OSINT, CIBERPATRULLAJE Y AGENTE ENCUBIERTO DIGITAL EN EL PROCESO PENAL

Diferencias conceptuales, límites constitucionales y nulidades típicas en la investigación penal contemporánea

I. Introducción

Investigación penal digital y erosión silenciosa de las garantías

La digitalización del delito no solo ha modificado el iter criminis. Ha alterado, de manera más profunda, las formas de investigar, los márgenes del control judicial y la relación entre el poder punitivo y la esfera de libertad individual. En este nuevo escenario, técnicas como el OSINT, el ciberpatrullaje y la actuación de agentes encubiertos digitales se han incorporado a la práctica forense con una velocidad muy superior a la de su elaboración dogmática.

El problema no reside en la utilización de tecnología, sino en la confusión conceptual que rodea a estas herramientas. En expedientes penales contemporáneos se observa una tendencia preocupante a tratarlas como si fueran expresiones intercambiables de una misma actividad investigativa, cuando en realidad responden a lógicas jurídicas distintas, con impactos constitucionales profundamente disímiles.

Esa confusión no es inocua. Funciona como un atajo argumental que permite aplicar controles mínimos a técnicas que, por su naturaleza, exigirían autorización judicial estricta. El resultado es una erosión silenciosa de las garantías del debido proceso, especialmente del derecho a la privacidad y del principio de legalidad.

II. Marco constitucional de la investigación digital

Privacidad, legalidad y control judicial reforzado

Toda técnica de investigación penal debe analizarse a la luz del bloque de constitucionalidad federal. En materia digital, este punto de partida adquiere una centralidad ineludible: la investigación estatal avanza, casi sin excepción, sobre datos personales, comunicaciones y espacios de intimidad protegidos por el art. 19 de la Constitución Nacional.

La Corte Suprema ha sido clara al respecto. Cuando el Estado interfiere en la vida privada de las personas, el estándar de control no se relaja: se intensifica. La tecnología no crea zonas exentas de la Constitución; por el contrario, multiplica los riesgos de afectación y exige respuestas jurídicas más exigentes.

Desde esta perspectiva, cualquier análisis serio sobre OSINT, ciberpatrullaje o agentes digitales debe comenzar por una pregunta básica: ¿estamos ante una simple observación de lo ya expuesto o ante una forma de vigilancia estatal que requiere habilitación legal y control judicial previo?

III. OSINT

Información de fuente abierta y su alcance constitucional real

El Open Source Intelligence (OSINT) refiere, en su concepción estricta, a la recolección y análisis de información disponible públicamente, accesible para cualquier usuario sin necesidad de engaño, acceso privilegiado ni vulneración de barreras técnicas o jurídicas.

Desde el punto de vista constitucional, el OSINT se apoya en una premisa clara: la ausencia de una expectativa razonable de privacidad. Quien decide —por voluntad, descuido o estrategia— publicar información en un entorno abierto asume el riesgo de que terceros, incluido el Estado, la observen.

Ahora bien, esta constatación inicial no habilita conclusiones apresuradas. Que una fuente sea abierta no la convierte en probatoriamente fiable ni autoriza cualquier modalidad de uso estatal.

En primer lugar, el carácter público del dato no garantiza su autenticidad. Identidades falsas, perfiles apócrifos, contenidos editados o sacados de contexto son fenómenos habituales en entornos digitales. El OSINT puede orientar una investigación, pero no reemplaza la necesidad de validación probatoria.

En segundo término —y esto es crucial— el OSINT no es ilimitado. Cuando la observación puntual se transforma en recolección sistemática, automatizada o masiva, la naturaleza de la actividad cambia. El problema ya no es el dato aislado, sino el uso acumulativo de información pública para reconstruir perfiles, rutinas y vínculos personales.

Allí donde el Estado deja de “mirar lo que está” y comienza a perfilar sujetos, el OSINT se agota como categoría justificante.

IV. Del OSINT al ciberpatrullaje

El quiebre dogmático y el efecto mosaico

El ciberpatrullaje constituye una técnica cualitativamente distinta. No se trata de una consulta ocasional, sino de una observación organizada, dirigida y sostenida en el tiempo, orientada a detectar conductas, prevenir delitos o identificar sujetos de interés.

Aunque muchas veces se apoya en datos formalmente públicos, el ciberpatrullaje introduce un elemento decisivo: la sistematicidad. Esa sistematicidad altera por completo el análisis constitucional.

La defensa habitual de estas prácticas se apoya en una afirmación engañosa: “si el dato es público, no hay privacidad”. Esta lógica desconoce el fenómeno del efecto acumulativo o efecto mosaico. Datos aislados pueden ser triviales; su acumulación permite al Estado conocer más sobre una persona que lo que esa persona recuerda haber expuesto.

En ese punto, la expectativa de privacidad no desaparece: se redefine. No por el contenido individual del dato, sino por la capacidad estatal de reconstruir una biografía digital completa sin control judicial.

El ciberpatrullaje, cuando se despliega sin causa previa, sin delimitación temporal ni material y sin autorización judicial específica, deja de ser una técnica investigativa legítima y se convierte en una forma de vigilancia preventiva, incompatible con el principio de legalidad.

Aceptar que el Estado “patrulle” redes para ver qué encuentra equivale a invertir la lógica constitucional: primero se vigila, luego se busca el delito. Esa inversión es precisamente lo que el proceso penal pretende evitar.

V. Primer balance dogmático

La función de la claridad conceptual

Hasta aquí, el deslinde es nítido.

El OSINT, en sentido estricto, puede ser una herramienta legítima de información preliminar cuando se limita a la observación puntual de fuentes abiertas y no deriva en perfilamiento sistemático.

El ciberpatrullaje, en cambio, constituye una técnica de vigilancia que no puede justificarse exclusivamente por el carácter público de los datos observados. Su ejercicio sin habilitación normativa clara ni control judicial previo compromete derechos fundamentales y contamina la validez de la prueba obtenida.

La confusión entre ambas categorías no es un error terminológico. Es una estrategia de deslizamiento que permite aplicar controles mínimos donde deberían regir los máximos estándares constitucionales.

VI. La frontera crítica: cuando el Estado deja de observar y empieza a intervenir

Este punto marca el pasaje a la zona más sensible de la investigación digital. Cuando el Estado ya no se limita a observar conductas existentes, sino que interactúa activamente bajo identidades falsas, se produce un salto cualitativo que exige un régimen jurídico completamente distinto.

Ese salto es el que introduce la figura del agente digital, en sus dos variantes dogmáticamente relevantes: el agente encubierto y el agente revelador.

VII. Agente encubierto digital

Infiltración, engaño y producción estatal del escenario probatorio

La figura del agente encubierto digital introduce una ruptura decisiva respecto de las técnicas analizadas hasta aquí. A diferencia del OSINT y del ciberpatrullaje, el agente encubierto no observa: se infiltra. Su actuación supone la creación o utilización de una identidad falsa para integrarse a un entorno digital cerrado, ganar la confianza de los participantes y acceder a información que, sin ese engaño, permanecería inaccesible.

Desde el punto de vista dogmático, el dato central no es la falsedad de la identidad, sino la alteración del curso natural de los hechos. El agente encubierto digital no se limita a registrar una conducta preexistente; interviene en la dinámica comunicacional del grupo, condiciona respuestas, habilita intercambios y, en no pocos casos, produce la evidencia que luego será utilizada en su contra.

Precisamente por ese potencial lesivo, la actuación encubierta ha sido históricamente considerada una técnica de investigación excepcional, sometida a estrictos requisitos de legalidad, necesidad y control judicial. El traslado de esta figura al entorno digital no atenúa esas exigencias; las refuerza.

Aceptar que el Estado pueda infiltrar comunidades digitales bajo la excusa de que “todo ocurre en internet” supone desconocer que la afectación a la autodeterminación personal es, en muchos casos, más intensa que en el mundo analógico.

VIII. El agente revelador

La zona de mayor riesgo dogmático y el corazón de las nulidades

La distinción entre agente encubierto y agente revelador es, hoy, uno de los puntos más relevantes —y más ignorados— de la práctica penal. No se trata de una sutileza académica, sino del núcleo de múltiples planteos de nulidad.

Mientras el agente encubierto se infiltra para observar y documentar una organización o dinámica delictiva preexistente, el agente revelador tiene un objetivo diferente: provocar la exteriorización del delito. Compra droga, solicita material ilícito, induce la entrega del

objeto prohibido. Su intervención es directa y decisiva para la consumación del hecho.

Aquí el riesgo constitucional se multiplica. Cuando el Estado no se limita a constatar una actividad en curso, sino que crea la oportunidad, estimula la decisión o facilita los medios, la frontera entre investigación y provocación se vuelve extremadamente delgada.

Desde una perspectiva dogmática, el problema no es solo ético o político. Es probatorio. Si el hecho investigado no habría ocurrido sin la intervención estatal, la evidencia obtenida deja de ser el resultado de una conducta libre del imputado y se convierte en el producto de una ingeniería investigativa.

En estos supuestos, la pregunta correcta no es si el imputado “aceptó” la propuesta, sino si el Estado fabricó el escenario delictivo que luego utiliza como fundamento de la acusación.

IX. Inducción, provocación y el límite constitucional

La diferencia entre investigación legítima e inducción ilegítima no puede resolverse con fórmulas simplistas. No toda intervención estatal configura provocación. Pero tampoco puede admitirse una zona gris en la que el engaño estatal quede librado a la discrecionalidad operativa.

La inducción aparece cuando la intervención del agente resulta determinante para la comisión del hecho. No basta con que el delito sea “posible” sin el agente; es necesario analizar si, en el caso concreto, la conducta se habría producido en los mismos términos y con la misma intensidad de no mediar la actuación estatal.

Este análisis es especialmente sensible en el ámbito digital, donde la interacción es persistente, asincrónica y capaz de generar una falsa sensación de intimidad o normalidad. Mensajes reiterados, incentivos implícitos, presión temporal o promesas de anonimato son herramientas que, lejos de ser neutrales, modelan la decisión del sujeto.

Cuando el agente revelador cruza ese umbral, la consecuencia no es una simple irregularidad: es la nulidad de la prueba por violación del debido proceso. La legitimidad del proceso penal se quiebra cuando el Estado castiga una conducta que él mismo contribuyó decisivamente a generar.

X. Errores típicos de la acusación en investigaciones digitales

La experiencia forense permite identificar patrones que se repiten con notable frecuencia en causas basadas en OSINT ampliado, ciberpatrullaje o agentes digitales.

Uno de los más comunes es la recalificación ex post de la técnica utilizada. Interacciones encubiertas son presentadas como “tareas de prevención”; infiltraciones activas se

describen como “observación de fuente abierta”. Esta maniobra retórica no sana el vicio. La naturaleza de la técnica se define por lo que el Estado hizo, no por cómo decide nombrarlo después.

Otro error habitual es la ausencia o vaguedad de la autorización judicial. Órdenes genéricas, sin delimitación temporal, sin identificación precisa de la técnica autorizada o sin control de la intensidad de la intervención son incompatibles con un modelo de investigación respetuoso de las garantías.

Finalmente, aparece la expansión indebida del objeto autorizado. Se habilita la observación de un perfil o grupo específico y la investigación deriva en la intervención de comunidades enteras, conversaciones ajenas y terceros no imputados. Esa expansión no es una cuestión de exceso menor: es una ruptura del marco de legalidad.

XI. Consecuencias procesales

Exclusión, nulidad y fuerza convictiva

Las consecuencias procesales de estas infracciones no admiten soluciones complacientes.

Cuando la actuación estatal —sea por ciberpatrullaje sin causa, infiltración sin control o inducción mediante agente revelador— vulnera garantías constitucionales, la prueba obtenida debe ser excluida. No por una lógica sancionatoria, sino porque admitirla implicaría validar una forma de investigación incompatible con el Estado de Derecho.

En otros casos, la irregularidad puede no alcanzar el umbral de la ilicitud, pero sí comprometer gravemente la confiabilidad del material. Allí la prueba puede subsistir formalmente, pero pierde fuerza convictiva, especialmente si constituye el eje central de la imputación. Una condena no puede apoyarse en evidencia producida bajo un esquema de vigilancia o provocación dudoso.

Reducir estas discusiones a la pregunta de si “sirvió” o “no sirvió” la investigación empobrece el análisis. La cuestión no es la eficacia, sino la legitimidad del método.

XII. Conclusión

Claridad conceptual como defensa de las garantías

OSINT, ciberpatrullaje, agente encubierto digital y agente revelador no son variantes terminológicas de una misma actividad. Son categorías dogmáticas distintas, con impactos constitucionales propios y exigencias de control diferenciadas.

La confusión entre ellas no es un error técnico inocente. Es una vía de escape que permite expandir el poder investigativo sin expandir, en la misma medida, el control judicial. Allí

donde esa confusión se consolida, las garantías se vacían.

El desafío para la defensa penal en la era digital no consiste en oponerse a la tecnología, sino en reinsertarla en el marco del proceso penal. Obligar al Estado a llamar a cada técnica por su nombre, a justificarla y a someterla a control no es obstaculizar la investigación: es preservar la legitimidad de la condena.

En el proceso penal, también en el digital, el fin no justifica los medios. Y cuando los medios son engañosos, invasivos o provocadores, el resultado —por más útil que parezca— deja de ser jurídicamente aceptable.