POR: DR. JUAN FRANCISCO SAHAGÚN ARIZAGA

"El Nuevo Sistema Nacional de Inteligencia, la Ofensiva de FinCEN y la Evolución Forzosa del Oficial de Cumplimiento en México"

México está enfrentando una transformación estructural sin precedentes en la historia contemporánea del país, ya que estamos viviendo un verdadero cambio del paradigma tradicional en las materias de seguridad pública, fiscalización y prevención de lavado de dinero, que hasta 2025 parecía que eran materias independientes unas de las otras, sin consecuencias entre ellas y completamente desconectadas, que además separaba administrativamente la función de prevención del delito (policía administrativa) de la función de investigación y persecución de los delitos (ministerio público federal), para transitar hacia un innovador modelo que podemos anticipadamente denominar "*policía de inteligencia*".

Esto se detona por la reciente reforma al artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, y de la misma se generó la expedición de la **Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNIIMSP)**, publicada el 16 de julio de 2025, que traa aperejado nuevos este nuevo riesgos existenciales para la emrpesa y el empresario en México, debido al nuevo paradigma de la "Inteligencia Fiscal – Financiera y Corporativa" en manos de la Secretaría de Seguridad y Protección Ciudadana.

La principal incorporación de estas nuevas herramientas legales con las que ahora cuentan diversas Dependencias de la Administración Pública Federal mexicana, es que la información que obtienen, gestionan y procesan, puede ser interpretada, no como una infracción fiscal subsanable, sino como un indicador de inteligencia criminal vinculado a delitos de alto impacto como el lavado de dinero o el financiamiento al terrorismo.

La modificación sustancial del artículo 21 constitucional, consolidada a finales de 2024, rompe con el monopolio de la investigación típico o tradicional que recaía en la figura a del Ministerio Público Federal y de la Policía Investigadora, ambos adscritos al Fiscalía General de la República, dado que ahora también se faculta explícitamente a la Secretaría de Seguridad y Protección Ciudadana (SSPC) para formular, coordinar y dirigir la Estrategia Nacional de Seguridad Pública, por lo que se les permite realizar investigaciones, obtener evidencia y poderla utilziar en contra de los investigados en diversas acusasiones o procesos penales federales. Aunado a lo anterior a la Guardia Nacional expresamente se le facultó para realizar investigaciones de delitos, recabar información y generar "inteligencia" que servirá como "dato de prueba" en los procesos judiciales.

Sin duda esta reforma constitucional, es de gran calado, dado que lo que se plasmó en la Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNIIMSP), es la dualidad de las investigaciones de las diversas autoridades federales, dado que ahora tenemos instalado en nuestro sistema jurídico, una investigación de carácter administrativo-fiscal desarrollada por el Servicio de Administración Tributaria (SAT), y otra de carácter "*inteligencia criminal*" desarrollado por la Secretaría de Seguridad y Protección Ciudadana (SSPC), siendo investigaciones que impacatarán en la esfera jurídica de las empresas y empresarios, cuando sus niveles de cumplimiento sean laxos.

Desde el punto de vista técnico procesal – penal, es fundamental entender que de ahora en adelante el valor probatorio de la "inteligencia" cambia radicalmente, dejan de ser considerados como meros "*indicios*", pasando a ser el resultado de las investigaciones desarrolladas por la Secretaría de Seguridad y Protección Ciudadana como "*productos de inteligencia*"[1], para luego ser "*datos de prueba*", tienendo entonces la capacidad de sustentar con mayor eficacia los procesos judiciales en favor del Gobierno, lo que eleva el estándar de riesgo para la defensa corporativa y minimiza las posibilidades de éxito desde el punto de vista de la defensa penal, haciendo esto que entonces y de manera inversamente proporcional las empresas cambien la óptica defensiva, por una óptica de prevención y mitigación de riesgos legales, a través de sistemas de gestión de cumplimiento.

Otro de los aspectos más disruptivos de la Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNIIMSP), es el mandato de interconectar los sistemas de inteligencia de la Federación con las entidades federativas y los municipios, e inclusive, con entes privados[2]. La información estará siendo compartida en tiempo real, resaltando que ya no hay distingo entre información pública y privada, generando una capacidad de obtener datos e información de cualquier clase o categoría en tiempo real, justificando todo esto en el concepto "seguridad pública", mininizando la protección de datos personales, pero más aún violentando los Derechos Humanos de última generación de todos los investigados y prácticamente reduciéndolos a la nada.

A partir de la entrada en vigor de la Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNIIMSP), las empresas concesionarias de telecomunicaciones, servicios financieros y tecnología financiera (Fintech) se convierten, *de facto*, en obligados proveedores de información para el Sistema Nacional, lo que le permitirá a la Secretaría de Seguridad y Protección Ciudadana (SSPC) recabar, compilar y procesar información para crear bases de datos criminalísticos, lo que en la práctica significa que los registros corporativos, transaccionales y de geolocalización pueden ser integrados a la "nube" de inteligencia del Estado, sin necesidad de una orden judicial.

De conformidad con los artículos 5 y 45 de la Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNIIMSP), se establece la obligación de interconectar todas las bases de datos del Estado, generando a favor de la Secretaría de Seguridad y Protección Ciudadana (SSPC) el *Big Data Estatal (*datos fiscales, datos financieros, datos patriminiales, datos de seguridad*)*, aunado al uso de la IA, para ser analizados, procesados y utilizados como **notitia criminis** o **datos de prueba,** para fundar y motivar actos de molestia (cateos, intervenciones telefónicas, congelamiento de cuentas), en términos del Código Nacional de Procedimientos Penales. Sin embargo, para que tengan valor en una sentencia, deben desahogarse en juicio oral mediante la comparecencia de los analistas o agentes que los generaron, sometiéndose al contradictorio.

[1] Debemos aclarar que estos "productos de inteligencia" serán incorporados a las Carpetas de Investigación como "datos de prueba", que deben ser perfeccionados para alcanzar el valor probatorio en juicio.
[2] Ante cualquier requerimiento de información financiera por parte de autoridades administrativas (no judiciales), se debe evaluar la interposición del Amparo, citando la tesis 1a./J. 188/2025 (11a.) , para proteger la esfera jurídica de la empresa y evitar responsabilidad civil frente a clientes o terceros.

El Oficial de Cumplimiento debe asumir que la autoridad tiene un mapa completo de las relaciones de su empresa (clientes, proveedores, socios, partes relacionadas), en tiempo real, y tiene que reconstruir su mapa de riesgos considerando este importante factor.

Considero que otro gran peligro al que nos enfrentamos, es que la autoridad utilice la "inteligencia" para obtener pruebas ilícitas (ej. acceso a cuentas sin orden judicial) y luego las "blanquee" a través de un hallazgo inevitable o fuente independiente en la carpeta de investigación.

Otra situación que debemos tener en cuanta como abogados de empresa u oficiales de cumplimiento, es el hecho de que no existe manera de controvertir los "productos de inteligencia" en la vía administrativa, en términos de lo dispuesto por la Ley Federal del Procedimiento Administrativo, simple y sencillamente por que no se contempla dicha posibilidad legal, pero además por que se obtienen bajo la justificación de la "seguridad pública" y materialmente es información que, en un primer momento, será confidencial y no será compartida por el gobierno con ningún ente investigado, por lo que esto necesariamente conllevará la indefensión administrativa. Sin duda, una vez que estos "productos de inteligencia" sean llevados u ofrecidos como evidencia en juicio, se podrán objetar, controvertir o oponer según los remedios que ofrece el propio Código Nacional de Procedimientos Penales y/o la Ley de Amparo.

Toda esta nueva tendencia de obtención de información, que ahora se le denomina "inteligencia", otorga la posibilidad del acceso a información personal, geolocalización, datos fiscales e información de cualqueir categoría, sin control judicial previo, lo que desdes nuestro punto de vista viola el "núcleo duro" de los derechos humanos protegidos por la Constitución y los tratados internacionales de los que el Estado Mexicano es parte, llevando a la indefectible conclusión de que la Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNIIMSP) permite una intromisión arbitraria en la vida privada bajo conceptos vagos de "inteligencia estratégica" o "mantenimiento del orden".

En específico la Secretaría de Seguridad y Protección Ciudadana (SSPC), ahora tiene la capacidad de solicitar información de manera directa a instituciones bancarias, fiscales y registrales para el esclarecimiento de hechos delictivos; generar sus propios "*productos*", no dependiendo de lo que la Unidad de Inteligencia Financiera (UIF) le comparta, por ejemplo, ya que ahora cuenta con sus propias Unidades de Análisis Financiero y Patrimonial para investigar las estructuras económicas de las organizaciones criminales; y finalmente tiene la facultad de hacer la coordinación operativa, dirigiendo las acciones de la Guardia Nacional y policías estatales, en operativos de lavado de dinero, extinción de dominio y aseguramiento de activos.

Paralemante la Guardia Nacional, misma que forma parte de la Secretaría de la Defensa Nacional, ha evolucionado al concepto de "Policía Científica y Cibernética", esto a travñes de la Dirección General Científica (Guardia Cibernética), que ahora tiene facultades expresas para el monitoreo de la red pública de internet, el análisis forense digital y la investigación de delitos financieros cometidos a través de medios electrónicos. Lo anterior, sin lugar a

dudas hace concluir que la Guardia Nacional tiene una participación verdaderamente activa en la vigilancia y escrituio en el ciberespacio coporativo, pudiendo traducir toda la data obtenida en el ciberespacio, redes sociales, foros, transacciones digitales, correos electrónicos, etc, en "*productos de inteligencia*", buscando patrones de lavado de dinero, defraudación fiscal, financiamiento al terrorismo, compra y venta de comprobantes fiscales, etc., pudiendo ser llevados a juicio, utilizandolos contra la empresa y/o el empresario, y más aún pudiendo compartir dicha información con agencias internacionales como FBI, Interpol, DEA, Departamento del Tesoro de los EEUU, etc, para el rastreo de criptoactivos y flujos financieros transfronterizos.

En este sentido la figura del "secreto bancario y fiscal" se volverá en mucho casos, difícil de aplicar, nuevamente bajo el argumento de la "seguridad pública", ya que la reforma permite a la SSPC acceder a información "de que dispongan" otras dependencias, como se ha mencionado en repetidas ocasiones, sin control judicial, pudiendo solicitar y obtener información tanto del Servicio de Administración Tributaria (SAT), como de la Comisión Nacional Bancaria y de Valores (CNBV), sin restricción alguna. No obstante, no debemos olvidar el 21 de mayo de 2025 la Prmera Sala de la Suprema Corte de Justicia de la Nación, al resolver el Amparo en Revisión 119/2025, estableció un precedente vital para la defensa corporativa, ya que esta sentencia declaró la inconstitucionalidad del artículo 142, fracción II de la Ley de Instituciones de Crédito, que permitía a Fiscalías estatales solicitar información bancaria sin orden judicial. En esta resolución la Corte determinó que el derecho a la privacidad y protección de datos personales, prevalecen sobre la facultad investigadora administrativa, y que para acceder a datos bancarios es necesaria la autorización del Juez de Control. En ese sentido, consideramos que la SSPC debe, en estos casos, solicitar autorización al Juez de Control, situación que de suyo se antoja difícil en la práctica que lo haga, sin embargo si actúa excesivamente al autoridad encargada del Sistema Nacional de Seguridad Pública, entonces tendremos argumentos defensivos.

Todo lo antes expuesto no lleva a generar una conclusión contundente: nos encontramos en un esencario jurídico de clara indefensión para los contribuyentes, ya que ahora las investigaciones pueden tomar un camino no solo de investigación administrativa, sino que se pueden derivar en investigaciones de carácter penal, por los "*productos de inteligencia*" obtenidos, por ejemplo, el SAT podría iniciar una auditoría fiscal, dar aviso a la SSPC y esta iniciar una investigación por lavado de dinero, generando duales investigaciones, pudiendo tener consecuencias catastróficas para las empresas en México, dado que podrían ser sujetas a dobles sanciones (administrativas y penales), por los mismos hechos, dejando en entre dicho el principio constitucional *Ne Bis In Idem.*[3]

Lo más preocupante es que se está replicando a nivel local este "sistema" o "paradigma" de seguridad pública, con una velocidad vertiginosa. Ya se han aprobado reformas en el Estado de México, Chihuahua y Sinaloa, en donde ya se han dotado a las Secretarías de Seguridad Estatales de facultades de investigación, análogas a las federales, esto bajo el principio de "federalismo cooperativo", con lo cual una empresa con operaciones nacionales debe lidiar

[3] No se trata solo de evitar la "doble sanción", sino de evitar el **"Procedimiento Paralelo Inquisitivo"**. Si la autoridad usa la coacción administrativa para obtener una confesión o prueba de cargo para el proceso penal, se viola el derecho a la no autoincriminación. El Oficial de Cumplimiento debe blindar la entrega de información en auditorías fiscales, pensando siempre en su potencial uso en un juicio oral penal.

no solo con la SSPC federal, sino con el sistema estatale de inteligencia de su propio Estado, que además puede tener criterios de investigación dispares y niveles de profesionalización de los funcionarios estatales dudosos.

En el entorno globalizado que ahora vivimos en el mundo, no podemos dejar de ver tampoco los lineamientos que se vas dando desde nuestro vecino del norte, Estados Unidos, ya que el Departamento del Tesoro, a través de FinCEN, va dictando los lineamientos en prevención de lavado de dinero, así como lista las personas fisicas o morales relacionadas con el tráfico de drogas y el lavado de dinero. Claro ejemplo de esto, fue que en junio de 2025 invocó las facultades de la Ley FEND Off Fentanyl y la Sección 311 de la *USA PATRIOT Act* para designar a tres instituciones financieras mexicanas como "preocupaciones principales de lavado de dinero", por lo que con este ejemplo la empresa mexicana tiene que tener bastante claro que lo que se va dictando en los EEUU tiene un impacto directo en el ecosistema empresarial mexicano, obligado a las empresas de todos los tamaños y giros a incorporar lineamiendos de debida diligencia y KWC con cliente, proveedores y/o con cualquier parte relacionada a la empresa, a fin de no estar vinculados de ninguna manera con aquellas entidades o personas que forman parte de los listados de FinCen, ya que estar vinculado a una entidad listada sería tanto como la "*muerte civil corporativa*".

Lo anterior es una fuerte invitación a contar con Sistemas de Gestión de Compliances, además auditorías inmediatas en las tesorerías de todas las empresas mexicanas, por que como ya se dijo, el permanente riesgo de ser listado por FinCen, con la finalidad de perseguir a cualquier entidad que provea soporte material, tecnológico o financiero a la cadena de tráfico de opioides o drogas de cualquier especie, debe generar el forzoso cumplimiento corporativo de las entidades mexicanas, especialemente aquellas que participan en áreas como la logística, transporte, química y farmacéutica.

Con todo lo dicho, podemos concluir que la frontera entre el derecho administrartivo, fiscal y el derecho penal se ha borrado. El Servicio de Administración Tributaria (SAT), armado con tecnología de inteligencia artificial y minería de datos en tiempo real, cruzando flujos de efectivo con declaraciones fiscales instantáneamente, información y datos que en todo momento estarán alimentando al Sistema Nacional de Inteligencia, con insumos que pueden detonar acciones penales devastadoras para cualquier indivudo o empresa en México. Por tanto, bajo la nueva óptica de la LSNIIMSP, una discrepancia fiscal (gastar más de lo declarado) ya no es solo una invitación a una revisión de gabinete; es un "indicador de riqueza inexplicable" que puede justificar una investigación patrimonial por parte de la SSPC o la UIF, lo que podría traer consecuencias de prisión preventiva oficiosa y la aplicación de la Ley Nacional de Extinción de Dominio.

Ante este panorama de hiper-fiscalización y vigilancia de inteligencia, la respuesta corporativa no puede ser pasiva. Se requiere una estrategia integral que combine Prevención (Compliance, "Debido Control Organizacional"), Reacción (Gestión de Crisis) y Defensa (Litigio).

Más en específico, los Oficiales de Cumplimientos deben pensar en tener, por ejemplo certificaciones en ISO 37301, esto para ser ofrecido como Prueba Pericial en juicio, de que la empresa si contaba con sistema de gestión certificado bajo ISO 37301, constituyendo

la evidencia más robusta para demostrar ante un juez que la empresa *sí* ejerció el debido control, demostrando que el delito fue un acto aislado de un empleado desleal (que eludió los controles) y no una falla sistémica o una política institucional de tolerancia al delito.

El Oficial de Cumplimiento debe evolucionar hacia un perfil de **ANALISTA DE INTELIGENCIA**, es decir antes de que el SAT/SSPC cruce los datos, la empresa debe hacerlo.[4] El Oficial de Cumplimiento debe tener establecido un "Protocolo de Crisis" ante la LSNIIMSP, contemplando las siguientes preguntas ¿Quién recibe a la autoridad (SSPC/Guardia Nacional) si llega con una solicitud de información basada en "inteligencia"? ¿El acto de autoridad está debidamente fundado y motivado, existe un mandamiento judicial? ¿Qué información se debe entregar? Esto a fin de no abrir nuevos frentes de investigación. Y sin duda debe estar haciendo un monitereo geopolítico, siguiendo las alertas de FinCEN y OFAC, como indicadores tempranos de riesgo sistémico en el sector financiero mexicano.

Así también, dado que la Guardia Nacional tiene facultades de "ciber-patrullaje" y monitoreo de la red pública , la ciberseguridad es ahora un pilar del cumplimiento legal, por lo que debemos encritar y segregar la información sensible (secretos industriales, datos personales), la información operativa común (dificultando su extracción masiva en caso de una intrusión o requerimiento digital excesivo).

CONCLUSIONES GENERALES

El entorno de negocios en México para el periodo 2025-2026 se define por la **hiper-vigilancia**. La frontera entre el cumplimiento administrativo y la responsabilidad penal ha desaparecido. La Ley del Sistema Nacional de Investigación e Inteligencia (LSNIIMSP) dota al Estado de un aparato omnisciente capaz de cruzar datos fiscales, bancarios y operativos en tiempo real, con facultades para actuar penalmente sin controles judiciales efectivos, sin la posibilidad de impugnar los "productos de inteligencia" de manera administrativa, debiendo enfrentar también el "cerco" internacional, donde el incumplimiento de las normas antilavado estadounidenses (FinCEN/CTA) conlleva la exclusión del sistema financiero global.

Los oficiales de cumplimiento y los abogados y contadores asesores de empresa deben transformarse en "estrategas de inteligencia", que entienda no solo de disposiciones legales o jursprudencia, sino los flujos de información del Sistema Nacional de Seguridad; deben combatir el fenómino de la hiper – vigilancia con integridad documentada y defensa estratégica[5] y tener presentes en todo momento las prioridades geopolíticas de Washington.

[4] Se recomienda realizar "Auditorías de Inteligencia" semestrales: cruzar la nómina, proveedores, geolocalización de flotillas y flujos financieros para detectar las mismas "anomalías" que buscará la IA del gobierno.

[5] El Oficial de Cumplimiento es hoy el arquitecto de esa defensa, el garante de la continuidad del negocio en un entorno donde el cumplimiento es la única vía para la supervivencia