
CSPS (COMMUNICATIONS SERVICE PROVIDERS)	Proveedores de servicios de comunicaciones; organizaciones que ofrecen y operan servicios de comunicación y conectividad (voz, datos, mensajería, video) mediante infraestructuras y redes de telecomunicaciones, gestionando su provisión, operación y soporte a usuarios finales o empresas.
DF (DIRECTION FINDING)	Técnica de radiogoniometría que estima la dirección de llegada de una señal de radiofrecuencia mediante antenas/sensores y métodos de procesamiento, para localizar o rastrear la fuente emisora.
DIAMETER	Conjunto de protocolos de señalización en redes telefónicas 4G y 5G que puede ser manipulado para tareas de localización e interceptación.

DOS/DDOS (DENIAL OF SERVICE / DISTRIBUTED DENIAL OF SERVICE)	Denegación de servicio; ataque que busca degradar o interrumpir la disponibilidad de un servicio o red saturando recursos (ancho de banda, CPU, memoria o sesiones).
DNS (DOMAIN NAME SERVICE)	Servicio que hace que nombres de dominio legibles (como example.com) funcionen, traduciéndolos a direcciones IP para que encuentren el servidor correcto.
DOWNSTREAM	Modalidad de obtención de datos en la que la información se adquiere directamente desde proveedores de servicios o plataformas, en lugar de interceptarse *upstream*, es decir, mientras circula por la infraestructura troncal de la red.
DPI (DEEP PACKET INSPECTION)	Inspección de tráfico de red que analiza paquetes más allá de los encabezados para identificar, clasificar, filtrar o priorizar comunicaciones.
DUAL-USE TECHNOLOGIES	Tecnologías de doble uso; tecnologías, componentes o conocimientos que pueden emplearse tanto con fines civiles y comerciales como para aplicaciones militares o de seguridad, por lo que suelen estar sujetas a controles y evaluación de riesgo.
ETSI (EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE)	Organismo europeo responsable de la estandarización de las telecomunicaciones.
EXPLOIT	Código, técnica o secuencia de acciones que aprovecha una vulnerabilidad para provocar un comportamiento no previsto en un sistema (p. ej., ejecución de código, escalamiento de privilegios o *bypass* de controles de seguridad).
EXPLOIT CHAIN	Cadena de *exploits* combinados para evadir defensas y lograr control no autorizado del sistema.
FADE (FAKE ANTENNA DETECTION PROJECT)	Proyecto/metodología para identificar antenas o estaciones base falsas (p. ej., *IMSI catchers*) mediante análisis de anomalías de red.
FINGERPRINTS	Huella digital; conjunto de características que permiten identificar o correlacionar de forma única o probabilística un dispositivo, usuario, aplicación o flujo de red, incluso sin identificadores explícitos.
GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS)	Estándar 2G de telefonía móvil digital que define la interfaz de radio, la señalización y la arquitectura de red para servicios de voz y datos (p. ej., SMS).
IMEI (INTERNATIONAL MOBILE EQUIPMENT IDENTITY)	Identidad internacional del equipo móvil; identificador numérico único (normalmente de 15 dígitos) asignado al equipo terminal móvil, usado por la red para identificar el dispositivo y apoyar funciones como control de acceso, inventario y bloqueo por lista negra.
IMSI (INTERNATIONAL MOBILE SUBSCRIBER IDENTITY)	Identidad internacional del abonado móvi; identificador único del abonado móvil almacenado en la tarjeta SIM, utilizado por la red celular para autenticar y gestionar la suscripción y la movilidad del usuario.

IP (INTERNET PROTOCOL ADDRESS)	Identificador numérico lógico asignado a una interfaz de red que permite el direccionamiento y enrutamiento de paquetes entre redes.
IOC (INDICATOR OF COMPROMISE)	Evidencia observable asociada a actividad maliciosa o intrusión (p. ej., hashes, dominios y direcciones IP, rutas, firmas, artefactos de host o patrones de red) utilizada para detectar, investigar y responder a incidentes.
ISP (INTERNET SERVICE PROVIDER)	Proveedor de servicios de internet; entidad que ofrece acceso a internet y servicios asociados.
JAMMERS / BLOQUEADORES / INHIBIDORES	Dispositivos electrónicos que generan interferencia para anular o bloquear señales de telefonía móvil, radiocomunicación o transmisión de datos.
KEYLOGGER	Software o dispositivo que registra las teclas pulsadas para capturar credenciales o mensajes.
LEA (LAW ENFORCEMENT AGENCY)	Organismos gubernamentales encargados de la aplicación de la ley y la seguridad pública.
LAWFUL INTERCEPTION (LI)	Interceptación legal; interceptación autorizada de comunicaciones por autoridades competentes bajo mandato judicial.
MITM (MAN-IN-THE-MIDDLE)	Ataque donde un tercero intercepta y/o modifica la comunicación entre dos partes sin ser detectado.
MALWARE	Software malicioso diseñado para dañar, acceder o robar información de sistemas.
MVT (MOBILE VERIFICATION TOOL)	Herramientas de código abierto para analizar logs de dispositivos móviles con el fin de detectar indicadores de compromiso (IOC) producto de infecciones por *spyware*.
N-DAY EXPLOIT	*Exploit* que aprovecha una vulnerabilidad que ya es de conocimiento público.
NETWORK INJECTION	Técnica que inyecta paquetes en el tráfico de Internet de un objetivo para bloquear, interceptar o manipular tráfico.
NETWORK MEASUREMENT METHODS	Técnicas para evaluar calidad, políticas o controles de redes (escaneo, medición de interferencia, etc.).
NOC (NETWORK OPERATIONS CENTER)	Unidad o instalación técnica dedicada a la supervisión, administración y mantenimiento continuo de una infraestructura de red.
NSA (NATIONAL SECURITY AGENCY)	Agencia de inteligencia de EE. UU. enfocada en señales e información y en ciberseguridad/criptografía para la protección de sistemas e infraestructuras gubernamentales.
OSINT (OPEN SOURCE INTELLIGENCE)	Disciplina de inteligencia que recolecta, procesa y analiza información disponible públicamente (fuentes abiertas) para generar conocimiento accionable, aplicando técnicas de verificación, correlación y contextualización.

PHISHING	Técnica de ingeniería social que induce a usuarios a revelar credenciales, datos sensibles o a ejecutar acciones maliciosas mediante suplantación de identidad (p. ej., correos, sitios o mensajes falsos).
PRISM	Nombre en clave de un programa de recolección de inteligencia de la NSA mediante el cual se obtenían comunicaciones y datos asociados directamente de proveedores de servicios de comunicaciones electrónicas con sede en EE. UU.
RANSOMWARE	Malware que cifra o bloquea sistemas y exige rescate para restaurar el acceso a la información.
RCE (REMOTE CODE EXECUTION)	*Exploit* que permite ejecutar código en un equipo de forma remota.
RCS (REMOTE CONTROL SYSTEM)	*Spyware* comercial desarrollado por la empresa italiana Hacking Team.
GDPR (GENERAL DATA PROTECTION REGULATION / REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)	Reglamento de la UE que establece el marco legal para el tratamiento de datos personales, definiendo principios, bases de licitud, derechos de los interesados y obligaciones de los responsables y encargados.
SOC (SECURITY OPERATIONS CENTER)	Unidad o instalación especializada en la supervisión, detección, análisis y respuesta ante incidentes de seguridad informática. El SOC monitorea de forma continua eventos y alertas provenientes de redes, sistemas, aplicaciones y dispositivos, con el objetivo de identificar actividades maliciosas, vulnerabilidades o accesos no autorizados y coordinar acciones de contención y mitigación.
SIGINT (SIGNALS INTELLIGENCE)	Inteligencia obtenida a partir de la interceptación y análisis de señales y comunicaciones electrónicas (p. ej., radio, telefonía, enlaces de datos), incluyendo tanto contenido como metadatos, para fines de inteligencia y seguridad.
SOCMINT (SOCIAL MEDIA INTELLIGENCE)	Disciplina de inteligencia que recolecta y analiza datos de redes sociales y plataformas sociales (contenido, metadatos e interacciones) para obtener información sobre actores, eventos, patrones y redes de relación.
SORM (SYSTEM FOR OPERATIVE INVESTIGATIVE ACTIVITIES)	Marco y especificación técnica de interceptación legal en Rusia que obliga a operadores/ISPs a instalar equipos que permiten a las agencias autorizadas (p. ej., FSB) interceptar y obtener comunicaciones o datos asociados.
SPYWARE	Software malicioso diseñado para obtener y exfiltrar información de un sistema (p. ej., datos, comunicaciones, credenciales o ubicación) o monitorear la actividad del usuario sin consentimiento y de forma encubierta.
SS7 (SIGNALING SYSTEM N.º 7)	Conjunto de protocolos de señalización usado en redes telefónicas para establecer y gestionar llamadas y servicios (roaming, SMS, enrutamiento), intercambiando información de control entre nodos de la red.
TACTICAL INFECTION	Vector de infección que opera en proximidad física al objetivo (p. ej., redes Wi-Fi maliciosas o estaciones base falsas).

TLS (TRANSPORT LAYER SECURITY)
Protocolo criptográfico de capa de transporte que proporciona confidencialidad, integridad y autenticación mediante *handshake* y cifrado simétrico, protegiendo comunicaciones cliente-servidor .

2 FA (TWO-FACTOR AUTH)
Mecanismo de control de acceso que requiere dos factores independientes para verificar la identidad, reduciendo el riesgo de compromiso por credenciales robadas.

UPSTREAM
Modalidad de adquisición en la que la NSA recolecta comunicaciones en tránsito mientras cruzan el backbone de internet, con asistencia obligatoria de las empresas que operan esa infraestructura, aplicando filtrado por *selectores* asociados a objetivos autorizados.

URL (UNIFORM RESOURCE LOCATOR)
Dirección de un recurso en internet; es una cadena de texto que indica dónde está (y normalmente cómo acceder) a algo como una página, imagen o archivo.

VENDORS
Empresas o proveedores responsables de ofrecer productos, servicios o soluciones tecnológicas.

VPN (VIRTUAL PRIVATE NETWORK)
Red privada virtual: método para comunicar redes de forma segura sobre redes públicas y/o ocultar identidad.

VOIP (VOICE-OVER-IP)
Tecnología que transporta voz en tiempo real sobre redes IP mediante digitalización, codificación y encapsulación en paquetes, usando protocolos de señalización y transporte (p. ej., SIP/RTP) para establecer y mantener llamadas.

XKEYSCORE
Nombre en clave de un sistema de análisis y consulta utilizado por la NSA para indexar, procesar y consultar grandes volúmenes de datos recolectados por distintos sistemas de inteligencia, permitiendo búsquedas por *selectores* (p. ej., email, IP, cookies) y análisis de actividad en red.

Sobre SocialTIC

SocialTIC es una organización mexicana sin fines de lucro que desde el 2012 se dedica a la investigación, formación, acompañamiento y promoción de la tecnología digital para fines sociales.
socialtic.org /@socialtic / contacto@socialtic.org

Autor

Lucas Dominguez Rubio

Agradecimientos

Al CeDInCI, en donde me formé y trabajo. A lxs colegas de Social TIC y a Paul Aguilar, junto con quien desarrollé esta investigación.
A Open Tech Fund y quienes impulsan este proyecto fundamental.
A las organizaciones de la sociedad civil y expertxs de sudamérica que desde hace ya décadas sostienen debates sobre estos temas.
A Iván Arce, Gary Miller, Beatriz Busaniche, Margarita Trovato, Patricia Diaz Charquero, Gaspar Pisanu y a 0xche, por compartir generosamente sus conocimientos y perspectivas.
Conté además con lecturas y apoyos decisivos: todo este trabajo no habría sido posible sin T. Le debo este recorrido; aprendí todo de ella, y mucho más.

SOCIALTIC

OPEN TECHNOLOGY FUND

ISBN: 978-970-96205-0-4