NUEVAS CAPACIDADES DEL ESTADO MEXICANO PARA LA INVESTIGACIÓN DE LA DELINCUENCIA CIBERNÉTICA DE CARA A LA CONVENCIÓN DE NACIONES UNIDAS

Jonathan LÓPEZ TORRES[1]
Ricardo SALGADO PERRILLIAT[2]

El 24 de junio de 2025, la Presidenta de México publicó en el Diario Oficial de la Federación el nuevo Reglamento Interior de la Secretaría de Seguridad Pública y Protección Ciudadana, a cargo del Secretario Omar García Harfuch (en adelante, el Reglamento), que reemplaza el publicado en el Diario Oficial de la Federación del 30 de abril de 2019 y establece una nueva arquitectura institucional para la investigación de la delincuencia cibernética en México.

I. ¿QUÉ CAPACIDADES INSTITUCIONALES SE CREAN?

De contar sólo con una Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico en 2019 para garantizar la ciberseguridad al interior de la Secretaría, ahora el nuevo Reglamento Interior de la Secretaría de Seguridad Pública y Protección Ciudadana crea la Unidad de Inteligencia, Investigación Cibernética y Operaciones Tecnológicas, con 3 direcciones generales adscritas:

1. Dirección General de Investigación Cibernética
2. Dirección General de Operaciones Aéreas y Tecnológicas
3. Dirección General Forense Digital

II. ¿CON QUÉ ATRIBUCIONES CONTARÁ LA UNIDAD DE INTELIGENCIA, INVESTIGACIÓN CIBERNÉTICA Y OPERACIONES TECNOLÓGICAS?

Esta Unidad tiene un perfil directivo que coordinará a las 3 Direcciones Generales de Investigación Cibernética, Operaciones Aéreas y Tecnológicas, así como a la Forense Digital, y contará con diversas atribuciones que se resumen a continuación:

a) *Prevención:* coordinará la implementación de las políticas y procedimientos para difundir acciones preventivas destinadas a la identificación y denuncia de los delitos cibernéticos.

b) *Diseño de herramientas para la investigación:* diseñará, dirigirá la implementación y aplicará técnicas, métodos y estrategias de investigación de los hechos y recopilación de los indicios digitales y tecnológicos.

1 Profesor de la Asignatura de Investigación de Delincuencia Cibernética en INFOTEC y autor del libro *Ciberespacio & Ciberseguridad. Elementos Esenciales*, Tirant lo Blanch, 2020.

2 Titular de la Unidad de Asuntos Jurídicos del Tribunal Federal de Justicia Administrativa.

c) *Planeación:* establecerá líneas de investigación policial en materia de ciberseguridad a partir del análisis e identificación de los modos de operación de las personas presuntamente responsables, así como de organizaciones delictivas y sus estructuras.

d) *Análisis de sistemas y equipos:* realizará el análisis técnico de sistemas y equipos informáticos, así como de telecomunicaciones que hayan sido utilizados para reproducir, sustraer, destruir, modificar o alterar información, con el fin de recuperar datos y obtener evidencia relacionada con el delito cometido y, en su caso, proceder a poner dicha información a disposición de las autoridades competentes.

e) *Alertas de ciberseguridad:* generar alertas de ciberseguridad relacionadas con los modos de operación de personas o grupos que emplean métodos electrónicos u otras plataformas tecnológicas para la probable comisión de delitos.

f) *Operativos para operaciones tecnológicas:* ejecutar operaciones tecnológicas y coordinar operativos conjuntos con otras autoridades de los tres órdenes de gobierno en la atención de hechos presuntamente constitutivos de delitos.

III. ¿QUÉ ATRIBUCIONES TENDRÁN LAS DIRECCIONES GENERALES ADSCRITAS A LA UNIDAD DE INTELIGENCIA, INVESTIGACIÓN CIBERNÉTICA Y OPERACIONES TECNOLÓGICAS?

La principal atribución de la *Dirección General de Investigación Cibernética* será coadyuvar con las autoridades competentes en la investigación de delitos cibernéticos e ilícitos cometidos con la utilización de medios electrónicos y tecnológicos.

En lo que respecta a la *Dirección General de Operaciones Aéreas y Tecnológicas* sus principales atribuciones consistirán en implementar sistemas y procedimientos tecnológicos especializados para el combate a la delincuencia; vigilar, ubicar y localizar personas y vehículos con equipos tecnológicos que operen con datos georreferenciados, y realizar actividades de reconocimiento aéreo para el apoyo a las investigaciones y a la persecución de hechos presuntamente constitutivos de delitos.

Por su parte, la *Dirección General Forense Digital* tendrá las atribuciones de operar procedimientos para la obtención de información en laboratorios, a través de herramientas y software especializados a efecto de procesar los indicios, evidencias y demás medios de prueba; establecer mecanismos de análisis forense; coordinar la obtención de información digital contenida y almacenada en dispositivos y medios electrónicos, así como colaborar en la fijación, levantamiento y embalaje de indicios y evidencias, con el objetivo de obtener elementos relacionados con hechos delictivos.

IV. ¿CON QUÉ HITOS EMPATA EL NUEVO REGLAMENTO?

El Reglamento empata con diversos hitos nacionales e internacionales que son los siguientes:

a) *Reforma constitucional en materia de seguridad pública 2024:* con una reforma al Artículo 21 constitucional publicada en el Diario Oficial de la Federación el pasado 31 de diciembre de 2024, se estableció a nivel constitucional que, la investigación de los delitos no sólo corresponde al Ministerio Público, sino a la secretaría del ramo de seguridad pública del Ejecutivo Federal, a la Guardia Nacional y a las policías, en el ámbito de su competencia, las cuales actuarán bajo la conducción y mando del Ministerio Público Federal.

b) *Reformas a la Ley Orgánica de la Administración Pública Federal 2024:* con una reforma publicada en el Diario Oficial de la Federación el pasado 28 de noviembre de 2024, se estableció que a la Secretaría de Seguridad y Protección Ciudadana le compete realizar, de acuerdo con lo establecido en el Artículo 21 constitucional, funciones de seguridad a cargo de la Federación, para cuyo fin deberá organizar, dirigir y supervisar las instituciones bajo su adscripción para realizar la investigación y persecución de delitos basada en inteligencia, información estratégica, análisis, colaboración, práctica de operaciones especiales y aprovechamiento de la tecnología informática, para generar y aportar mayores elementos de prueba que originen y fortalezcan carpetas de investigación ministerial, con la finalidad de que los indicios, datos y pruebas que se recaben sean admisibles en juicio con plena sujeción a los derechos humanos y libertades fundamentales, en coordinación con la Fiscalía General de la República y las dependencias competentes conforme a las disposiciones jurídicas aplicables.

c) *Estrategia Nacional de Seguridad Pública 2024-2030:* publicada en el Diario Oficial de la Federación el pasado 13 de mayo de 2025, la Estrategia Nacional de Seguridad Pública 2024-2030 contiene y desarrolla ejes, objetivos, líneas de acción y acciones estratégicas para garantizar la seguridad en México a nivel nacional. Esta estrategia tiene un punto relevante: reconoce la existencia de la delincuencia cibernética y establece 3 acciones en 2 objetivos estratégicos.

   El primero, el objetivo 3.2 consistente en "Neutralizar a los objetivos generadores de violencia y redes criminales que operan en el territorio nacional". Dentro de este objetivo, el Poder Ejecutivo Federal estableció 2 acciones estratégicas relacionadas con la delincuencia cibernética:

   - *Acción 3.2.1.3.* Colaborar con las instancias competentes en el rastreo, análisis y preservación de evidencia digital, que contribuya a la prevención e investigación de delitos cibernéticos.

- *Acción 3.2.2.3.* Realizar acciones de análisis de información e investigación de ciberdelitos a través del monitoreo, vigilancia, identificación y el rastreo en la red pública de Internet, así como generar alertas de ciberseguridad y gestionar la baja de contenidos o sitios que representen riesgos, amenazas o peligros para la seguridad ciudadana.

El segundo, el objetivo 4.1 consistente en "Establecer mecanismos de coordinación entre diversas dependencias de los tres órdenes de gobierno relacionadas con la seguridad pública". Dentro de este objetivo, a las autoridades de seguridad pública le fijaron la siguiente acción:

- *4.1.3.3* Coordinar acciones operativas en las fronteras norte y sur del país, para la prevención de delitos cibernéticos y/o basados en el uso de la tecnología.

d) *Convención de las Naciones Unidas contra la Ciberdelincuencia:* adoptada por la Asamblea General de las Naciones Unidas el 24 de diciembre de 2024 y que se abrirá a firma en octubre de 2025 en Vietnam, esta Convención parte de que las tecnologías de la información y las comunicaciones, si bien tienen un enorme potencial para el desarrollo de las sociedades, crean nuevas oportunidades para la delincuencia, pueden contribuir al aumento del número y la diversidad de las actividades delictivas y pueden tener un efecto adverso en los Estados, las empresas y el bienestar de las personas y de la sociedad en su conjunto.

   Esta Convención surge de la necesidad de aplicar, con carácter prioritario, una política en materia de justicia penal de alcance mundial con objeto de proteger a la sociedad de la ciberdelincuencia a través, entre otras cosas, de la adopción de la legislación adecuada, el establecimiento de delitos y facultades procesales comunes y el fomento de la cooperación internacional para prevenir y combatir más eficazmente esas actividades en los planos nacional, regional e internacional, buscando negar refugios seguros a quienes se dedican a la ciberdelincuencia persiguiendo estos delitos dondequiera que se produzcan.

Como podrá observarse, existen diversos hitos estratégicos y relevantes entorno al combate a la delincuencia cibernética tanto en México como a nivel internacional, por lo que se requiere un andamiaje jurídico nacional y transnacional que brinde una respuesta clara y contundente a la investigación y procesamiento de la delincuencia cibernética en México.

V. ¿QUÉ RETOS SE TIENEN PARA GARANTIZAR UNA VERDADERA JUSTICIA PENAL EN EL CIBERESPACIO?

Si bien los enfoques del Poder Ejecutivo Federal en materia de delincuencia cibernética son claros y positivos: la prevención y la investigación. Sin duda, se requiere una agresiva promoción de educación para prevenir la delincuencia cibernética como herramienta *ex – ante*. Pero no basta con prevenir, el Estado debe reaccionar de forma contundente e integral ante cualquier delito de delincuencia cibernética o que haga uso de cualquier tecnología o de las telecomunicaciones.

Para ello, el modelo que pretende instaurar la estrategia del Poder Ejecutivo Federal debe encuadrar y cumplir con el siguiente principio general del proceso de justicia penal: el proceso penal tendrá por objeto el esclarecimiento de los hechos (en, a través o fuera del ciberespacio), proteger al inocente, procurar que el culpable no quede impune y que los daños causados por el delito se reparen. Esto conforme a lo siguiente:

a) *Esclarecimiento de los hechos:* no hay actividad humana que no deje un rastro digital. Todas las interacciones humanas se dan en o a través de tecnología, telecomunicaciones y/o dispositivos. Los delincuentes usan la tecnología y cada vez en mayor medida. Por tanto, el Internet, las telecomunicaciones y los dispositivos pueden brindar amplia, abundante y diversa información que permita el esclarecimiento de hechos delictivos.

b) *Proteger al inocente:* los únicos que se oponen al uso de la tecnología para la investigación penal son aquellos quienes no han sido víctimas de un delito o del miedo de la inseguridad. El Estado no debe escatimar esfuerzos en proteger a los inocentes de los delitos que hacen uso de la tecnología para su comisión.

   Si cada avance en la materia se detiene por la percepción errónea del uso de la tecnología para la investigación penal, es como si al delincuente lo dejaran correr los 100 metros planos, y al Estado y a la población nunca los dejaran salir de la meta. En este momento, nosotros seguimos en la meta y ellos ya tienen su medalla.

   Pensemos en los inocentes que pierden el dinero de sus cuentas bancarias porque robaron su identidad (recursos que pudieron ser sus ahorros, sus salarios o el dinero para una emergencia); pensemos en las adolescentes o las mujeres a quienes destrozan sus vidas porque difundieron sus imágenes o videos íntimos; pensemos en quienes no tienen trabajo y los contactan por redes sociales para ofrecerles créditos y los estafan; pensemos en las empresas a quienes paralizan los ataques cibernéticos; pensemos en el robo de propiedad intelectual para ventajas anticompetitivas en los mercados; pensemos en

todos y a futuro. La tecnología es una gran herramienta a disposición del Estado para proteger a los inocentes.

c) *Procurar que el culpable no quede impune:* la impunidad es tal en el ciberespacio en México que no tenemos cifras oficiales sobre su incidencia delictiva y los casos que se denuncian no llegan a los tribunales para su sanción, basta ver en el Semanario Judicial de la Federación la ausencia de criterios judiciales sobre delincuencia cibernética.

d) *Que los daños causados por el delito se reparen:* es necesario contar con una investigación penal de la delincuencia cibernética fuerte, profesional y contundente para procesar estos delitos y aspirar a una reparación de los daños causados en el entorno más complejo para la justicia penal: el ciberespacio.

VI. CONCLUSIONES

Para todo lo anterior, son y serán muy positivos los esfuerzos de la Secretaría de Seguridad Pública y Protección Ciudadana para la investigación de la delincuencia cibernética, pero necesitan cambios de este nivel en el Ministerio Público Federal y los Ministerios Públicos de las entidades federativas, a efecto de contar con fiscales que entiendan de tecnología y telecomunicaciones y su regulación, dominen las técnicas de investigación penal, sean impecables en sus expedientes y procedimientos, sepan desahogar pruebas digitales, tengan destreza en los juicios orales para defender sus pruebas, tengan casos muy bien armados y sepan cómo defender sus asuntos en los procedimientos jurisdiccionales.

Que se garantice la justicia penal en el ciberespacio…