Horacio Azzolin, al mando de la Unidad especializada en Cibercrimen.

Poro atropar al ciberladrón

LEJOS DEL GLAMOUR DE LOS ESCUADRONES ANTIHACKERS DE HOLLYWOOD, LA FISCALÍA DE CIBERDELINCUENCIA A CARGO DE HORACIO AZZOLIN COMBATE LOS DELITOS ONLINE DE ARGENTINA. DE ROBOS DE IDENTIDAD Y FRAUDES A PORNOGRAFÍA INFANTIL, DE VENTA DE DROGAS Y ARMAS POR REDES SOCIALES A CASOS DE TERRORISMO, UN EQUIPO DE ABOGADOS E INGENIEROS NOS PROTEGE DE LAS AMENAZAS DE INTERNET. POR NATALIA ZUAZO · **FOTOS DE** FLOR COSIN

En el centro de su oficina, el fiscal Horacio Azzolin tiene un cuadro de Andy Warhol. Lo ve desde su escritorio cuando se sienta a la mañana, cuando baja a la sala de audiencias, cuando sale a dar clases al final del día. En el despacho también hay pelotas Gilbert de su pasado como *wing* de rugby; placas de bronce de las puertas que indicaron que fue secretario de Instrucción, juez subrogante, fiscal de la Procuración y fiscal federal; sus tres hijos en un portarretratos decorado con plasticola de colores; tomos del Código Penal y tratados internacionales; revistas de Derecho; medallas; pilas de expedientes ordenadas; gorritas de sus visitas a congresos de ciberseguridad; manuales de informática; dos teléfonos que vibran con mensajes de Telegram, y una computadora donde envía y recibe sus mails encriptados. Pero el cuadro de Warhol es el único objeto iluminado. Solo él recibe la luz del velador verde inglés y dorado que tiene prendido un martes de sol a las 11 de la mañana.

Al mando de la Unidad especializada en Cibercrimen, el de Azzolin podría ser un trabajo de sabueso entre cálculos y máquinas. Según Hollywood, su misión de encontrar a los delincuentes de internet podría resolverse en un laboratorio a lo *CSI*, con matemáticos y computadoras bajando líneas de código en cascada. Sin embargo, su oficio, mezcla de investigador penal y experto en tecnología, se trata de personas que se exponen y se esconden. De criminales que pasan desapercibidos o se dejan ver (por voluntad o por error) en algún rincón de lo digital. El método de Azzolin se basa en una *idea Warhol*: en internet, donde casi no queda lugar para esconderse, el éxito consiste en desaparecer.

El método de Azzolin es pararse a cada lado del límite invisible de internet hasta llegar al momento exacto en que el culpable se deja ver durante cinco minutos buscando la fama.

"El secreto es conocer la lógica de internet: cómo funcionan las redes, la encriptación, cómo se usa un navegador que no deja huellas", dice Azzolin (43 años, barba tan larga como la prolijidad judicial lo pide, frente bronceada, pelo húmedo hacia el costado, puños perfectos de una camisa celeste que asoma por un traje tan ajustado como para ser moderno, tan suelto como para ofrecer seriedad).

Parece obvio: el primer paso para atrapar cibercriminales es saber de tecnología para llegar a los que nos roban cuando nos conectamos al *home banking* desde un bar, a los que utilizan las redes sociales para captar mujeres para la prostitución, a los que siembran links de pornografía infantil en sitios con millones de visitas, a los que arman grupos de Facebook para difundir mensajes neonazis y a los que usan sus planes de datos para ejecutar atentados terroristas. Para acercarse a cualquiera de ellos, primero, hay que navegar el mapa de un universo que parece evidente, pero que no lo es (todos usamos internet; pocos saben cómo funciona). Azzolin conoce más que un usuario normal sobre redes: sabe de encriptación, de navegadores anónimos, de reglas de privacidad, de pagos en bitcoins. Pero solo con la técnica no garantiza su éxito.

–Yo busco qué motiva a las personas. Las rodeo hasta saber quiénes son, cómo se visten, dónde se mueven, qué usan. Llego al detalle que las delata. El mejor informático puede esconderse todo el día, pero yo descubro el momento en que se descuidó y pagó la luz por *pagomiscuentas* desde la IP de la casa.

Azzolin investiga y litiga hace 20 años. Sabe que en internet, o fuera de ella, todos tenemos un talón de Aquiles, un punto en que olvidamos, al menos por un segundo, que estamos rodeados de dispositivos y de rutas de datos. Allí, Azzolin gana. Su victoria ocurre en el momento en que somos más humanos que máquinas.

–Dos cosas hacen caer a cualquiera: el dinero y el ego –dice Azzolin mientras mira hacia arriba, cierra los ojos y se reclina hacia la derecha, un gesto que repite cuando está convencido de algo.

Aunque trabaje en medio de máquinas y aparatos, aunque Google ya les gane a los humanos al Go, aunque las heladeras ya hagan la lista del supermercado por nosotros, Azzolin está seguro de que sigue llevando ventaja: el delito online no se combate con técnicas sino entendiendo a las personas. Su método es pararse a cada lado del límite invisible de internet hasta llegar al momento exacto en que el culpable se deja ver durante cinco minutos buscando la fama.

El patio

Antes del Derecho a Azzolin le gustaban las computadoras. Lo supo en 1984, cuando los curas del Colegio Guadalupe compraron unas Sinclair 1000 y contrataron a Colombo, un profesor de computación que le enseñó sus primeras líneas de código. Tanto tiempo pasaba frente a los comandos del Basic –el lenguaje con el que su generación entró en la informática– que a los 13 ya programaba.

A los 17 tuvo una sola duda: ¿Historia, Ciencia Política o Derecho? Un profesor que además era juez lo convenció por las Leyes. Todavía alumno de la Universidad Católica, entró al Poder Judicial. A los 19, cuando cobró su primer sueldo en el Juzgado de Instrucción 21, ya no dudó: se gastó su paga completa en una Pentium 486 armada por un amigo.

Azzolin todavía no lo sabía, pero ya estaba construyendo su método. Internet era apenas un invento que usaban algunos académicos, empresas pioneras, diplomáticos y militares. Como invento reciente, se veía como una herramienta para hacer el bien. Su lado malo, la posibilidad de que en ella también se escondieran delincuentes, todavía quedaba lejos. Pero Azzolin ya se estaba preparando. Pasó por tres juzgados de Instrucción y una fiscalía en la provincia de Buenos Aires hasta que en 2008 llegó al Ministerio Público Fiscal, o "el estudio de abogados más grande del país", como él lo define. Sus años de entrenamiento en el litigio, sus horas estudiando e interrogando a estafadores, abusadores, criminales y toda clase de mentirosos profesionales lo estaban entrenando en el engaño.

En noviembre de 2015, Azzolin fue nombrado jefe de la Ufeci, una nueva oficina que se especializaba en investigar y combatir los delitos online. Lo puso al frente la jefa máxima de los fiscales, Alejandra Gils Carbó, que no dudó en elegirlo: Azzolin tenía 15 años de entrenamiento en el sistema acusatorio, sumados a un interés personal por la informática, que empezó conectando su primer juzgado a la internet de Impsat, armando la página web de su segunda oficina y tramitando la primera causa de pornografía que llegó a la Argentina desde Interpol. "La segunda también fue de pornografía: en 1996,

El equipo de la ciberfiscalía: Belén Ravarini, Diógenes Moreira, Cristian Mansilla y Azzolin.

una editorial denunció a un empleado por usar la conexión, que en ese entonces era carísima, para ver videos *hot* en horario laboral".

Uno a uno, cada expediente con algún elemento tecnológico terminaba en su escritorio: fiscales que le pedían rastrear la IP de un delincuente, denuncias de amenazas por mail, pedidos de información a Google y Microsoft. Entre 1998 y 2001, a medida que crecían los caños de internet en Argentina, los pedidos aumentaban. Azzolin los resolvía mientras trabajaba en juicios de lesa humanidad contra otros criminales, los de la dictadura militar. Más tarde, cuando hacia 2008 y 2009 ya todos tenían mails, blogs y las primeras cuentas en redes sociales, la demanda crecía. Pero fue en 2010 cuando las autoridades tuvieron que ocuparse en serio del asunto.

El boom

–En 2010, con la explosión de Facebook y las redes sociales, hubo un crecimiento exponencial de delitos informáticos –explica Azzolin, en un despacho prestado de la calle Perón que el Ministerio Público compró a la familia Bemberg, fundadora de la Cervecería Quilmes. En ese edificio con pasillos de laberinto, alfombras bordó viejas y escaleras de madera oscura, la procuradora le encargó que preparara los primeros protocolos de evidencia digital para una reunión del Mercosur y lo designó "punto focal" del cibercrimen. Los países comenzaban a trabajar en conjunto: la red, el sistema nervioso del mundo, no respetaba fronteras. Los nuevos ciberdelincuentes tampoco.

Desde el 2000, la Argentina contaba con una ley y una Dirección de Protección de Datos Personales que protegían la privacidad y los derechos de cualquier persona que tuviera información en una base de datos. En junio de 2008, se aprobó en el país una Ley de Delitos Informáticos que estableció (junto con el Código Penal) sanciones para la pornografía infantil, la violación de comunicaciones electrónicas, el acceso a sistemas informáticos, el fraude informático o los sabotajes a sistemas, entre otros. Las policías, como la Federal y la Metropolitana, sumaron recursos y tecnología a sus divisiones de cibercrimen. Pero sus funciones estaban (y están) más enfocadas en pericias e investigaciones a partir de casos en curso. Todavía faltaba, en el núcleo del sistema penal, una unidad específica capaz de llevar adelante casos e investigaciones propias desde cero, pero sobre todo de detectar patrones nuevos de delitos en el ámbito digital. Además, ese nuevo grupo de expertos tendría que cooperar con otras áreas que se enfrentaban a males "viejos" con formas "nuevas": delitos sexuales, económicos, de narcotráfico.

La experiencia de Azzolin como fiscal en otros casos no digitales fue decisiva para articular viejos métodos y problemas con nuevos conflictos y tecnologías.

–Los fiscales de lesa humanidad trabajábamos mucho en equipo. Un día nos dimos cuenta de que los defensores de los militares usaban las mismas estrategias en Salta o en Ushuaia –recuerda Azzolin–. Entonces establecimos un patrón común de acusaciones y dimos un salto exitoso.

Desde la Ufeci, Azzolin hoy coopera con otras áreas, con fiscales y con unidades que se enfrentan al desafío de inter-

net como potenciadora de delitos. Su equipo colabora con unidades especializadas en la trata de personas, la violencia contra la mujer, el narcotráfico, el lavado de dinero y la violencia institucional. También trabaja con otras oficinas del Estado, como Nic Argentina (encargada de dominios de internet), la Dirección Nacional de Datos Personales, la Datip (la oficina que brinda apoyo tecnológico a los fiscales) y el ICIC (el organismo que defiende a las infraestructuras de gobierno de ataques informáticos externos). Para el asesoramiento técnico recurre a instituciones públicas de prestigio como la UTN y la Fundación Sadosky. Y con privados como Mercado Libre, bancos o entidades de comercio electrónico. Para estas compañías, contar con una referencia experta en la Justicia como Azzolin es una ventaja: cuando detectan una nueva forma de delito o registran *modus operandi* novedosos, acercan la información a su oficina para sumarla a la biblioteca de amenazas.

Con 43 millones de habitantes, 30 millones de accesos a internet y 66 millones de líneas de celulares, el mapa online de Argentina es una geografía fértil para cometer delitos. Pero si además se suma cualquiera de los otros 3.200 millones de usuarios de internet del planeta, el atlas de la investigación cibercriminal se vuelve infinito. Por eso, nuestro país también coopera con el mundo para llegar a los delincuentes de las redes: en 2010, ratificó el Convenio de Budapest sobre Ciberdelincuencia y participa en foros regionales sobre el tema. En marzo de 2016, en su "Informe de Ciberseguridad 2016", la OEA reconoció el trabajo de Argentina. Destacó que, en medio de un aumento de los delitos informáticos, el país construyó "un exhaustivo marco jurídico para las TIC [Tecnologías de la Información y la Comunicación]" y desarrolló "la legislación procesal para el tratamiento de evidencia digital", donde reconoce a la Ufeci.

La cooperación es inevitable. Los delitos que se cometen en internet y por medio de internet crecen cada año y se vuelven transversales. Ya no se trata solamente de combatir las amenazas propias de internet (en la jerga, los *computer crimes*), como hackear computadoras, borrar datos o hacer ataques de denegación de servicio (también llamado DoS o *denial of service*: enviar millones de pedidos simultáneos a una página para que se sature y se "caiga"). Cada vez más, proliferan los delitos cometidos a través de internet (o *computer related crimes*), es decir, usando la red como medio para perpetuar delitos que ya existían, pero por otro medio, como reclutamiento de mulas para narcotráfico, ciberterrorismo, fraudes, robos de identidad. Para Azzolin, el mayor desafío es no "sobreinvestigar", sino dotar al sistema judicial de herramientas para que ellos mismos hagan sus investigaciones. En definitiva, el ciberterrorismo es terrorismo y un chat entre *dealers* es narcotráfico.

El equipo

En el método de Azzolin, la investigación penal y la programación tienen algo en común: probar caminos hasta llegar al que resuelve el problema. Para ser un buen abogado o un programador astuto se necesita curiosidad y lógica. Abstraerse de lo inminente y buscar patrones.

Pero nada de esto es posible en soledad. La Ufeci es un equipo de acción de seis personas. El abogado Cristian Mansilla aporta su experiencia en delitos federales. La letrada Belén Ravarini mantiene la comunicación y la capacitación con las otras áreas de la Justica. El politólogo Damián Neustadt, experimentado en investigación criminal, es el enlace con las fuerzas de seguridad. El informático Diógenes Moreira es el cerebro técnico del equipo. Con su apoyo, Azzolin detecta nuevos patrones de ciberdelitos.

–Como vengo del desarrollo de software, pienso lo que yo hubiera hecho. Pienso cómo puede equivocarse ese criminal. Todos dejamos huellas. Hasta los que más se cuidan –explica Diógenes.

Lejos del mundo del hacker con capucha de las películas o de los investigadores de trajes ceñidos tipo Matrix, el comando de la Ufeci trabaja con personas del mundo real. Para llegar a esos culpables hacen lo mismo que para cualquier investigación penal: los rodean en la periferia hasta encontrarles el flanco débil.

–Los narcos, por ejemplo, siempre hablan en código. Ninguno dice *Necesito 15 kilos de cocaína al 95 %*. Tienen un idioma propio. Cuando lo entendés, empezás a rodearlos.

En internet sucede lo mismo. El método de Azzolin sostiene que los ciberdelincuentes pueden operar con TOR (un navegador anónimo)

y mails encriptados, pero que en algún momento necesitan publicitar sus sitios o cobrar por sus servicios. Allí, el método recurre al tradicional "seguir el dinero". Internet también es un gran mercado.

–Hay vendedores de armas en la *deep web*. Pero también en Facebook, porque necesitan clientes. Es simple lógica de mercado –concluye Diógenes.

En la red actual, donde unas pocas empresas concentran la mayoría de los usuarios y de las transacciones, los investigadores tienen una ventaja. Como gran parte de los delitos se cometen adentro o a través de las mismas plataformas o servicios (Facebook, Google, Microsoft, Skype, Mercado Libre), los fiscales ya empiezan a conocer cómo investigar en cada plataforma. También que la mayoría de los 30 millones de usuarios de internet del país utilicen un servicio de tres o cuatro proveedores de internet facilita las investigaciones.

–Gran parte de nuestro trabajo es generar protocolos para que otros fiscales aprendan a pedir por sí mismos la información. Así, nosotros también podemos dedicar tiempo a nuestros propios casos de investigación –señala Belén Ravarini.

Allí, en el desarrollo de sus investigaciones propias, Azzolin se apasiona:

–Cada tanto, detectamos un patrón nuevo de ciberdelito. Por ejemplo, un tipo de mail que llega de una determinada forma para cometer fraudes o robar identidad. O transacciones bancarias destinadas a grandes compras de celulares que pueden llevarnos al lavado de dinero.

El equipo de Azzolin lleva la cuenta de los casos más frecuentes. En 2016, reciben una mayoría de denuncias sobre fraudes bancarios cometidos por internet. También siguen casos de sitios web de ofertas inmobiliarias vinculadas al lavado de dinero, monitorean falsas ofertas de trabajo relacionadas con la trata de personas o delitos sexuales, y páginas o redes donde se reclutan mulas para narcotráfico. Entre sus objetivos, la Ufeci empezará a llevar una estadística de delitos informáticos, ya que Argentina no cuenta con una base de datos centralizada al respecto. Y además, cuando otras unidades los requieren, se involucran con casos urgentes. El último verano, eso sucedió cuando cooperaron buscando en redes sociales a los integrantes de grupos neonazis de Mar del Plata que habían atacado a activistas de la comunidad LGBT.

El mundo

Mientras avanzan con sus investigaciones, Azzolin y su equipo tienen que lidiar con un problema creciente para la investigación criminal en la era de internet: cómo acceder a dispositivos o comunicaciones encriptados, o a comunicaciones que las empresas de contenidos de internet (Facebook, Google, WhatsApp) no están dispuestas a revelar para no perder la confianza de sus usuarios-clientes. El dilema es cómo garantizar el derecho a la seguridad sin violar otro derecho, el de la privacidad. Lo viven cuando, aun con una orden judicial, se enfrentan con la negativa de una empresa a cooperar con los datos de una comunicación digital, o cuando quieren acceder a un teléfono o aparato que podría contener datos relevantes para una investigación.

En el último verano, dos ejemplos pusieron sobre la mesa qué problema crece en los ámbitos de decisión más poderosos.

El primero, cuando el presidente de Apple, Tim Cook, se negó a desbloquear o crear una "puerta trasera" (o *back door*) para que el FBI accediera a los datos de un iPhone perteneciente al sospechoso de un tiroteo en San Bernardino, California. El caso escaló y llevó el debate al mundo: ¿Hasta dónde las empresas de tecnología pueden negarse a cooperar con la Justicia? El mismo presidente de Estados Unidos, Barack Obama, se pronunció: "Las compañías tecnológicas están yendo muy lejos. Si el gobierno no puede acceder a los dispositivos, entonces es como que todos están caminando con una cuenta en Suiza en el bolsillo". También levantaron su voz los activistas por los derechos digitales al reclamar el derecho humano a la privacidad, que tiene en la encriptación su aliado fundamental.

El segundo caso reavivó el debate, cuando las autoridades brasileñas arrestaron en San Pablo al vicepresidente de Facebook en América latina, el argentino Diego Dzodan, porque la corporación (dueña de WhatsApp) se negó a entregar informaciones de esa aplicación ante reiteradas órdenes judiciales.

El conflicto, sin solución en el mundo, apasiona a Azzolin. Como experto, él mismo sigue el manual: además de encriptar sus mails y celulares, cambia sus claves con regularidad, usa doble factor de autentificación, configura sus *routers* de wifi con frecuencia, mira al detalle la privacidad de cada aparato o aplicación que utiliza, hace *backups* prolijos de toda información relevante que le llega.

Reciben una mayoría de denuncias por fraudes bancarios cometidos en internet. También siguen casos de sitios web de ofertas inmobiliarias vinculadas al lavado de dinero.

–Como fiscal, tengo la obligación de investigar. Y, en algunos casos, me encuentro con obstáculos en las comunicaciones encriptadas –explica Azzolin.

Cristian, su ayudante informático, lo respalda:

–Tenemos la vida en el celular. Si accedés, te da diez veces más información que un allanamiento.

Aun con este límite, Azzolin sabe que su método funciona. Cree, además, que prohibir el uso de un servicio, como sucedió cuando Brasil bloqueó el uso de WhatsApp, provoca consecuencias más graves y la búsqueda de alternativas (Telegram sumó un millón y medio de usuarios en ese país durante esos dos días). Azzolin sabe que, incluso con obstáculos, siguiendo las reglas de la investigación siempre se llega a los culpables. Su experiencia también le indica que el estereotipo del hacker de capucha de las películas o de las series es solo eso, una caricatura.

–¿Cuántos *Mr. Robot* hay? Y si hubiera muchos, ¿cuántos podrían tener una vida en las sombras todo el tiempo? –pregunta Azzolin frente a su Warhol, que lo mira, a su vez, desde el ojo de una cámara.

Azzolin cree que los malos malísimos de las películas no son tantos. Que si están en internet, él sabe encontrarlos. Pero también que los peores no cometen el error de esconderse en la red.

–Estoy seguro: los malos de verdad están volviendo al papel –dice cerrando los ojos en señal de certeza. **B**