dic/15

Educar para vigilar

Una investigación acerca de la formación institucional estatal en vigilancia e investigación en el entorno digital

por los Derechos Civiles

Área de Privacidad

con el apoyo de

Diciembre de 2015
www.adc.org.ar

Índice

Educar para vigilar

Diciembre 2015*

I Introducción

A medida que los avances tecnológicos presentan innovaciones en los apartados técnicos, se genera un cambio rotundo en el paradigma del uso de la tecnología, lo que sumado a la evolución de internet y los servicios online, abre la puerta a la globalización en múltiples niveles tecnológicos. Esta convergencia es la que permite actualmente recolectar, analizar, diseminar y almacenar información sobre cualquier individuo en el mundo, por lo que la privacidad pasa a ser uno de los derechos humanos más fáciles de vulnerar.

Teniendo en cuenta este panorama es fundamental comprender el papel que juegan los entes gubernamentales y las fuerzas de seguridad en lo que a ciberseguridad, herramientas de interceptación de comunicaciones y vigilancia respecta. Mucho más en aquellos países que, como Argentina, han sufrido regímenes autoritarios y que, en el afán de evitar repetir prácticas antidemocráticas e ilegales, deberían ser rigurosos en el control exhaustivo del uso de recursos tecnológicos estatales y su adecuación a estándares respetuosos de los derechos humanos. Pero este no siempre es el caso, ya sea por atraso en la educación tecnológica, sea por falta de madurez en el funcionamiento de los entes estatales que aún guardan vestigios de aquellas prácticas autoritarias pasadas.

*Este trabajo fue realizado por Valeria Milanes y Leandro Ucciferri, del área de Privacidad de la Asociación por los Derechos Civiles (ADC).

A poco de reflexionar al respecto, la siguiente pregunta apareció como de urgente respuesta.

II ¿Qué formación reciben los funcionarios o agentes encargados de realizar tareas de vigilancia e investigación en el entorno digital?

Indagar acerca de la formación que reciben los funcionarios o agentes encargados de realizar tareas de vigilancia e investigación en el entorno digital nos pareció fundamental para comprender el grado de desarrollo de los sistemas de inteligencia y seguridad, como así también de las dependencias estatales dedicadas a la persecución e investigación de delitos, y su funcionamiento actual.

Sin embargo, al dar los primeros pasos en esta búsqueda pudimos ver que la información pública era escasa y en algunos casos inexistente. Asimismo pudimos confirmar que también son prácticamente inexistentes las instancias de capacitación y educación formal de los agentes y funcionarios en esta materia.

De tal suerte, ante la informalidad y precariedad del escenario descrito y a modo de abordaje exploratorio, debimos identificar las diferentes circunstancias en las que estas organizaciones efectúan tareas de vigilancia y/o investigación en el entorno digital, para luego intentar reconstruir la forma en que sus funcionarios o agentes van resolviendo estas tareas y así detectar qué herramientas o elementos utilizan para hacerlo. Tuvimos también que repasar ciertos aspectos generales de la formación que reciben, su historia y características, a fin de dar un marco institucional a los diversos elementos que fuimos recolectando.

Por otra parte, debemos tener presente que la legislación argentina es clara al indicar que para la interceptación de las comunicaciones hay un único organismo facultado, cuya intervención debe requerirse por vía judicial. Este organismo es el Departamento de Interceptación y Captación de las Comunicaciones (D.I.COM), dependiente de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (D.A.T.I.P.), perteneciente a su vez a la estructura del

Ministerio Público Fiscal de la Nación. Cualquiera sea el organismo o la fuerza que esté llevando a cabo la investigación, sin importar su jurisdicción, todos deben requerir la intervención del D.I.COM.

Sin embargo y más allá de la claridad de la norma, sabemos que coexisten múltiples organizaciones o unidades de inteligencia en las distintas fuerzas armadas y de seguridad, tanto federales como provinciales, como así también organismos encargados de investigaciones criminales que pueden tener acceso a este tipo de tecnologías. También sabemos que algunos de esos organismos están sospechados de arrastrar viejas prácticas (muchas de ellas heredadas de la última dictadura militar) reñidas con la legalidad y vulneradoras de derechos fundamentales.

Para esta construcción utilizamos información publicada en sitios web oficiales, comunicados de prensa y noticias institucionales con el fin de obtener información concreta sobre los programas lanzados y en funcionamiento, los cursos realizados y las carreras disponibles. A partir de dicha información identificamos a los funcionarios responsables y expertos en la materia, con la finalidad de entrevistarlos.

Cabe destacar que en la mayoría de los casos, el marco normativo que regula estas instituciones y sus ámbitos de enseñanza no se encuentran disponibles, sea porque tal marco regulatorio no existe, sea porque dichas normas se encuentran amparadas por su carácter de "reservado" o "secreto", característica usual en el sistema de inteligencia argentino.

Es por ello que este informe se nutre principalmente de información suministrada en entrevistas y consultas efectuadas a funcionarios, periodistas y otros actores claves. En la mayoría de los casos, los entrevistados dieron su autorización para citarlos como fuente, por lo que éstos serán debidamente identificados. En otros casos, los entrevistados pidieron permanecer en anonimato.

III Instituciones relevadas

Agencia Federal de Inteligencia

Cuando hablamos de inteligencia en Argentina, el organismo que sale naturalmente en la conversación es la A.F.I. o Agencia Federal de Inteligencia, conocida como S.I. (Secretaría de Inteligencia) entre 2005-2015, S.I.D.E. (Secretaría de Inteligencia de Estado) entre 1956-2005 y C.I.D.E. (Coordinación de Informaciones del Estado) entre 1946-1956.

La A.F.I. es el estamento superior jerárquico dentro del esquema del sistema de inteligencia nacional y viene con una ajetreada historia detrás que ha sido explorada por la ADC en su informe titulado "**El (des) control democrático de los organismos de inteligencia en Argentina**".[1]

La formación y capacitación de los agentes de la A.F.I., así como del resto de los organismos que integran el sistema nacional de inteligencia (que incluye a la Dirección Nacional de Inteligencia Criminal, dependiente del Ministerio de Seguridad, y la Dirección Nacional de Inteligencia Estratégica Militar, dependiente del Ministerio de Defensa), se desarrolla en el ámbito de la Escuela Nacional de Inteligencia (E.N.I.).

La E.N.I. se creó en el año 1967 por orden del entonces presidente de facto, Juan Carlos Onganía, y pasó a su ubicación actual, en una mansión ubicada en el barrio Recoleta en la calle Libertad 1235, bajo la presidencia de facto de Jorge Rafael Videla.

Desde los comienzos de la antigua C.I.D.E., los agentes eran entrenados para enfrentarse a un tipo de enemigo concreto. Así, en sus comienzos el enemigo al que se preparaban para enfrentar fue "el comunismo", y a quienes compartían dicha ideología, es decir, "los comunistas".

Este enemigo fue cambiando con el paso del tiempo, y según el clima político y social, los disidentes del gobierno de turno pasaban a ser blanco de la inteligencia

[1] ADC. (2015) Disponible en (PDF): http://www.adc.org.ar/el-des-control-democratico-de-los-organos-de-inteligencia-en-argentina

interna. Como bien señaló el periodista Claudio Savoia, lo que surge a partir de la enseñanza o el entrenamiento en base a blancos concretos es que estos *"pueden organizarse por grupos: los adversarios políticos, los jueces y fiscales curiosos, los periodistas, las organizaciones sociales, los judíos, los musulmanes (...)"*,[2] lo cual pone de manifiesto su clara raigambre persecutoria, no solo en el modo de llevar a cabo las tareas de inteligencia, sino en la formación y educación de los agentes en servicio.

En los inicios de la E.N.I., según Savoia, *"los alumnos eran formados en cerrajería, fotografía, seguimientos a distancia, infiltración y lecturas de labios"*. A fines de los años 40, para perfeccionar el trabajo de los agentes, estos eran enviados a entrenar y capacitarse junto con el Mossad, la agencia de inteligencia israelí. Esto fue cambiando a medida que las relaciones del gobierno de turno con los países extranjeros también cambiaba; en estos últimos años, la relación con las agencias de inteligencia extranjeras, por parte de la E.N.I., fue prácticamente nula.

Una vez que los agentes finalizaban su formación inicial, eran designados en alguna de las bases de la ex S.I.D.E., ubicadas en la Ciudad Autónoma de Buenos Aires, en el Gran Buenos Aires, y en el resto de las provincias del país. En la actualidad, las bases más importantes de la A.F.I. (sucesora de la S.I.D.E.), de las cuales tenemos conocimiento, son tres: Inteligencia Interior, ubicada en la calle Billinghurst al 2400, Contrainteligencia, ubicada en la calle Estados Unidos al 3100, y Terrorismo Internacional, ubicada en la Av. Coronel Díaz al 2000; las tres en la Ciudad Autónoma de Buenos Aires.

Hasta principios de diciembre de 2015, la Escuela estuvo bajo la dirección del Dr. Marcelo Saín, que fue diputado de la Provincia de Buenos Aires y ex-titular de la Policía de Seguridad Aeroportuaria (P.S.A.). La llegada de Saín a la E.N.I. a mediados de 2015, tuvo como principal objetivo continuar con la pretendida reforma del sistema de inteligencia dispuesta mediante ley 27.126 de marzo de 2015, encomendándole el desarrollo del Decreto 1311/15 –publicado en el mes de Julio de 2015-, reglamentario de aquella ley y que además estableció la Nueva

[2] Savoia, Claudio. (2015) Espiados. Argentina: Planeta. (Pag. 122)

Doctrina de Inteligencia Nacional.[3]

A partir de esta reforma, el ingreso a la A.F.I. debe hacerse mediante una preselección a través de universidades públicas y luego mediante una selección a cargo del área de Recursos Humanos de la Agencia, que determinará finalmente quiénes realizarán el curso de ingreso en la E.N.I. La única convocatoria de preselección que tuvo lugar desde la Reforma se realizó mediante llamados en cinco universidades: la Universidad Nacional del Centro de la Provincia de Buenos Aires, la Universidad Nacional de Quilmes, la Universidad Nacional de San Martín, la Universidad Tecnológica Nacional y la Universidad Nacional del Comahue. Estas Universidades no habrían sido elegidas al azar, sino que por el contrario, habrían sido seleccionadas teniendo en cuenta su distribución geográfica y la buena relación de las autoridades de E.N.I. y la A.F.I. con las autoridades universitarias, lo que habría facilitado que la convocatoria se pusiera en marcha de manera fácil y rápida.

La convocatoria estuvo planteada en cinco categorías: [4]

1. Analistas

    (a) Médicos psiquiatras con especialidad en adicciones

    (b) Licenciados en sociología

    (c) Licenciados en psicología

    (d) Economistas

    (e) Licenciados en administración de empresas

    (f) Licenciados en ciencia política

    (g) Licenciados en criminalística

    (h) Licenciados en relaciones internacionales

    (i) Abogados con orientación a derecho comercial, administrativo o penal

[3] Ley 27.126 disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm y Decreto 1311/15 disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

[4] Diario Infobae. 21 de agosto de 2015. Disponible en: http://www.infobae.com/2015/08/21/1749847-como-la-nueva-side-recluta-espias

(j) Traductores de inglés, ruso, chino o alemán

2. Oficiales

   (a) Técnico en investigación criminal

   (b) Estudiantes de informática con orientación al análisis de imágenes u orientación en seguridad informática

   (c) Estudiantes de criptología

   (d) Estudiantes de psicología, sociología, abogacía, licenciatura en criminalística

3. Asistentes administrativos: estudiantes de derecho, administración de empresas, relaciones públicas, relaciones del trabajo, contador público, recursos humanos, sociología, ciencia política.

4. Seguridad: estudiantes de carreras afines a la seguridad y la defensa personal

5. Informáticos

   (a) Ingenieros en sistema

   (b) Analistas de sistema Técnicos informáticos con especialidad en bases de datos

Según comentó Saín, los perfiles que se tuvieron en cuenta para esta búsqueda respondieron a un cambio surgido de la Nueva Doctrina de Inteligencia Nacional, así explicó que *"lo que se necesitan son recolectores, gestores de información, administradores de bases de datos y analistas, gente joven capaz de poder interpretar la información y las relaciones entre las mismas"*. [5]

El 13 de julio de 2015 se llevó a cabo en la E.N.I. el "Curso de Capacitación y Actualización Profesional en Inteligencia", con un total de 400 asistentes. De acuerdo a una presentación publicada por el sitio web oficial de Casa Rosada, los temas principales del curso fueron "nuevas definiciones, concepciones y principios

[5] Saín, Marcelo. Entrevista. 9 de diciembre de 2015.

en línea con la Nueva Doctrina de Inteligencia Nacional". [6] Como afirmó Saín, *"nosotros necesitábamos capacitar a la gente sobre qué trata la inteligencia, cuáles son las normas de este organismo, qué son las criminalidades complejas, la criminalidad política, el terrorismo, los atentados contra el orden constitucional, la criminalidad organizada relacionada al narcotráfico, la trata de personas, el tráfico de armas, la delincuencia económica y financiera (...)"*. [7]

La formación de los agentes propiamente dicha depende del escalafón al que hayan sido asignados, sea Inteligencia, Seguridad o Apoyo. El curso está dividido en tres módulos (General, de Especialización, de Residencia) que, así como su duración, dependen del escalafón correspondiente. El Módulo General debe ser realizado por los tres escalafones; el Módulo de Especialización debe ser realizado solo por los del escalafón de Inteligencia y contempla dos bloques, uno sobre Recolección de Datos e Información y otro sobre Análisis y Sistematización de la Información. Finalmente, el Módulo de Residencia debe ser realizado por los tres escalafones y en el mismo desarrollarán tareas específicas de acuerdo a su especialidad, bajo la supervisión de un tutor. En cuanto a la duración, el total es de 12 meses para el escalafón de Inteligencia, 7 meses para el de Seguridad y 6 meses para el de Apoyo.

Según refirió Saín, *"el viejo espía que se metía detrás de las líneas y que conseguía la información, eso quedó atrás, la mayoría de las fuentes son públicas y la mayoría de ellas están distribuidas en bases de datos que de alguna manera están en el Estado, migraciones, policías (...)"*, con lo cual, a partir del Decreto 1311/15, se le cierra la puerta a los investigadores callejeros. *"Acá, en la A.F.I., no va a haber escuchadores y, por ende, en la E.N.I., no se capacita a nadie para escuchar. En la A.F.I., no se escucha más a nadie. Las escuchas judiciales deben pedirse a un Juez y pasar por D.I.COM y, en ese marco, la escucha tiene relevancia en la parte final de una investigación criminal, donde vos tenés claro el funcionamiento de las relaciones y la existencia de dichas relaciones, es decir, cuando yo tengo que corroborar algo que ya está sospechado en la investigación, nada más. Pero eso*

[6] AFI, Presidencia de la Nación. Julio de 2015. Disponible en (PDF): http://www.casarosada.gob.ar/pdf/AFI.pdf

[7] Saín, Marcelo. Entrevista. 9 de diciembre de 2015.

no es una tarea de la A.F.I. sino de la justicia penal". [8]

Históricamente, la principal herramienta con la cual trabajaban los agentes de la ex S.I.D.E. era la intervención de teléfonos. Savoia relató en su libro que esta pieza clave en el poder que fueron ganando los espías de la agencia *"comenzó formalmente con la sanción de la ley secreta 19.083, del 16 de junio de 1971. (...) Alejandro Lanusse dispuso que cien agentes de la S.I.D.E. se incorporaran a la Empresa Nacional de Telecomunicaciones (E.N.TEL) para pinchar líneas telefónicas y vigilar las conversaciones que quisieran, mecanismo que se repitió en el Correo".*[9] Pero no sería sino hasta el 6 de noviembre de 1992 cuando el entonces Presidente Carlos Menem decidiera realizar el traslado de la Dirección de Observaciones Judiciales (conocida vulgarmente como "Ojota") y el trabajo de las escuchas a la base de Avenida de los Incas 3834, en el barrio de Belgrano, con todo el equipo que se había adquirido en los años anteriores. El lugar que en tiempos pasados supo concentrar el monopolio de las escuchas bajo el mundo secreto de la inteligencia, a partir de la llegada de la ley 27.126 y el Decreto 1311/15, pasó a depender del Ministerio Público Fiscal de la Nación, con el nombre de Departamento de Interceptación y Captación de las Comunicaciones (D.I.COM.), a cargo de la fiscal Cristina Caamaño.[10]

Policía Federal Argentina

En la comisaría 8 en la calle Urquiza 550, frente al Hospital Ramos Mejía en el barrio Balvanera, Ciudad de Buenos Aires, se ubica la "escuelita", como es conocida por sus alumnos y profesores. La "escuelita" es el alma mater de la división de inteligencia de la Policía Federal Argentina (P.F.A.), pues allí se forman "los plumas", sus agentes de inteligencia. Si bien sus comienzos no están del todo claros, el primer indicio nos lleva al gobierno de Juan D. Perón, que habría designado como primer jefe de la división de Inteligencia de la Policía Federal al coronel Jorge Manuel Osinde.

[8] Saín, Marcelo. Entrevista. 9 de diciembre de 2015.

[9] Savoia, Claudio. (2015) Espiados. Argentina: Planeta (Pag. 131)

[10] Procuración General de la Nación. 7 de julio de 2015. Disponible en: https://www.fiscales.gob.ar/procuracion-general/se-concreto-el-traspaso-de-la-doj-al-ministerio-publico-fiscal/

De acuerdo al relato de Iosi (o José Alberto Pérez, tal su nombre real), un ex-agente de los plumas, la Escuela se armó siguiendo el modelo del servicio de Inteligencia de la Alemania nazi. *"En la época del Proceso, el área de Inteligencia cobró fuerza en relación muy firme con los militares. Tenía el poder de decidir sobre la vida y la muerte de la gente que detenía. Cuando volvió la democracia, comenzó a haber peleas internas fuertes con las otras áreas. De ahí proviene la costumbre de llamarnos plumas, despectivamente, como revancha, en lugar de halcones"*.[11]

Al igual que en la ex S.I.D.E., los plumas de la Policía Federal debían mantener su verdadera identidad reservada usando un nombre falso y les aconsejaban aislarse de sus amigos y no contar nada de lo que hacían a su familia. Estas órdenes surgían del Decreto 2263 del año 1967, firmado por el entonces presidente de facto Juan Carlos Onganía. Este decreto permanece desde su sanción con carácter de Reservado, por lo que su acceso público no es posible.

A mediados de los años '80, el curso para convertirse en pluma duraba cinco años. En la Escuelita se estudiaba derecho civil y penal, historia de los partidos políticos, historia de los grupos antiterroristas, psicología y otras materias como "actividades antidemocráticas". Según Iosi, *"Era una contradicción que aprendiéramos leyes porque, por otro lado, nos instruían para cometer delitos, como por ejemplo, la irrupción subrepticia en un domicilio, es decir, entrar en un lugar, sacar lo que necesitábamos y dejar las cosas igual, de manera que nadie se diera cuenta de que habíamos estado ahí (...) Aprendías la norma y también como violarla"*. Además del curso, realizaban un entrenamiento de veinte días en el aquella época denominado Centro de Adiestramiento Policial Especial (C.A.P.E.), en Puente de la Noria, y allí recibían capacitación sobre seguimiento, sabotaje, infiltración y atentados.

La división de Inteligencia (según el relato de Iosi) cuenta con tres categorías de cuadros: el cuadro A son los operativos, el cuadro B los dedicados al análisis y el cuadro C los de apoyo (médicos, abogados, contadores, etcétera). Dentro del cuadro A se encuentran los "filtros", que son considerados la elite dentro de los

[11]Lewin, Miriam; Lutzky, Horacio. Iosi; el Espía Arrepentido. (2015) Argentina: Sudamericana. (Pag. 23)

plumas, debido a sus estrictos requisitos de ingreso.

Actualmente, según relató Claudio Savoia, llegan a la Escuelita cada año aproximadamente 150 postulantes, quienes para poder ingresar a cursar deben tener menos de 30 años de edad y aprobar una serie de exámenes sobre cultura general, desde la situación social, política y económica de Argentina y países extranjeros, hasta la farándula y el cine, además de hablar varios idiomas. Una vez aprobado el ingreso, comienzan su período de estudio por dos años y luego, a su fin, deben buscar un trabajo de superficie como cobertura, bajo otro nombre y con un sueldo que les alcance para vivir.[12]

Señaló Savoia que los profesores que enseñan actualmente en la Escuelita, *"son policías superiores, especialistas en algunos temas concretos, pero sobre todo son plumas en actividad o ex-plumas, que les enseñan cosas prácticas en su mayoría. Tienen que ser tipos muy cultos"*.[13]

Para fines de los años '80, principios de los '90, los plumas ya contaban con dispositivos para realizar escuchas telefónicas propias. La comisaría 9, desde su área técnica, les proveía los maletines para intervenir las líneas telefónicas y grabar las conversaciones, entre otros artilugios como cámaras ocultas. Pero con el pasar de los años y el consecutivo avance de las tecnologías, la situación se fue complicando para los agentes de la Policía Federal, quienes se vieron en la necesidad de pedir ayuda a la ex S.I.D.E. para acceder a las conversaciones de las personas que estaban espiando.

Según relata Savoia, *"hasta la sanción de la Ley de Inteligencia en diciembre de 2001, los espías se presentaban directamente ante la Ojota (denominación coloquial de la Dirección de Observaciones Judiciales) y le pedían que interviniera tal o cual línea para avanzar en la investigación de la causa equis, siempre del fuero federal. A los dos o tres días, el agente volvía a esa oficina de la S.I.D.E. en Av. de los Incas y preguntaba cuánto había de producido de esa línea (...) los escuchas de la S.I.D.E. tampoco eran muy melindrosos para comprobar que la causa equis efectivamente existiera y tuviera algo que ver con el pedido que los plumas traían a sus manos, con el correspondiente atuendo de sellos y lacres*

[12] Savoia, Claudio. (2015) Espiados. Argentina: Planeta (Pag. 77)
[13] Savoia, Claudio. Entrevista. 15 de octubre de 2015.

oficiales".[14]

A partir de la llegada de la Ley de Inteligencia en el año 2001, los agentes debían dirigirse al juez que estaba llevando el expediente y realizarle el pedido específico de la línea a intervenir. Pero esta situación llevó a que se hagan cada vez más comunes las vías ilícitas para llegar al contenido de las escuchas. Dentro de estas prácticas podemos mencionar: desde conocidos en la misma S.I.D.E. que hacían el trámite en su lugar, contactos en la Comisión Nacional de Comunicaciones (actualmente A.F.T.I.C.), o un policía amigo que agregaba el número a intervenir en el pedido de alguna investigación en curso.

El traspaso de la Dirección de Observaciones Judiciales desde la ex S.I.D.E. al Ministerio Público Fiscal habría buscado revertir estas prácticas.

Policía Metropolitana

A través de la ley 2894 del año 2008, se creó en el ámbito de la Ciudad Autónoma de Buenos Aires esta fuerza policial con competencia exclusiva en dicha jurisdicción. Debido a determinados convenios con el Estado Nacional se le transfirieron a la Ciudad competencias para habilitar a la Metropolitana para actuar en ciertos delitos como tenencia y portación de armas, lesiones en riña, abandono de personas, amenazas, violación de domicilio, usurpación, y daños, por nombrar algunos ejemplos.

Su estructura se compone de cuatro áreas, cada una a cargo de un superintendente: Seguridad, Investigaciones, Comunicaciones y Planificación. Dentro de la Superintendencia de Investigaciones se encuentra el Área de Cibercrimen, que junto a la Policía Federal Argentina y la Policía de la Provincia de Buenos Aires, son las únicas policías que tienen una división especializada en materia de delitos informáticos.

La ley vigente en la jurisdicción de la Ciudad de Buenos Aires prohíbe a las fuerzas de seguridad la realización de tareas de inteligencia criminal preventiva, motivo por el cual, según una fuente cercana que pidió permanecer anónima, la Policía

[14] Savoia, Claudio. (2015) Espiados. Argentina: Planeta (Pag. 89)

Metropolitana no mantiene bases de datos propias con el contenido obtenido a través de sus investigaciones, pero sí mantienen estadísticas o métricas de sus casos.

De acuerdo a nuestra fuente, la Policía Metropolitana, y más concretamente la división de Cibercrimen, no cuenta con herramientas tecnológicas de interceptación de comunicaciones, y en términos más amplios, la situación actual es que el personal que integra la división de Cibercrimen usualmente debe recurrir a la utilización de sus propias herramientas para el desarrollo de sus tareas de investigación, refiriéndose a notebooks, celulares, tablets, etc.

La principal tarea de investigación del área de Cibercrimen es a través de fuentes abiertas de datos, realizando una especie de verificación de antecedentes pero más extensa y detallada. Para esto trabajan con los canales oficiales de las principales empresas de Internet en términos de usuarios y masividad de datos, como Google y Facebook, en tres ámbitos:

Preservación del contenido: Por medio de los canales oficiales pueden solicitarle a la empresa que preserve determinada prueba. Si bien esto no los habilita a ver el contenido en sí, se aseguran que el mismo sea guardado por un cierto período de tiempo.

Registros: Solicitan a la empresa datos de suscripción, como las fechas de creación de una cuenta, la dirección de email utilizada, el número de teléfono, las direcciones IP; además de los historiales de conexión. Para suministrar este tipo de información las empresas requieren de una orden firmada por un juez o un fiscal.

Contenido: Para acceder al mismo se debe realizar a través de una rogatoria internacional (dado que las sedes de estas empresas se encuentran en jurisdicción extranjera) y los plazos en estos casos pueden llegar a ser de más de un año. La Policía Metropolitana no suele utilizarlo en sus investigaciones, principalmente porque en estos años no se habrían visto en la necesidad de hacerlo pero además, porque los plazos procesales necesarios para el trámite de la rogatoria internacional desalentarían su uso.

La fuente anónima nos mencionó también que la relación de la Policía Metropolitana con la ex S.I.D.E. no habría sido de lo más fluida, al menos hasta el traspaso de la ex D.O.J. a D.I.COM. En los únicos casos en que se habría visto en la necesidad de pedir colaboración fue para causas grandes de narcotráfico. En esos casos la operatoria habría sido la siguiente: la Policía Metropolitana determinó los domicilios de las personas investigadas en la causa, a través del juzgado interviniente se requirió a los proveedores de Internet de la zona para que informaran si brindaban o no servicio allí, luego con la orden del juez se le encargó a la ex-DOJ que interceptara el tráfico de Internet de esos usuarios. La ex-DOJ grabó los datos de tráfico en DVDs, que fueron entregados a la Policía Metropolitana para su análisis.

En cuanto a la formación del personal que integra esta fuerza, las personas que quieren ingresar a la Policía Metropolitana deben realizar un curso en el Instituto Superior de Seguridad Pública, dependiente del Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires, con una duración de un año. De acuerdo a nuestra fuente entrevistada, la academia no prepara a los agentes en cuestiones técnicas vinculadas a tecnología; respecto del área de Cibercrimen, quienes la integran ya estaban capacitados previamente a su ingreso a la fuerza. Nuestra fuente también destacó un marcado desinterés del personal por aprender y mejorar profesionalmente, esto sumado a que no se recibe capacitación internamente en el área y que, para el caso de querer hacerlo, deben ir a buscarla externamente por sus propios medios.

Ministerio Público Fiscal

Los fiscales juegan uno de los papeles más importantes en la persecución delictual, ya que son ellos quienes deben impulsar judicialmente las investigaciones con la ayuda de sus auxiliares, como las fuerzas policiales. Con la llegada de nuevas tecnologías en las últimas décadas, la labor de investigación fue cobrando nuevos matices que en ocasiones generan más dudas que respuestas concretas. La normativa procesal que durante años brindó pautas claras para el desarrollo de las investigaciones criminales, resulta insuficiente para canalizar el desafío que

presenta el nuevo paradigma tecnológico; y muchas veces aquellas normas deben ser reinterpretadas – con éxito diverso – a fin de sortear dicho desafío.

Para poder actuar acorde al nuevo panorama tecnológico, la Procuración General de la Nación (P.G.N.), que tiene a su cargo el Ministerio Público Fiscal (M.P.F.), comenzó a trabajar desde hace dos años en temáticas de cibercrimen en varios niveles. A nivel MERCOSUR lo hizo a través de la Reunión Especializada de Ministerios Públicos, en la que anualmente se juntan los representantes de los Ministerios Públicos de los Estados miembro para coordinar acciones regionales de cooperación en materia de crimen organizado, además de intercambiar experiencias y prácticas exitosas; y a nivel iberoamericano (Latinoamérica, Portugal y España), a través de IberRed que es una red de cooperación jurídica internacional formada por miembros de los Ministerios de Justicia, Fiscalías, Ministerios Públicos y Poderes Judiciales de los 22 Estados que la componen.

La persona elegida por la P.G.N. para encabezar el trabajo en temas de cibercrimen fue el fiscal Horacio Azzolín, actualmente a cargo de la Unidad Fiscal Especializada en Ciberdelincuencia (U.F.E.CI.), con quien nos hemos entrevistado para entender mejor la posición del M.P.F. en los temas que hacen a este informe.[15]

Actualmente, la tarea principal del M.P.F. en materia tecnológica está orientada a la capacitación de sus fiscales para perfeccionar sus métodos de investigación y enseñar nuevas herramientas con las cuales hacer frente a las actividades delictuales que suceden, sea por completo o en parte, en un entorno digital.

Desde cuestiones básicas como herramientas para comprobar la integridad de archivos descargados de Internet, usar servicios como WHOIS[16] para saber quién registró un sitio web, o entender cómo funcionan los DNS (por sus siglas en inglés, o "Sistema de Nombres de Dominio"), hasta técnicas de investigación para perfeccionar el uso de fuentes abiertas de información en Internet, el uso de software de investigación forense o cómo conservar prueba digital.

El Ministerio Público Fiscal no está desarrollando software propio para sus investigaciones. Para las tareas forenses utiliza en su mayoría productos libres y

[15] Azzolín, Horacio. Entrevista. 23 de octubre de 2015.

[16] ICANN. ¿Qué es WHOIS? https://whois.icann.org/es/acerca-de-whois

gratuitos, y ocasionalmente se adquieren licencias para poder realizar trabajos específicos como el análisis de imágenes forenses (que básicamente es una copia que replica la estructura y contenido de un dispositivo de almacenamiento, como por ejemplo el disco duro de una computadora).

Según nos comentó Azzolín, este panorama lleva a *"plantearte los futuros desafíos de las investigaciones en los próximos años, interceptación de tráfico de Internet en vivo por ejemplo, y otras cuestiones que tienen que ver con cómo se está desarrollando el ecosistema de Internet y de las comunicaciones en este momento del mundo con todo lo que pasa con las comunicaciones cifradas, si es lícito que el Estado descifre con fuerza bruta, si es lícito que el Estado pueda acceder remotamente a la información contenida en un dispositivo a través de lo que es el acceso remoto de datos y para eso utiliza un troyano o alguna forma de intrusión en una máquina, si eso afecta más los derechos que allanar y secuestrar la computadora (...) La Convención de Budapest sobre ciberdelincuencia trabaja, dentro de lo que son las posibilidades de investigación, con el acceso remoto de datos, entonces ahí se empezaron a disparar problemas con cuáles son los estándares para acceder remotamente, si es ético que el Estado utilice estos mecanismos, bajo qué estándares los va a utilizar, quién va a desarrollar ese software de intrusión"*.[17]

Argentina aún está en proceso de adherirse a la convención, por lo que según Azzolín este es el momento más oportuno para avivar la conversación y el debate sobre el uso de este tipo de software por parte del Estado, ¿quién debería tener las facultades para su uso?, ¿los fiscales, las fuerzas policiales, la A.F.I., o -al igual que con las interceptaciones telefónicas- exclusivamente D.I.COM?

"Todo lo que es la investigación en el ámbito digital, fundamentalmente con Internet, genera debates en torno a la invasión de la privacidad" refirió Azzolín, "a lo mejor la revisión de un dispositivo secuestrado con orden judicial, peritado con una copia forense, implica una invasión a la intimidad más fuerte que el propio allanamiento domiciliario, que creo es el estándar más alto de la privacidad protegida constitucionalmente, el cuerpo y la casa, y vos en tu computadora tenés otras cuestiones, hoy tenés tu vida, tus fotos, tus gastos, tus estudios médicos,

[17] Azzolin, Horacio. Entrevista. 23 de octubre de 2015.

datos sensibles, entonces si como Juez tengo que acceder a una computadora, ¿es necesario que acceda a toda esa información? ¿Puedo filtrar lo que estoy buscando? ¿Puedo acceder quirúrgicamente a la información?".[18]

En lo que respecta a capacitación en Derechos Humanos, Azzolín consideró que aún hay mucho por hacer, fundamentalmente con la comunidad técnica, dado que *"el problema por lo general es que, básicamente por la formación y por el mundo en el que viven, se manejan sin límites, no es solamente una falta de conciencia sobre lo que es la noción de derecho humano y el derecho personal como un derecho humano, o la intimidad como derecho humano, sino que no tienen límites en general, no tienen fronteras"*, es la tecnología la que pone el límite, no a la inversa.

Es por este motivo que resaltó *"hay que hacer un puente entre la comunidad técnica y la comunidad jurídica, para explicarles cuáles son los límites (...) hasta dónde están del lado blanco digamos, dónde hay grises y dónde hay negros directamente, porque tal vez un técnico en seguridad informática no entiende o no le importa el tema. Nuestra idea es que si hacemos un ecosistema de Internet más sano, más seguro, más robusto jurídicamente, lo que vos hacés es fomentar el desarrollo, porque Internet fomenta el desarrollo, y con un buen ecosistema el país tiene un clima de crecimiento mejor, por ejemplo, tenés un comercio electrónico que puede crecer, y me parece que es una cuestión de la que el derecho se tiene que ocupar, y no comerse soluciones enlatadas de vigilancia masiva, intrusiones innecesarias (...) el cuidado de la privacidad y la revelación de datos con orden judicial tiene que tener estándares que con el tema de Internet tienen que ser más fuertes"*.[19]

En lo que respecta a interceptación de comunicaciones, sean telefónicas o digitales, el M.P.F. canaliza internamente los pedidos a través del Departamento de Interceptación y Captación de las Comunicaciones. En cuanto a preservación de contenido, opinó Azzolín que *"como está la legislación actual, debe ordenarlo un Juez; lo que es datos de tráfico, me parece, debería poder preservarlo un fiscal, luego sí la revelación de ese contenido debería ser mediante la orden del Juez (...)*

[18] Azzolín, Horacio. Entrevista. 23 de octubre de 2015.
[19] Id.

Lo que estamos trabajando con las prestatarias de servicios es ver qué tecnología tienen para saber que les podemos pedir a futuro en materia de investigaciones".

Situación en las provincias

Al momento de comenzar a analizar el panorama de las policías provinciales, lo primero que surge es que la educación que reciben los miembros de las fuerzas en temas tecnológicos está orientada a los aspectos más básicos de una preparación para llevar a cabo sus funciones como personal oficial, esto es herramientas ofimáticas y cuestiones elementales de computación.

Entre las provincias que se salen de la regla podemos remarcar a Córdoba, Santiago del Estero, Misiones y La Pampa. La Policía de Córdoba ofrece varios convenios educativos con distintas universidades del país para desarrollar una carrera o especialización en temas relacionados a la informática. La Policía de Santiago del Estero tiene una División Informática, la cual está encargada de mantener en óptimas condiciones los equipos de comunicación entre las unidades de la provincia (básicamente trabajo I.T.), mas no es una división de investigación. La Policía de Misiones capacita a sus oficiales en la Escuela Superior de Policía "General D. Manuel Belgrano", que cuenta en su programa con asignaturas de "Seguridad en Telecomunicaciones", "Derechos Humanos", e "Informática aplicada". La Policía de La Pampa suministra capacitación en Informática y Derechos Humanos.

Lo cierto es que el relevamiento efectuado permite inferir que, en el caso de las policías provinciales, la educación está orientada hacia las problemáticas puntuales que enfrenta la provincia respectiva en materia delictual, desde robos hasta tráfico de drogas o trata de personas. Visto en este contexto, la interceptación o vigilancia de comunicaciones queda en un plano secundario, relegado a la ayuda que se puede solicitar a los actores federales.

En el caso de los Ministerios Públicos Fiscales provinciales, la situación resulta similar, siendo el caso de Córdoba una de las excepciones, al contar con un área de cibercrimen. Su labor está orientada al asesoramiento del resto de las fiscalías, buscando que se respeten las garantías y derechos de las personas, alertando cuando una tecnología o método solicitado en una investigación puede vulnerar

derechos humanos. Según una fuente cercana al M.P.F. de Córdoba, que ha solicitado permanecer anónima, el contacto que hay con el resto de los M.P.F. de las provincias es prácticamente nulo, salvo en materia de pornografía infantil debido a convenios para compartir información de investigaciones y capacitación.

Departamento de Interceptación y Captación de las Comunicaciones (D.I.COM)

Uno de los cambios más significativos en el sistema de inteligencia surgió a partir de la ley 27.126 de marzo de 2015, y es la creación del Departamento de Interceptación y Captación de las Comunicaciones (D.I.COM), a cargo de la fiscal Cristina Caamaño, que forma parte de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (D.A.T.I.P.) bajo la órbita del Ministerio Público Fiscal.[20] Con este cambio se habría intentado darle mayor independencia a los funcionarios a cargo del trabajo de las interceptaciones, sacándolas del dominio de la Agencia Federal de Inteligencia.

De esta manera, como bien establece el artículo 17 de la mencionada ley, el D.I.COM. es *"el único órgano del Estado encargado de ejecutar las interceptaciones o captaciones de cualquier tipo autorizadas u ordenadas por la autoridad judicial competente"*.[21] Esto implicó que tanto la A.F.I., las fuerzas federales (Policía Federal Argentina, Gendarmería, Prefectura, Policía de Seguridad Aeroportuaria), Policía Metropolitana y las policías provinciales, en el caso de necesitar intervenir una línea telefónica o cualquier otro tipo de comunicación de un usuario, deben formalizar su pedido judicialmente, para ser luego procesado por D.I.COM., por lo que cualquier otra vía utilizada es ilícita.

El oficio que llega a D.I.COM. debe ser firmado por el Juez, fiscal o secretario autorizado y debe contener *"los datos del juzgado solicitante y su titular, teléfono y correo electrónico oficial, número de causa y carátula del expediente, las*

[20] Procuración General de la Nación. Resolución N° 2067/15. 7 de julio de 2015. Disponible en (PDF): http://www.fiscales.gob.ar/procuracion-general/wp-content/uploads/sites/9/2015/07/PGN-2067-2015-001.pdf

[21] Artículo 17, Ley 27.126 disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

líneas telefónicas y radiales, cuentas de correo electrónico o servicios web que se vinculan a la medida, y el plazo de duración de la medida ordenada".[22] Una vez corroborados estos requisitos, DICOM se encarga de comunicarse con la operadora telefónica o el proveedor de Internet correspondiente para que deriven el contenido al edificio en Av. de los Incas donde será grabado para luego ser enviado al juzgado correspondiente. Según información brindada por la fiscal Caamaño, actualmente se graban aproximadamente 3500 CDs por día.[23]

En D.I.COM. no se accede al contenido de las escuchas. Existen solo dos excepciones:

- en los casos de secuestros extorsivos o privaciones ilegales de la libertad, en los que el Juez solicita al personal de D.I.COM. que escuche directamente para actuar en forma inmediata.
- cuando el Juez designa personal policial para ir a escuchar las líneas de manera directa en las cabinas que tiene D.I.COM. para tal efecto.

Lo mismo ocurre con el contenido de las interceptaciones de las comunicaciones en el entorno digital y de Internet realizadas por el mismo proveedor del servicio (ISPs): D.I.COM. no analiza directamente esa información, sino que el Juez debe pedirle expresamente dicha tarea a D.A.T.I.P. En el caso de los e-mails, D.I.COM. puede pedirlos a los ISP correspondientes (es decir, el webmail de empresas como Telefónica, Telecentro, Fibertel, etcétera), y cuando se trata de empresas extranjeras (Gmail de Google, Outlook de Microsoft, Yahoo Mail, etcétera), D.I.COM. realiza un exhorto directamente a la empresa prestataria del servicio determinado en el pedido del Juez.

En el año 2000, el Juez federal Jorge Urso ordenó el allanamiento del edificio de la ex-D.O.J. que se encontraba en su momento bajo el control de la ex S.I.D.E, en el marco de una investigación por escuchas clandestinas. Los agentes de la entonces S.I.D.E. no permitieron que los policías y peritos pudieran llevar a cabo más que una inspección ocular del lugar y tan solo en una parte del edificio,

[22] MPF. DICOM. Disponible en: http://www.mpf.gob.ar/dicom/
[23] Caamaño, Cristina. Presentación en taller de ADC. 2 de diciembre de 2015.

según se consignó en un artículo del Diario Página 12.[24] En dicho procedimiento pudieron constatar que en aquel edificio terminaban los cables de fibra óptica derivados de las empresas Telefónica y Telecom, a través de los cuales la ex D.O.J. recibía 3780 líneas. Sólo 2380 de esas líneas se encontraban respaldadas por su respectiva orden judicial. Como también lo menciona Gerardo Young, *"Para agilizar las intervenciones, se acordó que las empresas telefónicas debían enviar a la base de Avenida de los Incas un duplicado de la comunicación que les solicitaba la S.I.D.E.. Se hacía a través de un sistema de cableado telefónico, que más tarde sería reemplazado por fibras ópticas, instalado en el subsuelo de la base"*.[25]

Gracias al allanamiento se determinó que la ex S.I.D.E. tenía en el sótano de la base cuatro equipos interceptores marca Siemens. En el acta final del procedimiento se estableció que *"con los equipos que cuenta la D.O.J. no se encuentra en condiciones de intervenir a un abonado en forma directa, sin la anuencia de la compañía prestataria, dependiendo de la conexión que lleve a cargo la empresa prestataria del servicio básico telefónico"*.

En el año 2014, Spiegel Online[26] y Global Voices Advocacy[27] publicaron los resultados de un pedido de acceso a la información pública realizado por el Partido Verde alemán. El objetivo del pedido era conocer la situación de la exportación de tecnologías de vigilancia, de empresas alemanas a gobiernos extranjeros. El gobierno alemán estableció en su respuesta que en el período de 2003 a 2013 había otorgado licencias a empresas para que exporten sus tecnologías a unos 25 países, dentro de los cuales se encontraba Argentina; aunque la participación del gobierno alemán en las transacciones no queda del todo claro, del documento parecería surgir que la participación del gobierno alemán se limitó al otorgamiento de licencias de exportación.

[24] Verbitsky, Horacio. (2000) Diario Página 12. Disponible en: http://www.pagina12.com.ar/2000/00-06/00-06-11/pag03.htm

[25] Young, Gerardo. (2015) Código Stiuso. (Pag. 137) Argentina: Planeta.

[26] Gebauer, Matthias. Meiritz, Annett. Spiegel Online. 22 de agosto de 2014. Disponible en: http://www.spiegel.de/politik/deutschland/deutsche-spaehtechnik-gabriels-ausfuhrkontrollen-bleiben-wirkungslos-a-987555.html

[27] Global Voices Advocacy. 5 de septiembre de 2014. Disponible en: https://advox.globalvoices.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/

En la respuesta brindada por el Ministerio de Economía y Energía alemán, publicada en el blog de Agnieszka Brugger del Partido Verde,[28] se estableció que en los años 2010 y 2011 se exportaron tecnologías a Argentina por un total de 1.183 millones de euros y 169.357 euros, respectivamente.

Si bien la noticia fue receptada por los medios argentinos, desde el Estado Nacional no se dieron explicaciones claras sobre las compras, sus características o destino. Savoia relató en su libro que *"informalmente, algunos funcionarios dejaron saber que ese equipamiento en apariencia había ido a parar a la Secretaría de Inteligencia"*.[29] Caamaño ha comentado públicamente que los equipos que tiene actualmente D.I.COM. datan del 2011, aunque no ha confirmado el nivel de sofisticación de los mismos "por una cuestión de seguridad".[30]

Como la ex-D.O.J. siguió bajo control de la A.F.I. hasta la entrada en funcionamiento del D.I.COM., en forma previa al traspaso la Agencia presidida por Oscar Parrilli llevó a cabo varias tareas de re-estructuración del sistema de inteligencia para hacer más ameno el traspaso a lo que sería la nueva D.I.COM., y así se encargó de hacer una limpieza de la base de escuchas que había en Avenida de los Incas.

"Lo único que nos dejó la A.F.I. fueron 3621 escuchas activas", comentó Caamaño.[31] La primera tarea de la fiscal al mando del D.I.COM. fue comprobar que las mismas tuviesen de respaldo las correspondientes órdenes judiciales. Si bien la fiscal corroboró que esas órdenes existían, el escenario era un poco caótico, con intervenciones que databan de hacía más de 10 años, algunas correspondientes a causas judiciales que se encontraban ya cerradas y otras incluso sin plazo de duración alguno.

Los equipos que dejó la A.F.I en D.I.COM. son las viejas grabadoras que utilizaba la ex S.I.D.E.. Actualmente D.I.COM. se encuentra intentando desarrollar su propia tecnología, de origen nacional. Para este fin se creó el Equipo de Desarrollo

[28] Ministerio de Economía y Energía alemán. Agosto de 2014. Disponible en (PDF): https://www.agnieszka-brugger.de/fileadmin/dateien/Dokumente/Abruestung/Ruestungsexporte/20140808_Antwort_KA_Spaehsoftware_Drs

[29] Savoia, Claudio. (2015) Espiados. Argentina: Planeta (Pag. 220)

[30] Caamaño, Cristina. Presentación en taller de ADC. 2 de diciembre de 2015.

[31] Caamaño, Cristina. Entrevista. 4 de diciembre de 2015.

Tecnológico, integrado por representantes del Ministerio de Ciencia, Tecnología e Innovación Productiva, de la Facultad de Ciencias Exactas y Naturales y la Facultad de Ingeniería de la Universidad de Buenos Aires, de la Facultad de Informática de la Universidad de La Plata, del Instituto Nacional de Tecnología Industrial del Ministerio de Industria (INTI), de la Empresa Argentina de Soluciones Satelitales (ARSAT) y de Investigación Aplicada (INVAP).[32]

El objetivo de esta iniciativa es tener tecnología enfocada a las necesidades del Departamento, con la posibilidad de ser actualizadas rápidamente acorde a las innovaciones tecnológicas, además de poder unificar su uso con las operadoras de telefonía y proveedores de Internet.

Pero la tecnología no fue lo único que quedó de la ex-SIDE en la actual D.I.COM. Un gran porcentaje de los empleados que quedaron durante la transición venían de la agencia de inteligencia, *"no podíamos reemplazar a todos con gente de la Procuración, (...) necesitábamos capacitación. Pero los que quedaron son trabajadores, ningún jefe o empleado de alto rango"*, estableció Caamaño,[33] quien a partir del 9 de diciembre de 2015 comenzó a sacar a los empleados que venían de la ex-SI, con el objetivo de eliminar el perfil de inteligencia del personal de D.I.COM., ya que su necesidad se centra en personal de tipo administrativo.

Actualmente D.I.COM. cuenta con 24 delegaciones en varias de las provincias del país, que tienen prohibido realizar escuchas directas. Al momento de redactar este informe, D.I.COM. se encontraba evaluando el cierre de estas delegaciones, a fin de concentrar la actividad en el edificio de Avenida de los Incas y facilitar el control de los procedimientos para las interceptaciones.

En diciembre de 2015 se publicó el primer informe de gestión del D.I.COM., correspondiente al período julio-diciembre, que puede consultarse en el sitio web de la P.G.N.[34] A partir de febrero de 2016, el Departamento comenzaría a publicar

[32] Procuración General de la Nación. 16 de septiembre de 2015. Disponible en: http://www.fiscales.gob.ar/procuracion-general/primera-reunion-del-equipo-de-desarrollo-tecnologico-para-el-departamento-de-interceptacion-y-captacion-de-comunicaciones/

[33] Martinez, Diego. Página 12. 6 de septiembre de 2015. Disponible en: http://www.pagina12.com.ar/diario/elmundo/4-281042-2015-09-06.html

[34] Informe de Gestión. Procuración General de la Nación. 23 de diciembre de 2015. Disponible en: http://www.fiscales.gob.ar/procuracion-general/el-departamento-de-interceptacion-y-captacion-de-las-comunicaciones-presento-su-informe-de-gestion/

reportes mensuales con información sobre la cantidad de solicitudes de conexión, los tipos de delitos a los que responden las interceptaciones y los tiempos de escucha.

Fuerzas Armadas

Si bien las Fuerzas Armadas no tienen facultades para desarrollar tareas vinculadas a ciberseguridad o inteligencia interior, sí las tienen para efectuar tareas vinculadas a ciberdefensa.

Mediante Resolución Nº 343/2014 del Ministerio de Defensa se creó el Comando Conjunto de Ciberdefensa, cuya misión – según detalla el artículo 3 de dicha Resolución – es *"ser capaz de conjurar y repeler ciberataques contra las infraestructuras críticas de la información y los activos del Sistema de Defensa Nacional y de su instrumento militar dependiente"*.

No es objetivo de este trabajo analizar las tareas de ciberdefensa a cargo de las Fuerzas Armadas, sino que la mención de la creación del Comando Conjunto y las entrevistas que realizamos a personal allegado a esta unidad nos permitió acceder a información relativa a la formación y capacitación que recibe el personal de las Fuerzas Armadas en temas vinculados al entorno digital.

Así sabemos que el personal asignado a ciberdefensa se capacita mediante cursos que brinda la organización A.D.A.C.S.I. (Asociación de Auditoría y Control de Sistemas de Información, o por sus siglas en inglés I.S.A.C.A.) filial 15, que corresponde al capítulo argentino de esta organización internacional.

La formación también incluye cursos en institutos universitarios del Ejército y de la Fuerza Aérea. En el Instituto del Ejército se realizan curso de posgrado en Criptografía y Seguridad de la Información, y en el Instituto de la Fuerza Aérea se realizan cursos de posgrado de Seguridad Informática.

También se encuentra en trámite de aprobación ante la CONEAU (Comisión Nacional de Evaluación y Acreditación Universitaria) la Maestría en Ciberdefensa, planificada por las Fuerzas Armadas.

IV Conclusiones

Como mencionamos anteriormente, intentar responder a la pregunta relativa a la formación que reciben los funcionarios o agentes encargados de realizar tareas de vigilancia e investigación en el entorno digital nos generó mucha incertidumbre y, quizás, una única certeza, que es la absoluta informalidad y precariedad que en general caracterizan a la formación o capacitación que reciben estos agentes y funcionarios, con excepción de algún caso aislado.

Esta circunstancia condicionó, por decirlo de alguna manera, la suerte de este informe, que terminó siendo un abordaje más bien exploratorio, producto de una recopilación casi artesanal de distintos elementos, atento la falta de información sistematizada.

De tal suerte, a modo de conclusión, podemos identificar las siguientes características:

- La educación que reciben los agentes y personal dedicado a la inteligencia, a la persecución y a la investigación de delitos es en términos generales, sumamente informal, sin una base institucional fuerte.
- La temática de las tecnologías de la información y entorno digital ha sido receptada por las fuerzas de seguridad, armadas y de inteligencia, y por organismos de investigación criminal, en forma incipiente.
- La problemática derivada de esta recepción incipiente parece estar siendo resuelta a medida que los diversos sucesos van aconteciendo, sin haber una planificación cabal de su enseñanza y desarrollo.
- Los programas de enseñanza y formación adolecen de una falta total de adecuación a la realidad que los funcionarios y agentes deben enfrentar en el entorno virtual.
- En general la formación que reciben estos agentes y funcionarios no contiene una perspectiva respetuosa de Derechos Humanos.

De lo dicho hasta aquí, consideramos que existe un enorme trabajo por hacer, tendiente a capacitar en forma adecuada a los funcionarios y agentes encargados de realizar tareas de vigilancia e investigación en el entorno digital.

Sería apropiado entonces actualizar las programas de enseñanza, incorporando una fuerte impronta consagratoria de Derechos Humanos, para lo cual podría resulta una guía adecuada los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[35]

Si bien los 13 Principios deben ser considerados en forma holística, cuando hablamos de educación en el ámbito de la inteligencia y la vigilancia, hay dos principios que poner de resalto.

Por un lado, el principio de transparencia. Actualmente una gran parte del sistema de inteligencia, incluyendo en gran parte a la E.N.I., sigue funcionando bajo reserva o secreto. El alto grado de secretismo que impregna a todo el sistema de inteligencia en el país, sólo sirve para ocultar la ineficacia y las deficiencias del mismo, e impedir que la ciudadanía conozca el funcionamiento del sistema.

Por otro lado, es fundamental el principio de la supervisión pública. Como ha concluído previamente ADC en su informe titulado "**Quién vigila a quienes vigilan**",[36] la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia del Congreso de la Nación trabaja bajo un paradigma de secreto excesivo que ha impedido, entre otras cuestiones, saber si funciona como indica la ley, o si simplemente funciona, de lo que puedo colegirse – al menos en los hechos – la falta de adecuada supervisión o control externo.

Las instancias de formación y capacitación de los agentes y funcionarios aparecen como las más adecuadas para el saneamiento de prácticas de vigilancia e investigación reñidas con la ley, como así también para incorporar conocimientos y saberes alineados con una perspectiva respetuosa de garantías y libertades fundamentales.

[35] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. 10 de mayo de 2014. Disponible en: https://es.necessaryandproportionate.org/text

[36] ADC. Quién vigila a quienes vigilan. Mayo de 2014. Disponible en (PDF): http://www.adc.org.ar/2013/wp-content/uploads/2014/06/2014-05-Quien-Vigila-pp.pdf

V Comentario final

Es importante mencionar que a la finalización de este documento, las autoridades nacionales se encontraban evaluando dos medidas que de llevarse adelante afectarían en alguna medida el contenido de este informe:

- El traspaso del D.I.COM. desde el Ministerio Público Fiscal a la órbita de la Corte Suprema de Justicia de la Nación.
- El traspaso de la Policía Federal Argentina a la Policía Metropolitana, unificando ambas fuerzas policiales bajo la dirección de esta última.