Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2026,
Volumen 10, Número 2.

https://doi.org/10.37811/cl_rcm.v10i2

SPYWARE Y DEBIDO PROCESO EN EL SISTEMA PENAL ACUSATORIO: REVISIÓN CRÍTICA DEL MARCO NORMATIVO MEXICANO Y LOS PRECEDENTES DE LA SUPREMA CORTE Y LA CORTE INTERAMERICANA

SPYWARE AND DUE PROCESS IN THE ADVERSARIAL CRIMINAL JUSTICE SYSTEM:A CRITICAL REVIEW OF THE MEXICAN LEGAL FRAMEWORK AND THE PRECEDENTS OF THE SUPREME COURT AND THE INTER-AMERICAN COURT OF HUMAN RIGHTS

Shiomara Escartin Cruz
Centro Universitario Continental, México

DOI: https://doi.org/10.37811/cl_rcm.v10i2.23455

SPYWARE y Debido Proceso en el Sistema Penal Acusatorio: Revisión Crítica del Marco Normativo Mexicano y los Precedentes de la Suprema Corte y la Corte Interamericana

Shiomara Escartin Cruz[1]
escrsh20d15@redcuc.edu.mx
Centro Universitario Continental
Hidalgo, México

RESUMEN

El presente artículo de revisión tiene como objetivo analizar críticamente el uso de tecnologías de vigilancia digital, particularmente el spyware, en el marco del sistema penal acusatorio mexicano, evaluando su compatibilidad con las garantías del debido proceso, el derecho a la privacidad y los estándares internacionales de derechos humanos. Se examinan los precedentes jurisprudenciales desarrollados por la Suprema Corte de Justicia de la Nación y la Corte Interamericana de Derechos Humanos en relación con la intervención de comunicaciones privadas y el control judicial de las técnicas de investigación tecnológica. La investigación se desarrolló mediante un enfoque cualitativo de revisión sistemática de la literatura, aplicando la metodología PRISMA para la identificación, selección y análisis de estudios académicos, documentos jurídicos y jurisprudencia relevante publicados entre 2005 y 2024. Se consultaron bases de datos científicas y repositorios jurídicos especializados, estableciendo criterios de inclusión orientados a investigaciones sobre vigilancia digital, privacidad, debido proceso y regulación del espionaje tecnológico. Los resultados evidencian que el uso de spyware plantea importantes desafíos jurídicos en el contexto del proceso penal, debido a su carácter altamente invasivo y a los vacíos normativos existentes en la regulación de estas tecnologías. La revisión muestra que los estándares desarrollados por la jurisprudencia nacional e interamericana enfatizan la necesidad de controles judiciales estrictos, así como la aplicación de los principios de legalidad, necesidad y proporcionalidad para garantizar la protección de los derechos fundamentales en el entorno digital.

Palabras claves: spyware, debido proceso, sistema penal acusatorio.

[1] Autor principal
Correspondencia: escrsh20d15@redcuc.edu.mx

Spyware and Due Process in the Adversarial Criminal Justice System: A Critical Review of the Mexican Legal Framework and the Precedents of the Supreme Court and the Inter-American Court of Human Rights

ABSTRACT

This review article aims to critically analyze the use of digital surveillance technologies, particularly spyware, within the framework of the Mexican adversarial criminal justice system, evaluating their compatibility with due process guarantees, the right to privacy, and international human rights standards. Additionally, the study examines the jurisprudential precedents developed by the Supreme Court of Justice of the Nation and the Inter-American Court of Human Rights regarding the interception of private communications and judicial oversight of technological investigative techniques. The research was conducted using a qualitative approach through a systematic literature review, applying the PRISMA methodology for the identification, selection, and analysis of academic studies, legal documents, and relevant jurisprudence published between 2005 and 2024. Scientific databases and specialized legal repositories were consulted, with inclusion criteria focused on research related to digital surveillance, privacy, due process, and the regulation of technological espionage. The results show that the use of spyware poses significant legal challenges in the context of criminal proceedings due to its highly invasive nature and the existing regulatory gaps in the oversight of these technologies. Furthermore, the review highlights that standards established by national and inter-American jurisprudence emphasize the need for strict judicial controls and the application of the principles of legality, necessity, and proportionality to ensure the protection of fundamental rights in the digital environment.

Keywords: spyware, due process, adversarial criminal justice system.

Artículo recibido 28 febrero 2026
Aceptado para publicación: 28 marzo 2026

INTRODUCCIÓN

En las últimas décadas, el desarrollo acelerado de las tecnologías digitales ha transformado profundamente las formas de vigilancia estatal y la obtención de información en el ámbito de la seguridad pública y la persecución penal. Entre estas herramientas emergentes destaca el uso de programas informáticos de vigilancia conocidos como spyware, capaces de infiltrarse en dispositivos electrónicos para recolectar información privada sin el conocimiento del usuario. Este tipo de tecnologías ha generado un intenso debate jurídico y ético en torno a su compatibilidad con los derechos fundamentales, particularmente con el derecho a la privacidad, la protección de datos personales y el debido proceso en los sistemas de justicia penal contemporáneos (Deibert, 2019; Marczak et al., 2018). En el caso de México, el uso de software de vigilancia como Pegasus ha provocado controversias significativas al evidenciar tensiones entre las facultades del Estado para investigar delitos y la obligación de respetar las garantías procesales establecidas tanto en la Constitución como en los tratados internacionales de derechos humanos (R3D, 2022; Citizen Lab, 2023).

El spyware, entendido como un conjunto de herramientas tecnológicas diseñadas para obtener acceso remoto a dispositivos electrónicos y recopilar información de manera encubierta, representa una de las expresiones más sofisticadas de la vigilancia digital contemporánea. Estos programas permiten acceder a mensajes, llamadas, correos electrónicos, ubicaciones geográficas e incluso activar micrófonos o cámaras de los dispositivos infectados, lo que implica una intrusión profunda en la esfera privada de las personas (Deibert, 2019). En particular, el software Pegasus, desarrollado por la empresa israelí NSO Group, ha sido objeto de numerosas investigaciones internacionales debido a su presunto uso para espiar a periodistas, defensores de derechos humanos, activistas y figuras políticas en diversos países, incluido México (Marczak et al., 2018). Estas prácticas han generado preocupación a nivel global, pues evidencian cómo las tecnologías de vigilancia pueden ser utilizadas de forma desproporcionada o sin controles judiciales adecuados, lo que plantea desafíos significativos para el respeto de las libertades fundamentales (Access Now, 2021).

En el contexto mexicano, el debate sobre el uso del spyware ha adquirido particular relevancia debido a diversos casos documentados que evidencian la posible utilización de estas herramientas con fines distintos a los previstos por la ley. Investigaciones periodísticas y reportes de organizaciones de

derechos digitales han señalado que el software Pegasus fue utilizado en distintos periodos gubernamentales para vigilar a periodistas, activistas y opositores políticos, lo que generó cuestionamientos sobre la legalidad y legitimidad de dichas prácticas (R3D, 2022; Marczak et al., 2018). Incluso organismos internacionales han advertido sobre la necesidad de investigar el uso de estas tecnologías en México, especialmente cuando afectan a actores fundamentales para el funcionamiento de una sociedad democrática, como periodistas y defensores de derechos humanos (CIDH, 2023). En este sentido, la Comisión Interamericana de Derechos Humanos ha llamado al Estado mexicano a esclarecer los casos relacionados con Pegasus y garantizar que las investigaciones se conduzcan conforme a estándares internacionales de protección de derechos humanos.

El problema adquiere una dimensión aún más compleja cuando se analiza a la luz del sistema penal acusatorio mexicano, instaurado formalmente con la reforma constitucional de 2008. Este modelo procesal se caracteriza por principios como la presunción de inocencia, la publicidad, la contradicción y el respeto al debido proceso, los cuales buscan garantizar un equilibrio entre la eficacia de la investigación penal y la protección de los derechos fundamentales de las personas imputadas (Carbonell, 2013). Dentro de este sistema, la obtención de pruebas mediante técnicas de investigación intrusivas, como la intervención de comunicaciones privadas o el acceso a información digital, debe realizarse bajo estrictos controles judiciales y conforme a los principios de legalidad, necesidad y proporcionalidad (Fix-Zamudio & Valencia Carmona, 2015). Sin embargo, la incorporación de herramientas tecnológicas altamente invasivas, como el spyware, plantea interrogantes sobre la suficiencia de los marcos normativos existentes para regular su uso y evitar abusos por parte de las autoridades.

En este contexto, el debido proceso se configura como una garantía fundamental que limita el ejercicio del poder punitivo del Estado y asegura que toda persona sea juzgada mediante procedimientos justos, imparciales y respetuosos de sus derechos. Este principio, reconocido tanto en la Constitución Política de los Estados Unidos Mexicanos como en diversos instrumentos internacionales, implica que cualquier forma de obtención de pruebas debe respetar estándares de legalidad y control judicial previo (Fix-Zamudio, 2017). La intervención de comunicaciones privadas, por ejemplo, solo puede realizarse con autorización judicial fundada y motivada, lo que busca evitar prácticas arbitrarias o invasivas que

vulneren la intimidad de las personas. Sin embargo, la naturaleza encubierta del spyware dificulta en muchos casos la supervisión judicial efectiva, lo que puede generar riesgos significativos para el respeto de estas garantías procesales (Deibert, 2019).

La Suprema Corte de Justicia de la Nación ha desempeñado un papel central en la delimitación de los alcances constitucionales de las medidas de vigilancia estatal. A través de diversas resoluciones, el máximo tribunal mexicano ha establecido criterios que buscan garantizar que las intervenciones en comunicaciones privadas se realicen únicamente bajo autorización judicial y con estricto apego a los principios constitucionales. En una decisión relevante, la Corte invalidó disposiciones legales que permitían a las autoridades militares intervenir comunicaciones sin orden judicial, al considerar que dichas prácticas vulneraban el derecho a la privacidad y el principio de control judicial previo. Este precedente reafirma la importancia de que cualquier forma de vigilancia estatal esté sujeta a mecanismos de supervisión que garanticen la protección de los derechos fundamentales.

La Suprema Corte ha intervenido en debates relacionados con la transparencia y rendición de cuentas respecto al uso de tecnologías de vigilancia. En 2024, el tribunal determinó que las autoridades federales debían hacer públicos los contratos relacionados con la adquisición del software Pegasus, al considerar que la reserva absoluta de dicha información carecía de justificación suficiente y contravenía el principio de acceso a la información pública. Este tipo de resoluciones reflejan la creciente preocupación del poder judicial por garantizar que el uso de herramientas de vigilancia tecnológica esté sujeto a mecanismos de control democrático y transparencia institucional.

Paralelamente, la Corte Interamericana de Derechos Humanos ha desarrollado una sólida jurisprudencia en materia de protección de la privacidad y vigilancia estatal. En diversos casos, el tribunal interamericano ha sostenido que la intervención de comunicaciones privadas constituye una medida altamente invasiva que solo puede justificarse cuando cumple con criterios estrictos de legalidad, necesidad y proporcionalidad (Corte IDH, 2012). Además, ha enfatizado que los Estados deben establecer marcos normativos claros que regulen estas prácticas y aseguren mecanismos de supervisión judicial y rendición de cuentas. Estas directrices son particularmente relevantes para los países de América Latina, incluidos México, que han incorporado los tratados internacionales de derechos humanos como parte de su sistema jurídico interno.

La interacción entre el derecho constitucional mexicano y el sistema interamericano de derechos humanos ha contribuido a fortalecer los estándares de protección en materia de vigilancia estatal y debido proceso. A partir de la reforma constitucional en materia de derechos humanos de 2011, los jueces mexicanos están obligados a interpretar las normas nacionales conforme a los tratados internacionales y a los criterios establecidos por la Corte Interamericana (Fix-Zamudio, 2017). Este marco normativo refuerza la obligación del Estado mexicano de garantizar que cualquier forma de vigilancia tecnológica se realice dentro de los límites establecidos por el derecho internacional de los derechos humanos.

No obstante, a pesar de estos avances normativos y jurisprudenciales, persisten importantes desafíos en la regulación del spyware dentro del sistema penal mexicano. La rápida evolución de las tecnologías de vigilancia ha superado en muchos casos la capacidad de los marcos jurídicos tradicionales para regular su uso de manera efectiva. En particular, la opacidad en la adquisición y utilización de software de espionaje por parte de diversas instituciones gubernamentales ha generado dudas sobre la existencia de mecanismos adecuados de control y supervisión (R3D, 2022). La dificultad para detectar este tipo de programas y probar su uso en procesos judiciales plantea desafíos adicionales para la protección de los derechos fundamentales.

En este escenario, resulta fundamental realizar un análisis crítico del marco normativo y jurisprudencial que regula el uso del spyware en México, con especial énfasis en su compatibilidad con el debido proceso dentro del sistema penal acusatorio. La revisión de los precedentes de la Suprema Corte de Justicia de la Nación y de la Corte Interamericana de Derechos Humanos permite identificar los estándares jurídicos aplicables a estas prácticas y evaluar su implementación en el contexto mexicano. El análisis de la literatura académica y jurídica sobre vigilancia digital contribuye a comprender las implicaciones más amplias de estas tecnologías para el Estado de derecho y la protección de los derechos humanos.

En este sentido, el presente artículo de revisión tiene como objetivo analizar críticamente el uso del spyware en el sistema penal acusatorio mexicano, examinando su relación con el debido proceso a partir del marco normativo nacional y de los precedentes jurisprudenciales de la Suprema Corte de Justicia de la Nación y de la Corte Interamericana de Derechos Humanos.

Para ello, se realiza una revisión sistemática de la literatura académica, documentos jurídicos y decisiones judiciales relevantes, con el fin de identificar los principales debates doctrinales y los desafíos regulatorios asociados a la vigilancia digital en el contexto de la justicia penal.

La relevancia de este estudio radica en que el uso creciente de tecnologías de vigilancia plantea interrogantes fundamentales sobre los límites del poder estatal en una sociedad democrática. Si bien estas herramientas pueden contribuir a fortalecer las capacidades de investigación y combate al crimen, su utilización sin controles adecuados puede derivar en violaciones graves a los derechos humanos y erosionar la confianza pública en las instituciones de justicia. Por ello, resulta indispensable analizar críticamente los marcos jurídicos que regulan estas prácticas y proponer enfoques que permitan equilibrar la seguridad pública con la protección efectiva de las libertades fundamentales.

El análisis del spyware y su relación con el debido proceso constituye un tema de creciente relevancia en el derecho penal contemporáneo, especialmente en contextos donde la tecnología ha ampliado las capacidades de vigilancia estatal. El caso mexicano ofrece un escenario particularmente significativo para examinar estas dinámicas, debido a los debates generados por el uso de software como Pegasus y la intervención de diversas instancias judiciales y organismos internacionales. A través de una revisión crítica del marco normativo y jurisprudencial, este artículo busca contribuir a la comprensión de los desafíos jurídicos que plantea la vigilancia digital y a la construcción de propuestas que fortalezcan el respeto de los derechos humanos en el sistema penal acusatorio.

Contexto y Relevancia del Estudio

El avance acelerado de las tecnologías digitales ha transformado profundamente las formas de vigilancia estatal y la obtención de información en el ámbito de la seguridad pública y la investigación penal. En este contexto, el uso de software de vigilancia o spyware ha adquirido una relevancia creciente debido a su capacidad para acceder de manera encubierta a dispositivos electrónicos y recolectar grandes volúmenes de información personal, incluyendo comunicaciones privadas, ubicaciones geográficas, archivos y registros de actividad digital (Deibert, 2019). Estas herramientas tecnológicas han sido justificadas por los Estados como instrumentos necesarios para combatir delitos complejos como el crimen organizado, el terrorismo y las redes transnacionales de delincuencia; sin embargo, su

utilización también ha generado preocupaciones significativas en relación con la protección de los derechos fundamentales y el respeto al debido proceso (Marczak et al., 2018).

En el caso de México, el debate sobre el uso de spyware ha adquirido especial relevancia a partir de la divulgación de investigaciones periodísticas y reportes de organizaciones de la sociedad civil que documentan la presunta utilización del software Pegasus para vigilar a periodistas, defensores de derechos humanos y actores políticos. Estos hallazgos han generado un intenso debate jurídico y político sobre la legalidad de dichas prácticas y la existencia de mecanismos adecuados de control judicial y rendición de cuentas (R3D, 2022). La controversia también ha evidenciado las tensiones existentes entre las facultades del Estado para investigar delitos y la obligación de respetar los derechos fundamentales de las personas, especialmente el derecho a la privacidad, la inviolabilidad de las comunicaciones y las garantías del debido proceso (Fix-Zamudio, 2017).

El sistema penal acusatorio mexicano, instaurado mediante la reforma constitucional de 2008, se fundamenta en principios como la presunción de inocencia, la legalidad, la contradicción y la publicidad del proceso, los cuales buscan garantizar un equilibrio entre la eficacia de la persecución penal y la protección de los derechos humanos (Carbonell, 2013). Dentro de este modelo, cualquier forma de intervención en la esfera privada de las personas debe estar estrictamente regulada por la ley y contar con autorización judicial previa, conforme a estándares de necesidad, proporcionalidad y razonabilidad. No obstante, la incorporación de tecnologías altamente invasivas como el spyware plantea nuevos desafíos jurídicos que cuestionan la suficiencia del marco normativo existente para regular estas prácticas (Deibert, 2019).

En este sentido, el análisis del uso de spyware en el sistema penal mexicano resulta particularmente relevante debido a la creciente digitalización de las comunicaciones y a la necesidad de garantizar que las herramientas tecnológicas utilizadas por las autoridades no vulneren los principios fundamentales del debido proceso. La revisión de los precedentes de la Suprema Corte de Justicia de la Nación y de la Corte Interamericana de Derechos Humanos permite comprender los estándares jurídicos aplicables a estas prácticas y evaluar su compatibilidad con los derechos humanos reconocidos en el ordenamiento jurídico nacional e internacional (Corte IDH, 2012).

Fundamentación Teórica

La discusión sobre el uso de spyware en la investigación penal se encuentra estrechamente vinculada con el desarrollo del derecho a la privacidad y con las garantías del debido proceso en los sistemas jurídicos contemporáneos. El derecho a la privacidad ha sido reconocido como un componente esencial de la dignidad humana y como una condición necesaria para el ejercicio de otras libertades fundamentales, como la libertad de expresión y la libertad de asociación (Solove, 2008). En el ámbito jurídico, este derecho implica que las personas tienen la facultad de controlar el acceso a su información personal y de mantener protegida su esfera íntima frente a interferencias arbitrarias por parte del Estado o de terceros.

En el contexto de las tecnologías digitales, la protección de la privacidad ha adquirido una dimensión particularmente compleja, debido a la capacidad de los sistemas informáticos para recopilar, almacenar y analizar grandes cantidades de datos personales. El spyware representa una de las manifestaciones más avanzadas de la vigilancia digital, ya que permite acceder de manera remota y encubierta a dispositivos electrónicos sin el conocimiento del usuario, lo que genera riesgos significativos para la protección de los derechos fundamentales (Deibert, 2019). Desde una perspectiva jurídica, el uso de estas herramientas plantea interrogantes sobre los límites del poder estatal y sobre la necesidad de establecer mecanismos de control que garanticen el respeto de las garantías constitucionales.

El principio del debido proceso constituye uno de los pilares fundamentales del Estado de derecho y se refiere al conjunto de garantías que deben observarse en cualquier procedimiento judicial o administrativo que pueda afectar los derechos de las personas. En el ámbito penal, este principio implica que las autoridades deben actuar conforme a la ley, respetar los derechos del imputado y garantizar que las pruebas obtenidas durante la investigación sean recabadas de manera lícita y conforme a estándares de legalidad y proporcionalidad (Fix-Zamudio & Valencia Carmona, 2015). La obtención de pruebas mediante métodos ilegales o que vulneren derechos fundamentales puede dar lugar a su exclusión del proceso penal, conforme al principio de la prueba ilícita.

La jurisprudencia internacional también ha desempeñado un papel clave en el desarrollo de estándares relacionados con la vigilancia estatal y la protección de la privacidad. La Corte Interamericana de Derechos Humanos ha establecido que cualquier medida de intervención en las comunicaciones

privadas debe cumplir con requisitos estrictos de legalidad, finalidad legítima, necesidad y proporcionalidad (Corte IDH, 2012). Ha señalado que los Estados deben contar con marcos normativos claros y mecanismos efectivos de supervisión judicial que permitan prevenir abusos en el uso de tecnologías de vigilancia.

En el caso mexicano, la reforma constitucional en materia de derechos humanos de 2011 fortaleció la protección de los derechos fundamentales al incorporar el principio pro persona y al reconocer la jerarquía constitucional de los tratados internacionales de derechos humanos (Fix-Zamudio, 2017). Esto implica que las autoridades judiciales deben interpretar las normas nacionales de conformidad con los estándares internacionales, incluyendo los desarrollados por la Corte Interamericana. En consecuencia, el análisis del uso de spyware en México requiere considerar tanto el marco constitucional interno como las obligaciones internacionales del Estado en materia de derechos humanos.

Desde una perspectiva teórica, el debate sobre la vigilancia digital también se relaciona con el concepto de proporcionalidad en el ejercicio del poder estatal. Este principio establece que cualquier restricción a los derechos fundamentales debe ser adecuada para alcanzar un objetivo legítimo, necesaria en ausencia de medidas menos restrictivas y proporcional en sentido estricto, de manera que el beneficio obtenido por la medida no supere el daño causado a los derechos de las personas (Alexy, 2010). En el caso del spyware, la aplicación de este principio resulta esencial para evaluar la legitimidad de su uso dentro de las investigaciones penales.

Problemática

El uso de tecnologías de vigilancia digital en el ámbito de la investigación penal ha generado uno de los debates más complejos del derecho contemporáneo, particularmente en lo que respecta al equilibrio entre la seguridad pública y la protección de los derechos fundamentales. En el caso del spyware, esta problemática se intensifica debido a la capacidad de estas herramientas para acceder de manera encubierta a grandes volúmenes de información personal, lo que implica una intrusión profunda en la esfera privada de las personas (Deibert, 2019). Si bien los Estados justifican el uso de estas tecnologías como una estrategia necesaria para combatir delitos complejos, su utilización sin controles adecuados puede derivar en prácticas de vigilancia arbitraria y en violaciones graves a los derechos humanos.

En México, la problemática se ha evidenciado particularmente a partir de los casos relacionados con el uso del software Pegasus, que ha sido señalado en diversas investigaciones como una herramienta utilizada para espiar a periodistas, activistas y defensores de derechos humanos. Estas revelaciones han generado cuestionamientos sobre la legalidad de las prácticas de vigilancia realizadas por las autoridades y sobre la existencia de mecanismos efectivos de control judicial y rendición de cuentas (Marczak et al., 2018). Han puesto en evidencia la falta de transparencia en la adquisición y utilización de tecnologías de vigilancia por parte de diversas instituciones gubernamentales.

Uno de los principales problemas jurídicos asociados con el uso de spyware radica en la dificultad para garantizar el respeto del debido proceso dentro del sistema penal acusatorio. Este sistema se basa en principios como la presunción de inocencia, la igualdad entre las partes y la legalidad en la obtención de pruebas, lo que implica que cualquier evidencia utilizada en un proceso penal debe haber sido obtenida de manera lícita y conforme a los procedimientos establecidos por la ley (Carbonell, 2013). Sin embargo, la naturaleza encubierta del spyware puede dificultar la supervisión judicial efectiva y generar dudas sobre la legalidad de las pruebas obtenidas mediante estas herramientas.

Otro aspecto problemático se relaciona con la insuficiencia del marco normativo para regular el uso de tecnologías de vigilancia digital. Aunque la legislación mexicana contempla la posibilidad de intervenir comunicaciones privadas bajo autorización judicial, muchas de estas disposiciones fueron diseñadas antes del desarrollo de herramientas tecnológicas como el spyware, lo que genera vacíos legales en su regulación (Fix-Zamudio & Valencia Carmona, 2015). Esta situación plantea la necesidad de actualizar los marcos jurídicos existentes para garantizar que las nuevas tecnologías se utilicen de manera compatible con los derechos fundamentales.

La jurisprudencia de la Suprema Corte de Justicia de la Nación y de la Corte Interamericana de Derechos Humanos ha establecido estándares importantes para regular las intervenciones en comunicaciones privadas. No obstante, la aplicación práctica de estos criterios en el contexto de la vigilancia digital sigue siendo objeto de debate. En particular, persisten interrogantes sobre la manera en que los tribunales deben evaluar la legalidad de las pruebas obtenidas mediante spyware y sobre los mecanismos que deben implementarse para garantizar la transparencia y la rendición de cuentas en el uso de estas tecnologías (Corte IDH, 2012).

En consecuencia, la problemática central de este estudio radica en la necesidad de analizar críticamente si el marco normativo mexicano y los precedentes jurisprudenciales existentes son suficientes para regular el uso del spyware dentro del sistema penal acusatorio y garantizar el respeto del debido proceso. Este análisis resulta fundamental para identificar los desafíos jurídicos que plantea la vigilancia digital y para proponer estrategias que permitan fortalecer la protección de los derechos humanos en el ámbito de la justicia penal.

Objetivos y Preguntas de Investigación

El presente artículo de revisión tiene como objetivo general analizar críticamente el uso del spyware en el sistema penal acusatorio mexicano, examinando su compatibilidad con el principio del debido proceso a partir del marco normativo nacional y de los precedentes jurisprudenciales de la Suprema Corte de Justicia de la Nación y de la Corte Interamericana de Derechos Humanos.

De manera específica, el estudio busca identificar los principales debates doctrinales y jurídicos en torno al uso de tecnologías de vigilancia digital en la investigación penal, así como analizar los estándares constitucionales e internacionales aplicables a la intervención de comunicaciones privadas y al uso de herramientas tecnológicas de espionaje. Se pretende evaluar si el marco jurídico mexicano vigente ofrece garantías suficientes para prevenir abusos en el uso del spyware y proteger los derechos fundamentales de las personas involucradas en procesos penales (Fix-Zamudio, 2017; Corte IDH, 2012).

A partir de estos objetivos, el estudio plantea las siguientes preguntas de investigación: ¿cuáles son los principales estándares jurídicos que regulan el uso de spyware en el sistema penal acusatorio mexicano?, ¿de qué manera la jurisprudencia de la Suprema Corte de Justicia de la Nación y de la Corte Interamericana de Derechos Humanos aborda la relación entre vigilancia digital y debido proceso?, y ¿qué desafíos normativos y jurisprudenciales persisten para garantizar la protección efectiva de los derechos fundamentales frente al uso de tecnologías de espionaje digital en el contexto de la justicia penal contemporánea?

METODOLOGÍA

El presente estudio se desarrolló bajo un enfoque cualitativo mediante un diseño de revisión sistemática de la literatura, orientado a analizar críticamente el uso del spyware en el sistema penal acusatorio

mexicano y su relación con el principio del debido proceso, a partir del marco normativo nacional y de los precedentes jurisprudenciales relevantes. Para garantizar la transparencia, la rigurosidad metodológica y la replicabilidad del estudio, se adoptó la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), ampliamente utilizada en revisiones sistemáticas en diferentes áreas del conocimiento para organizar el proceso de identificación, selección, evaluación y síntesis de la evidencia científica (Page et al., 2021).

Diseño de la revisión

La investigación se estructuró siguiendo las cuatro fases principales del modelo PRISMA: identificación, cribado, elegibilidad e inclusión. Este proceso permitió organizar de manera sistemática la búsqueda y selección de fuentes académicas, normativas y jurisprudenciales relacionadas con el uso de tecnologías de vigilancia digital en el ámbito de la investigación penal, así como con los estándares jurídicos del debido proceso en el derecho constitucional y en el sistema interamericano de derechos humanos.

El diseño metodológico se orientó hacia un análisis documental y jurídico comparado, integrando literatura científica, marcos normativos nacionales, decisiones jurisprudenciales de tribunales nacionales e internacionales y documentos institucionales relevantes para el tema de estudio.

Estrategia de búsqueda

La búsqueda bibliográfica se realizó en diversas bases de datos académicas reconocidas por su relevancia en el ámbito jurídico, social y tecnológico. Entre las principales bases de datos consultadas se encuentran Scopus, Web of Science, Scielo, Google Scholar, Redalyc y Dialnet, las cuales contienen literatura científica revisada por pares y publicaciones académicas relevantes en el campo del derecho, las ciencias sociales y los estudios tecnológicos.

Adicionalmente, se revisaron fuentes institucionales y jurídicas especializadas, tales como:

- bases de jurisprudencia de la Suprema Corte de Justicia de la Nación de México,
- sentencias y opiniones consultivas de la Corte Interamericana de Derechos Humanos,
- informes de organismos internacionales y organizaciones especializadas en derechos digitales.

La estrategia de búsqueda se realizó mediante la combinación de palabras clave en español e inglés utilizando operadores booleanos (AND, OR). Entre los principales términos utilizados se incluyen:

- “spyware”
- “vigilancia digital”
- “intervención de comunicaciones”
- “debido proceso”
- “derechos humanos”
- “proceso penal acusatorio”
- “digital surveillance”
- “privacy rights”
- “criminal procedure”
- “Pegasus spyware”

Un ejemplo de cadena de búsqueda utilizada fue:

("spyware" OR "digital surveillance") AND ("due process" OR "criminal procedure") AND ("Mexico" OR "Inter-American Court of Human Rights").

El período de búsqueda comprendió publicaciones entre 2010 y 2025, considerando que durante este periodo se produjo un crecimiento significativo de la literatura sobre vigilancia digital, derechos humanos y tecnologías de espionaje.

Criterios de inclusión y exclusión

Para garantizar la pertinencia y calidad de la información analizada, se establecieron criterios específicos de inclusión y exclusión.

Criterios de inclusión

Se incluyeron en el análisis:

- artículos científicos revisados por pares,
- libros y capítulos de libros académicos,
- documentos jurídicos relevantes,
- informes institucionales sobre vigilancia digital,
- jurisprudencia de tribunales nacionales e internacionales.

Los documentos seleccionados debían abordar al menos uno de los siguientes temas:

1. uso de spyware o tecnologías de vigilancia digital,

2. derecho a la privacidad y protección de datos,
3. debido proceso en el sistema penal,
4. estándares jurisprudenciales sobre intervención de comunicaciones.

Criterios de exclusión

Se excluyeron del análisis:

- documentos duplicados,
- artículos sin revisión académica o con escaso rigor metodológico,
- publicaciones que no abordaran directamente la relación entre vigilancia digital y derechos fundamentales,
- textos sin acceso completo o con información insuficiente para el análisis.

Proceso de selección de estudios

El proceso de selección de documentos se desarrolló en varias etapas siguiendo el modelo PRISMA.

En la fase de identificación, se localizaron inicialmente un total de documentos provenientes de las diferentes bases de datos consultadas. Posteriormente, en la fase de cribado, se eliminaron registros duplicados y se realizó una revisión preliminar de títulos y resúmenes para verificar su relevancia con respecto al tema de investigación.

En la fase de elegibilidad, los textos seleccionados fueron analizados en su totalidad con el fin de evaluar su pertinencia temática, calidad académica y contribución al análisis del problema de investigación.

En la fase de inclusión, se seleccionaron los documentos que cumplían con todos los criterios establecidos y que aportaban evidencia relevante para el desarrollo del estudio.

Este proceso sistemático permitió reducir progresivamente el número de documentos hasta conformar el corpus final de análisis utilizado en la investigación.

Categorías de análisis

Para el análisis de la información recopilada se establecieron diversas categorías analíticas, definidas a partir de la revisión de la literatura y de los objetivos de investigación. Estas categorías permitieron organizar la información y facilitar la interpretación crítica de los hallazgos.

Las principales categorías de análisis fueron las siguientes:

1. Vigilancia digital y spyware

   Se analizaron las características técnicas, el funcionamiento y las implicaciones jurídicas del uso de software de espionaje digital en el contexto de la seguridad pública y la investigación penal.

2. Derecho a la privacidad y protección de datos personales

   Esta categoría permitió examinar el alcance del derecho a la privacidad en el entorno digital, así como los estándares jurídicos relacionados con la protección de la información personal frente a la vigilancia estatal.

3. Debido proceso en el sistema penal acusatorio

   Se analizaron los principios fundamentales del debido proceso y su aplicación en la obtención de pruebas mediante tecnologías de vigilancia.

4. Marco normativo mexicano

   Se revisaron las disposiciones constitucionales y legales que regulan la intervención de comunicaciones privadas y el uso de herramientas tecnológicas en la investigación penal.

5. Jurisprudencia de la Suprema Corte de Justicia de la Nación

   Se analizaron precedentes judiciales relevantes relacionados con la protección de la privacidad, la intervención de comunicaciones y los límites del poder estatal en materia de vigilancia.

6. Estándares del sistema interamericano de derechos humanos

   Se examinaron las sentencias y criterios desarrollados por la Corte Interamericana de Derechos Humanos en relación con la vigilancia estatal y la protección de los derechos fundamentales.

Análisis de la información

Una vez seleccionados los documentos finales, se procedió a realizar un análisis cualitativo de contenido, orientado a identificar patrones conceptuales, tendencias jurisprudenciales y debates doctrinales en torno al uso del spyware en el ámbito de la justicia penal. Este proceso implicó la lectura crítica de las fuentes, la codificación temática de la información y la comparación de los diferentes enfoques presentes en la literatura y en los precedentes judiciales.

La síntesis de los resultados permitió identificar convergencias y divergencias entre las diferentes perspectivas analizadas, así como los principales desafíos jurídicos asociados con la regulación de las tecnologías de vigilancia digital en el contexto del sistema penal acusatorio mexicano.

RESULTADOS Y DISCUSIÓN

1. Vigilancia digital y spyware en la investigación penal contemporánea

El desarrollo de tecnologías digitales ha transformado profundamente los mecanismos de vigilancia utilizados por los Estados para la prevención e investigación de delitos. Entre estas herramientas, el spyware se ha consolidado como una de las tecnologías más sofisticadas de monitoreo digital, debido a su capacidad para infiltrarse en dispositivos electrónicos y obtener acceso remoto a información personal sin el conocimiento del usuario. Esta capacidad tecnológica ha ampliado significativamente las posibilidades de las autoridades para recopilar información en investigaciones criminales, pero también ha generado importantes debates jurídicos y éticos relacionados con el respeto a los derechos fundamentales y los límites del poder estatal en sociedades democráticas (Deibert, 2019).

El spyware puede definirse como un tipo de software diseñado para recopilar información de un dispositivo informático sin el consentimiento del usuario, permitiendo el acceso a datos personales, comunicaciones privadas, registros de actividad digital y ubicaciones geográficas. En algunos casos, estas herramientas también pueden activar funciones del dispositivo, como la cámara o el micrófono, lo que incrementa su potencial intrusivo en la vida privada de las personas (Solove, 2008). Desde una perspectiva tecnológica, estas herramientas se insertan dentro de lo que algunos autores denominan el "ecosistema de vigilancia digital", caracterizado por el uso de tecnologías avanzadas para monitorear comportamientos individuales y recopilar grandes volúmenes de datos (Lyon, 2018).

En el ámbito de la investigación penal, los Estados han justificado el uso de spyware como una herramienta necesaria para enfrentar delitos complejos que utilizan tecnologías digitales para ocultar sus actividades, como el terrorismo, el crimen organizado y la ciberdelincuencia. Estas amenazas han impulsado a los gobiernos a adoptar estrategias de vigilancia cada vez más sofisticadas, con el objetivo de anticipar conductas delictivas y recopilar evidencia digital que pueda utilizarse en procesos judiciales (Deibert, 2019). Sin embargo, el uso de estas tecnologías plantea importantes interrogantes sobre su compatibilidad con los principios fundamentales del derecho penal y del Estado de derecho.

Uno de los principales debates en torno al spyware se relaciona con su potencial para generar prácticas de vigilancia masiva o indiscriminada. A diferencia de otras técnicas tradicionales de investigación criminal, como la intervención telefónica autorizada judicialmente, el spyware puede recopilar una

cantidad mucho mayor de información personal, incluyendo datos que no necesariamente están relacionados con la investigación penal en curso. Esto genera el riesgo de que las autoridades accedan a información privada que excede los límites de la investigación legítima, lo que puede constituir una violación del derecho a la privacidad y de otras libertades fundamentales (Solove, 2008).

El caso del software Pegasus ha ilustrado de manera particularmente clara los riesgos asociados con el uso de spyware en contextos democráticos. Diversas investigaciones internacionales han documentado el uso de este software para espiar a periodistas, activistas y opositores políticos en distintos países, lo que ha generado preocupaciones significativas sobre la falta de controles efectivos en el uso de estas tecnologías (Marczak et al., 2018). En el caso de México, estos hallazgos han desencadenado un amplio debate sobre la necesidad de fortalecer los mecanismos de supervisión judicial y de transparencia en la adquisición y uso de herramientas de vigilancia digital.

Desde una perspectiva jurídica, el uso de spyware plantea desafíos importantes para los marcos normativos tradicionales que regulan la intervención de comunicaciones privadas. Muchas de estas normas fueron diseñadas en un contexto tecnológico diferente, en el que las comunicaciones se realizaban principalmente a través de medios telefónicos o electrónicos menos complejos. En contraste, las tecnologías actuales permiten acceder a grandes volúmenes de datos almacenados en dispositivos personales, lo que amplía significativamente el alcance de la vigilancia estatal (Lyon, 2018).

Otro aspecto relevante del debate se relaciona con la dificultad para detectar el uso de spyware y para demostrar su utilización en procesos judiciales. Debido a su naturaleza encubierta, estos programas suelen operar sin dejar rastros evidentes en los dispositivos infectados, lo que dificulta que las víctimas puedan demostrar que han sido objeto de vigilancia ilegal. Esta situación genera desafíos importantes para la protección de los derechos fundamentales y para la rendición de cuentas de las autoridades responsables (Deibert, 2019).

El uso de spyware plantea interrogantes sobre la legitimidad de las pruebas obtenidas mediante estas herramientas. En muchos sistemas jurídicos, la evidencia obtenida mediante métodos que vulneran derechos fundamentales puede ser considerada ilícita y, por lo tanto, inadmisible en un proceso penal. Este principio, conocido como la doctrina de la prueba ilícita o “fruto del árbol envenenado”, busca

garantizar que el Estado respete los límites legales en la obtención de evidencia y que no se beneficie de prácticas ilegales (Carbonell, 2013).

Desde esta perspectiva, la incorporación de tecnologías de vigilancia digital en la investigación penal exige un replanteamiento de los marcos normativos y de los mecanismos de control institucional que regulan estas prácticas. Los Estados deben garantizar que el uso de spyware se realice únicamente en circunstancias excepcionales, bajo estrictos controles judiciales y conforme a principios de necesidad, proporcionalidad y legalidad. De lo contrario, existe el riesgo de que estas herramientas se utilicen de manera abusiva, erosionando las garantías del debido proceso y debilitando la confianza de la ciudadanía en las instituciones de justicia.

La vigilancia digital mediante spyware representa uno de los desafíos más complejos para los sistemas jurídicos contemporáneos. Si bien estas tecnologías pueden contribuir a fortalecer las capacidades de investigación del Estado, su utilización debe estar sujeta a límites claros y a mecanismos de supervisión efectivos que garanticen el respeto de los derechos fundamentales. El análisis de estos desafíos resulta particularmente relevante en el contexto del sistema penal acusatorio mexicano, donde el respeto al debido proceso constituye un principio fundamental para la legitimidad de la justicia penal.

Derecho a la privacidad y protección de datos personales frente a la vigilancia estatal

El derecho a la privacidad constituye uno de los pilares fundamentales del sistema internacional de derechos humanos y se encuentra estrechamente vinculado con la protección de la dignidad humana y la autonomía individual. En términos generales, este derecho se refiere a la facultad de las personas para controlar el acceso a su vida personal y a la información que les concierne, evitando interferencias arbitrarias o abusivas por parte del Estado o de terceros (Solove, 2008). En el contexto de las sociedades contemporáneas, caracterizadas por una creciente digitalización de las comunicaciones y de las interacciones sociales, la protección de la privacidad ha adquirido una relevancia aún mayor.

La expansión de las tecnologías digitales ha generado nuevas formas de recopilación y tratamiento de datos personales que desafían los marcos jurídicos tradicionales de protección de la privacidad. El uso de spyware por parte de las autoridades constituye una de las manifestaciones más intrusivas de la vigilancia estatal, ya que permite acceder de manera remota a dispositivos electrónicos y recopilar información privada sin el conocimiento ni el consentimiento de las personas afectadas (Deibert, 2019).

Esta capacidad tecnológica plantea interrogantes fundamentales sobre los límites del poder estatal y sobre la necesidad de establecer mecanismos efectivos de regulación y supervisión.

Desde el punto de vista jurídico, el derecho a la privacidad se encuentra reconocido en diversos instrumentos internacionales de derechos humanos. El Pacto Internacional de Derechos Civiles y Políticos establece que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y que toda persona tiene derecho a la protección de la ley contra tales injerencias (Naciones Unidas, 1966). De manera similar, la Convención Americana sobre Derechos Humanos reconoce el derecho a la protección de la honra y de la dignidad, prohibiendo las interferencias arbitrarias o abusivas en la vida privada de las personas.

La jurisprudencia de los tribunales internacionales ha desarrollado estándares importantes para la protección de la privacidad frente a la vigilancia estatal. En particular, la Corte Interamericana de Derechos Humanos ha establecido que cualquier medida de intervención en las comunicaciones privadas debe cumplir con requisitos estrictos de legalidad, finalidad legítima, necesidad y proporcionalidad (Corte IDH, 2012). Estos criterios buscan garantizar que las restricciones a la privacidad se realicen únicamente cuando sean indispensables para alcanzar un objetivo legítimo y cuando no existan medios menos invasivos para lograrlo.

En el caso de México, la Constitución reconoce el derecho a la inviolabilidad de las comunicaciones privadas, estableciendo que únicamente la autoridad judicial puede autorizar su intervención mediante una resolución fundada y motivada. Esta disposición busca proteger la privacidad de las personas frente a posibles abusos de poder por parte de las autoridades, garantizando que cualquier forma de vigilancia estatal esté sujeta a controles institucionales (Fix-Zamudio, 2017). No obstante, la aparición de tecnologías como el spyware plantea nuevos desafíos para la aplicación efectiva de estas garantías constitucionales.

Uno de los principales problemas relacionados con la protección de la privacidad en el contexto de la vigilancia digital radica en la asimetría de poder entre el Estado y los individuos. Las autoridades gubernamentales cuentan con recursos tecnológicos y capacidades técnicas que les permiten acceder a grandes volúmenes de información personal, mientras que los ciudadanos suelen tener un conocimiento limitado sobre las herramientas utilizadas para recopilar y analizar estos datos (Lyon, 2018). Esta

situación puede generar un desequilibrio que debilite la capacidad de las personas para defender sus derechos frente a posibles abusos de vigilancia.

Otro aspecto relevante se relaciona con el impacto que la vigilancia digital puede tener sobre otras libertades fundamentales. Diversos estudios han señalado que la percepción de estar siendo vigilado puede generar efectos inhibitorios en el ejercicio de la libertad de expresión, la libertad de prensa y la participación política, especialmente en contextos donde periodistas y activistas pueden ser objeto de monitoreo por parte de las autoridades (Solove, 2008). En este sentido, la protección de la privacidad no solo constituye un derecho individual, sino también una condición necesaria para el funcionamiento de una sociedad democrática.

En consecuencia, el análisis del uso de spyware en el contexto del sistema penal acusatorio mexicano requiere considerar no solo las implicaciones tecnológicas de estas herramientas, sino también su impacto en la protección de los derechos fundamentales. La regulación adecuada de la vigilancia digital debe buscar un equilibrio entre la necesidad de garantizar la seguridad pública y la obligación de proteger la privacidad y la dignidad de las personas.

Debido proceso en el sistema penal acusatorio frente al uso de tecnologías de vigilancia digital

El debido proceso constituye uno de los principios fundamentales del Estado de derecho y representa una garantía esencial para la protección de los derechos humanos dentro de los sistemas de justicia penal. En términos generales, el debido proceso se refiere al conjunto de garantías jurídicas que deben observarse en cualquier procedimiento judicial o administrativo para asegurar que las personas sean tratadas de manera justa, imparcial y conforme a la ley (Fix-Zamudio & Valencia Carmona, 2015). En el ámbito del derecho penal, este principio adquiere una relevancia particular, ya que limita el ejercicio del poder punitivo del Estado y protege a los individuos frente a posibles abusos de autoridad.

En el contexto del sistema penal acusatorio mexicano, instaurado formalmente mediante la reforma constitucional de 2008, el debido proceso se encuentra estrechamente vinculado con principios como la presunción de inocencia, la igualdad entre las partes, la publicidad del proceso, la contradicción de las pruebas y la legalidad en la obtención de la evidencia (Carbonell, 2013). Estos principios buscan garantizar que las investigaciones y los juicios penales se desarrollen dentro de un marco de

transparencia y respeto a los derechos fundamentales, evitando prácticas arbitrarias o ilegales por parte de las autoridades encargadas de la persecución penal.

Sin embargo, la incorporación de tecnologías de vigilancia digital, como el spyware, plantea nuevos desafíos para la aplicación efectiva del debido proceso. Estas herramientas permiten acceder a grandes cantidades de información almacenada en dispositivos electrónicos, lo que puede incluir comunicaciones privadas, archivos personales, registros de navegación y datos de ubicación. Si bien esta información puede resultar útil para la investigación de delitos, su obtención mediante mecanismos invasivos plantea interrogantes sobre la legalidad y legitimidad de las pruebas obtenidas (Deibert, 2019).

Uno de los aspectos centrales del debido proceso en el ámbito de la investigación penal se relaciona con la obtención lícita de la prueba. De acuerdo con los principios del derecho procesal penal, las autoridades deben respetar las garantías constitucionales y legales al momento de recopilar evidencia, de manera que cualquier prueba obtenida mediante violaciones a los derechos fundamentales pueda ser declarada inadmisible en el juicio. Este principio se encuentra estrechamente relacionado con la doctrina de la prueba ilícita, la cual establece que la evidencia obtenida de forma ilegal no puede ser utilizada para sustentar una acusación penal (Carbonell, 2013).

En el caso del spyware, la aplicación de esta doctrina adquiere una complejidad adicional debido a la naturaleza encubierta de estas tecnologías. A diferencia de otros métodos tradicionales de investigación, como los cateos o las intervenciones telefónicas, el uso de software de espionaje digital puede realizarse sin dejar evidencias visibles de la intrusión en los dispositivos afectados. Esta característica dificulta que las personas investigadas puedan conocer que han sido objeto de vigilancia y, en consecuencia, limita su capacidad para impugnar la legalidad de las pruebas obtenidas (Deibert, 2019).

Otro aspecto relevante del debate se relaciona con el principio de proporcionalidad, el cual exige que cualquier medida restrictiva de derechos fundamentales sea adecuada, necesaria y proporcional para alcanzar un objetivo legítimo. En el contexto del uso de spyware, este principio implica que las autoridades deben demostrar que la intervención digital es indispensable para la investigación de un delito grave y que no existen medios menos invasivos para obtener la información requerida (Alexy,

2010). La aplicación de este principio resulta fundamental para evitar que las tecnologías de vigilancia se utilicen de manera indiscriminada o desproporcionada.

El debido proceso también exige que las personas investigadas tengan la posibilidad de conocer y controvertir las pruebas presentadas en su contra. Este principio, conocido como derecho de defensa, constituye un elemento esencial del sistema penal acusatorio, ya que garantiza la igualdad de condiciones entre la acusación y la defensa en el desarrollo del juicio (Fix-Zamudio & Valencia Carmona, 2015). Sin embargo, cuando la evidencia se obtiene mediante herramientas tecnológicas complejas como el spyware, pueden surgir dificultades para que las partes comprendan plenamente el origen y la fiabilidad de la información recopilada.

En este sentido, diversos autores han señalado la necesidad de fortalecer los mecanismos de control judicial y de transparencia en el uso de tecnologías de vigilancia digital. Estos mecanismos pueden incluir la exigencia de autorizaciones judiciales específicas para el uso de spyware, la implementación de auditorías independientes sobre las herramientas utilizadas por las autoridades y la obligación de notificar a las personas afectadas una vez concluida la investigación (Lyon, 2018).

La incorporación de tecnologías de vigilancia digital en el sistema penal acusatorio plantea desafíos significativos para la protección del debido proceso. Si bien estas herramientas pueden contribuir a mejorar las capacidades de investigación del Estado, su utilización debe estar sujeta a estrictos controles legales y judiciales que garanticen el respeto de las garantías procesales y eviten posibles abusos de poder.

Marco normativo mexicano sobre intervención de comunicaciones y vigilancia digital

El marco normativo mexicano establece diversas disposiciones destinadas a regular la intervención de comunicaciones privadas y el uso de herramientas de vigilancia en el ámbito de la investigación penal. Estas normas buscan equilibrar dos objetivos fundamentales del sistema jurídico: por un lado, la necesidad de garantizar la seguridad pública y combatir la delincuencia; y por otro, la obligación de proteger los derechos fundamentales de las personas, especialmente el derecho a la privacidad y las garantías del debido proceso (Fix-Zamudio, 2017).

La Constitución Política de los Estados Unidos Mexicanos reconoce en su artículo 16 el principio de inviolabilidad de las comunicaciones privadas, estableciendo que únicamente la autoridad judicial

puede autorizar su intervención mediante una resolución fundada y motivada. Esta disposición representa una de las principales garantías constitucionales frente a posibles abusos de vigilancia por parte del Estado, ya que exige la existencia de un control judicial previo antes de que las autoridades puedan acceder a las comunicaciones de una persona (Carbonell, 2013).

Además del marco constitucional, la legislación mexicana incluye diversas normas que regulan las técnicas de investigación relacionadas con la vigilancia digital. Entre ellas se encuentran el Código Nacional de Procedimientos Penales y diversas leyes en materia de seguridad nacional y telecomunicaciones, las cuales establecen los procedimientos y requisitos que deben cumplir las autoridades para intervenir comunicaciones o acceder a información digital en el contexto de investigaciones criminales.

Estas disposiciones legales suelen exigir que las autoridades presenten ante un juez una solicitud debidamente fundamentada que justifique la necesidad de la medida de vigilancia. El juez debe evaluar si la intervención solicitada cumple con los principios de legalidad, necesidad y proporcionalidad, así como verificar que exista una investigación en curso relacionada con delitos graves (Fix-Zamudio & Valencia Carmona, 2015). Este procedimiento busca garantizar que la vigilancia estatal se realice dentro de los límites establecidos por la ley y bajo la supervisión de una autoridad judicial independiente.

Sin embargo, la aparición de tecnologías avanzadas como el spyware ha generado cuestionamientos sobre la capacidad del marco normativo existente para regular adecuadamente estas prácticas. Muchas de las normas que regulan la intervención de comunicaciones fueron diseñadas en un contexto tecnológico anterior al desarrollo de herramientas de espionaje digital capaces de acceder a dispositivos completos y recopilar grandes cantidades de datos personales (Deibert, 2019).

Esta situación ha llevado a diversos especialistas a señalar la existencia de vacíos legales en la regulación de la vigilancia digital. En particular, se ha cuestionado si las disposiciones actuales sobre intervención de comunicaciones pueden aplicarse de manera efectiva al uso de software de espionaje que permite acceder no solo a comunicaciones en curso, sino también a información almacenada en dispositivos electrónicos (Lyon, 2018).

La falta de transparencia en la adquisición y uso de herramientas de vigilancia por parte de algunas instituciones gubernamentales ha generado preocupaciones sobre la rendición de cuentas y el control

democrático de estas prácticas. En varios casos, la información relacionada con los contratos y las capacidades técnicas de los sistemas de espionaje ha sido clasificada como información reservada, lo que dificulta el escrutinio público y el debate sobre su legalidad.

En consecuencia, el análisis del marco normativo mexicano revela la necesidad de actualizar las regulaciones existentes para adaptarlas a las nuevas realidades tecnológicas. Esto implica no solo establecer reglas claras sobre el uso de spyware en investigaciones penales, sino también fortalecer los mecanismos de supervisión judicial, transparencia institucional y protección de los derechos fundamentales.

Jurisprudencia de la Suprema Corte de Justicia de la Nación sobre privacidad y vigilancia estatal

La Suprema Corte de Justicia de la Nación ha desempeñado un papel fundamental en la interpretación de las normas constitucionales relacionadas con la protección de la privacidad y la intervención de comunicaciones privadas. A través de su jurisprudencia, el máximo tribunal mexicano ha desarrollado criterios que buscan delimitar los alcances del poder estatal en materia de vigilancia y garantizar el respeto de los derechos fundamentales de las personas (Fix-Zamudio, 2017).

Uno de los principios centrales establecidos por la jurisprudencia constitucional es la necesidad de contar con autorización judicial previa para la intervención de comunicaciones privadas. Este requisito se deriva directamente del artículo 16 de la Constitución y constituye una garantía esencial para evitar prácticas de vigilancia arbitraria por parte de las autoridades. La Suprema Corte ha reiterado en diversas decisiones que cualquier forma de intervención en la esfera privada de las personas debe estar debidamente justificada y sujeta a control judicial (Carbonell, 2013).

Además, la Corte ha desarrollado criterios relacionados con la protección del derecho a la privacidad en el contexto de las nuevas tecnologías. En varias resoluciones, el tribunal ha reconocido que la evolución de las tecnologías de la información plantea nuevos desafíos para la protección de los derechos fundamentales y que los principios constitucionales deben interpretarse de manera dinámica para responder a estas transformaciones (Fix-Zamudio & Valencia Carmona, 2015).

En este sentido, la Suprema Corte ha enfatizado la importancia de aplicar el principio de proporcionalidad al analizar medidas de vigilancia estatal. De acuerdo con este principio, cualquier restricción al derecho a la privacidad debe cumplir con tres requisitos fundamentales: ser adecuada para

alcanzar un objetivo legítimo, ser necesaria en ausencia de alternativas menos restrictivas y ser proporcional en relación con el beneficio que se pretende obtener (Alexy, 2010).

La jurisprudencia también ha abordado el problema de la prueba ilícita en el ámbito del proceso penal. La Corte ha señalado que las pruebas obtenidas mediante violaciones a los derechos fundamentales no pueden ser utilizadas en un juicio penal, ya que su admisión comprometería la legitimidad del sistema de justicia y vulneraría las garantías del debido proceso (Carbonell, 2013). Este criterio resulta especialmente relevante en el contexto del uso de spyware, donde existe el riesgo de que la evidencia sea obtenida mediante prácticas de vigilancia que no cumplen con los requisitos legales establecidos.

En conjunto, la jurisprudencia de la Suprema Corte refleja una creciente preocupación por garantizar que el uso de tecnologías de vigilancia se realice dentro de los límites establecidos por la Constitución. No obstante, el desarrollo de nuevas herramientas tecnológicas plantea desafíos adicionales que requieren una interpretación continua y evolutiva de los principios constitucionales.

Estándares de la Corte Interamericana de Derechos Humanos sobre vigilancia estatal y debido proceso

La Corte Interamericana de Derechos Humanos ha desarrollado una jurisprudencia amplia en materia de protección de la privacidad, vigilancia estatal y garantías del debido proceso. Sus decisiones han establecido estándares jurídicos que los Estados miembros del sistema interamericano deben observar al adoptar medidas de vigilancia que puedan afectar los derechos fundamentales de las personas (Corte IDH, 2012).

Uno de los principios centrales establecidos por la Corte es que cualquier intervención en las comunicaciones privadas debe cumplir con requisitos estrictos de legalidad, necesidad y proporcionalidad. Esto significa que las medidas de vigilancia solo pueden adoptarse cuando estén previstas en la ley, persigan un objetivo legítimo y sean indispensables para alcanzar dicho objetivo sin afectar de manera desproporcionada los derechos de las personas (Corte IDH, 2012).

Además, la Corte ha enfatizado la importancia de que las medidas de vigilancia estén sujetas a control judicial independiente y a mecanismos efectivos de supervisión. Estos controles buscan garantizar que las autoridades no utilicen las herramientas de vigilancia de manera arbitraria o abusiva, y que las personas afectadas tengan la posibilidad de impugnar la legalidad de dichas medidas.

Otro aspecto relevante de la jurisprudencia interamericana se relaciona con la obligación de los Estados de proteger el ejercicio de la libertad de expresión y el trabajo de periodistas y defensores de derechos humanos. La Corte ha señalado que la vigilancia indebida de estos actores puede tener un efecto inhibidor sobre el debate público y la participación democrática, lo que constituye una amenaza para el funcionamiento de las sociedades democráticas.

En el contexto del uso de spyware, estos estándares resultan particularmente relevantes, ya que las tecnologías de vigilancia digital tienen el potencial de afectar de manera significativa la privacidad y las libertades fundamentales. Por esta razón, diversos especialistas han señalado la necesidad de aplicar los criterios desarrollados por la Corte Interamericana al analizar la legalidad del uso de estas herramientas en investigaciones penales (Deibert, 2019).

La jurisprudencia de la Corte Interamericana proporciona un marco normativo robusto para evaluar la compatibilidad de las prácticas de vigilancia estatal con los derechos humanos. La incorporación de estos estándares en el derecho interno de los países de la región constituye un elemento clave para garantizar que el uso de tecnologías de espionaje digital se realice dentro de los límites establecidos por el derecho internacional de los derechos humanos.

Tabla 1: Síntesis principales hallazgos

Categoría de análisis	Aspectos analizados	Principales hallazgos de la revisión	Implicaciones jurídicas y teóricas
1. Vigilancia digital y spyware en la investigación penal	Concepto de spyware, funcionamiento tecnológico, uso en investigaciones criminales, casos documentados de vigilancia digital.	La literatura muestra que el spyware constituye una herramienta altamente invasiva capaz de acceder a información privada almacenada en dispositivos electrónicos. Su utilización ha sido justificada por los Estados para combatir delitos complejos como el crimen organizado o el terrorismo. Sin embargo, diversos estudios evidencian que estas tecnologías también han sido utilizadas para vigilar a periodistas, activistas y actores políticos, lo que genera preocupaciones sobre posibles abusos de poder.	Se evidencia la necesidad de establecer marcos regulatorios más claros que delimiten el uso de tecnologías de vigilancia digital. El spyware plantea desafíos significativos para el equilibrio entre seguridad pública y protección de derechos fundamentales.
2. Derecho a la privacidad y protección de datos personales	Alcance del derecho a la privacidad en el entorno digital, protección de datos personales, estándares	El análisis de la literatura muestra que la vigilancia digital puede afectar gravemente la privacidad y la autonomía individual. Instrumentos internacionales como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre	La protección de la privacidad se consolida como un elemento central en la regulación de la vigilancia digital. La literatura destaca la necesidad de aplicar criterios de legalidad, necesidad y

Categoría de análisis	Aspectos analizados	Principales hallazgos de la revisión	Implicaciones jurídicas y teóricas
	internacionales de derechos humanos.	Derechos Humanos reconocen el derecho a la protección frente a interferencias arbitrarias en la vida privada. El uso de spyware incrementa los riesgos de vigilancia masiva y acceso indebido a datos personales.	proporcionalidad para legitimar cualquier intervención estatal en las comunicaciones privadas.
3. Debido proceso en el sistema penal acusatorio	Principios del debido proceso, presunción de inocencia, legalidad en la obtención de pruebas, prueba ilícita.	Los estudios analizados evidencian que el uso de tecnologías de espionaje digital puede comprometer las garantías del debido proceso si no se encuentra sujeto a controles judiciales estrictos. La obtención de evidencia mediante spyware plantea interrogantes sobre la legalidad de las pruebas y su admisibilidad en procesos penales.	El debido proceso exige que cualquier forma de vigilancia estatal esté sujeta a autorización judicial y a mecanismos de control que garanticen la legalidad de la evidencia obtenida. El uso de spyware requiere nuevas interpretaciones jurídicas para evitar vulneraciones a las garantías procesales.
4. Marco normativo mexicano sobre intervención de comunicaciones	Normas constitucionales, legislación penal, regulación de técnicas de investigación y vigilancia digital.	El análisis del marco jurídico mexicano muestra que la Constitución reconoce la inviolabilidad de las comunicaciones privadas y establece que su intervención solo puede realizarse con autorización judicial. No obstante, muchas normas fueron diseñadas antes del desarrollo de tecnologías de espionaje digital, lo que genera vacíos legales en su regulación.	Se identifica la necesidad de actualizar la legislación para adaptarla a las nuevas realidades tecnológicas. La regulación debe contemplar de manera específica el uso de herramientas de vigilancia digital y establecer mecanismos de transparencia y rendición de cuentas.
5. Jurisprudencia de la Suprema Corte de Justicia de la Nación	Interpretación constitucional sobre privacidad, intervención de comunicaciones y límites de la vigilancia estatal.	La jurisprudencia de la Suprema Corte ha reafirmado la necesidad de contar con autorización judicial previa para cualquier intervención en la esfera privada de las personas. El tribunal ha desarrollado criterios relacionados con la proporcionalidad de las medidas de vigilancia y con la exclusión de pruebas obtenidas de manera ilícita.	Los precedentes judiciales fortalecen la protección de los derechos fundamentales frente a prácticas de vigilancia arbitraria. Sin embargo, la evolución tecnológica exige que la jurisprudencia continúe desarrollando criterios específicos para regular el uso de herramientas de espionaje digital.
6. Estándares de la Corte Interamericana de Derechos Humanos	Jurisprudencia interamericana sobre privacidad, vigilancia estatal, libertad de expresión y debido proceso.	La Corte Interamericana ha establecido que las intervenciones en comunicaciones privadas solo son legítimas cuando cumplen con requisitos estrictos de legalidad, finalidad legítima, necesidad y proporcionalidad. Además, ha destacado la importancia del control judicial y de la protección de periodistas y defensores de derechos humanos frente a prácticas de vigilancia indebida.	Los estándares interamericanos constituyen un marco jurídico fundamental para evaluar la legalidad del uso de spyware en el ámbito penal. Su incorporación en el derecho interno fortalece la protección de los derechos humanos y promueve la armonización entre la normativa nacional y el derecho internacional.

Fuente: Elaboración propia

CONCLUSIONES

El presente artículo de revisión permitió analizar de manera crítica y sistemática el uso de tecnologías de vigilancia digital, particularmente el spyware, dentro del sistema penal acusatorio mexicano, examinando su relación con el principio del debido proceso y con los estándares jurídicos establecidos tanto en el derecho constitucional mexicano como en el sistema interamericano de derechos humanos. A partir de la revisión de la literatura especializada, del marco normativo vigente y de los precedentes jurisprudenciales relevantes, fue posible identificar los principales desafíos que plantea la incorporación de herramientas tecnológicas de espionaje digital en el ámbito de la investigación penal, así como las implicaciones que estas prácticas tienen para la protección de los derechos fundamentales en contextos democráticos.

En primer lugar, uno de los hallazgos más relevantes de esta revisión se relaciona con la creciente expansión de la vigilancia digital como herramienta utilizada por los Estados para enfrentar fenómenos delictivos complejos en la era de la información. El desarrollo acelerado de las tecnologías de comunicación y de almacenamiento de datos ha transformado profundamente las dinámicas de interacción social, económica y política, generando nuevas oportunidades, pero también nuevos riesgos en materia de seguridad. En este contexto, las autoridades encargadas de la persecución penal han incorporado herramientas tecnológicas cada vez más sofisticadas para obtener información relevante en investigaciones criminales, incluyendo el uso de software de espionaje digital capaz de acceder a dispositivos electrónicos de manera remota y recopilar grandes cantidades de datos personales.

Sin embargo, la revisión de la literatura evidencia que el uso de spyware constituye una de las formas más intrusivas de vigilancia estatal, ya que permite acceder no solo a comunicaciones privadas, sino también a archivos, fotografías, registros de actividad digital, ubicaciones geográficas y otros tipos de información altamente sensible almacenada en dispositivos electrónicos. Esta capacidad tecnológica amplía significativamente el alcance de la vigilancia estatal y plantea interrogantes fundamentales sobre los límites del poder público en sociedades democráticas. En este sentido, uno de los principales desafíos identificados en la investigación radica en la necesidad de garantizar que el uso de estas herramientas se realice dentro de un marco jurídico claro y conforme a los principios fundamentales del Estado de derecho.

En segundo lugar, el análisis realizado permitió confirmar que el derecho a la privacidad constituye uno de los derechos fundamentales más directamente afectados por el uso de tecnologías de vigilancia digital. La privacidad no solo protege la esfera íntima de las personas, sino que también se encuentra estrechamente vinculada con otros derechos fundamentales, como la libertad de expresión, la libertad de asociación y la participación política. Cuando las personas perciben que sus comunicaciones o actividades digitales pueden ser objeto de vigilancia, existe el riesgo de que se genere un efecto inhibidor que limite el ejercicio de estos derechos, afectando así el funcionamiento de las instituciones democráticas.

En el contexto de la vigilancia digital, la protección de la privacidad adquiere una complejidad adicional debido a la enorme cantidad de datos que pueden recopilarse mediante herramientas tecnológicas avanzadas. A diferencia de las formas tradicionales de vigilancia, como la intervención telefónica, el spyware permite acceder a sistemas completos de información personal, lo que puede implicar una intrusión mucho más profunda en la vida privada de las personas. Por esta razón, la literatura revisada enfatiza la necesidad de aplicar criterios estrictos de legalidad, necesidad y proporcionalidad para justificar cualquier forma de intervención estatal en la esfera privada.

Otro aspecto central que emerge de esta investigación se relaciona con el impacto del spyware en las garantías del debido proceso dentro del sistema penal acusatorio. Este modelo procesal, adoptado en México a partir de la reforma constitucional de 2008, se basa en principios como la presunción de inocencia, la igualdad entre las partes, la publicidad del proceso y la legalidad en la obtención de pruebas. Estas garantías buscan asegurar que los procedimientos penales se desarrollen de manera justa, transparente y respetuosa de los derechos humanos.

No obstante, el uso de tecnologías de vigilancia digital plantea desafíos importantes para la aplicación efectiva de estos principios. En particular, la obtención de evidencia mediante herramientas como el spyware puede generar dudas sobre la legalidad de las pruebas y sobre su admisibilidad en los procesos judiciales. La doctrina de la prueba ilícita establece que la evidencia obtenida mediante violaciones a los derechos fundamentales no puede ser utilizada para sustentar una acusación penal, ya que ello comprometería la legitimidad del sistema de justicia. En este sentido, el uso indebido de tecnologías de

espionaje digital podría dar lugar a la exclusión de pruebas y a la eventual nulidad de los procedimientos penales.

Además, la naturaleza encubierta del spyware genera dificultades adicionales para la protección del derecho de defensa. En muchos casos, las personas investigadas pueden desconocer que han sido objeto de vigilancia digital, lo que limita su capacidad para cuestionar la legalidad de las pruebas obtenidas en su contra. Esta situación plantea la necesidad de fortalecer los mecanismos de control judicial y de transparencia en el uso de tecnologías de vigilancia, con el fin de garantizar que las investigaciones penales se desarrollen dentro de los límites establecidos por el derecho.

En relación con el marco normativo mexicano, el análisis realizado permitió identificar avances importantes en la protección de la privacidad y de las comunicaciones privadas. La Constitución mexicana reconoce expresamente el principio de inviolabilidad de las comunicaciones y establece que cualquier intervención debe contar con autorización judicial previa, lo que constituye una garantía fundamental frente a posibles abusos de vigilancia. Diversas leyes en materia de procedimiento penal y telecomunicaciones establecen procedimientos específicos para la autorización y supervisión de técnicas de investigación que implican la intervención de comunicaciones.

Sin embargo, la revisión también evidencia que muchas de estas normas fueron diseñadas en un contexto tecnológico distinto al actual, lo que genera vacíos legales en la regulación de herramientas avanzadas de vigilancia digital. En particular, las disposiciones existentes no siempre contemplan de manera explícita el uso de software de espionaje que permite acceder a dispositivos completos y recopilar grandes volúmenes de información personal. Esta situación pone de manifiesto la necesidad de actualizar el marco jurídico para adaptarlo a las nuevas realidades tecnológicas y garantizar una regulación adecuada de estas prácticas.

En este escenario, la jurisprudencia de la Suprema Corte de Justicia de la Nación desempeña un papel fundamental en la interpretación de los principios constitucionales relacionados con la protección de la privacidad y las garantías del debido proceso. A través de sus decisiones, el máximo tribunal mexicano ha reafirmado la importancia de contar con autorización judicial previa para cualquier forma de intervención en las comunicaciones privadas y ha desarrollado criterios basados en el principio de proporcionalidad para evaluar la legitimidad de las medidas de vigilancia estatal.

Estos precedentes judiciales contribuyen a fortalecer la protección de los derechos fundamentales frente a posibles abusos de poder, pero también evidencian la necesidad de continuar desarrollando criterios específicos para enfrentar los desafíos planteados por las nuevas tecnologías de vigilancia. En particular, resulta necesario que la jurisprudencia constitucional aborde de manera más directa las implicaciones jurídicas del uso de spyware y establezca lineamientos claros para su regulación dentro del sistema penal acusatorio.

Por otro lado, la jurisprudencia de la Corte Interamericana de Derechos Humanos ofrece un marco normativo robusto para evaluar la compatibilidad de las prácticas de vigilancia estatal con los derechos humanos. Este tribunal ha establecido que cualquier intervención en las comunicaciones privadas debe cumplir con requisitos estrictos de legalidad, finalidad legítima, necesidad y proporcionalidad, además de estar sujeta a controles judiciales independientes y a mecanismos efectivos de supervisión.

La aplicación de estos estándares resulta especialmente relevante en el contexto del uso de spyware, ya que las tecnologías de vigilancia digital tienen el potencial de afectar de manera significativa la privacidad y las libertades fundamentales. La incorporación de los criterios desarrollados por la Corte Interamericana en el derecho interno de los países de la región contribuye a fortalecer la protección de los derechos humanos y a garantizar que las prácticas de vigilancia estatal se realicen dentro de los límites establecidos por el derecho internacional.

En términos generales, los resultados de esta revisión permiten concluir que el uso de spyware en el sistema penal acusatorio mexicano constituye un tema complejo que requiere un análisis jurídico multidimensional. Si bien estas tecnologías pueden contribuir a mejorar las capacidades de investigación del Estado y a enfrentar fenómenos delictivos cada vez más sofisticados, su utilización sin controles adecuados puede generar riesgos significativos para la protección de los derechos fundamentales.

Por esta razón, resulta fundamental promover reformas legislativas y políticas públicas que permitan regular de manera clara y transparente el uso de tecnologías de vigilancia digital. Estas reformas deben incluir la definición precisa de los supuestos en los que puede autorizarse el uso de spyware, el establecimiento de procedimientos judiciales rigurosos para su aprobación y la creación de mecanismos de supervisión independientes que garanticen la rendición de cuentas de las autoridades.

Es necesario fortalecer la capacitación de jueces, fiscales y defensores públicos en materia de tecnologías digitales y derechos humanos, con el fin de asegurar que las decisiones judiciales relacionadas con la vigilancia digital se basen en una comprensión adecuada de las implicaciones técnicas y jurídicas de estas herramientas.

El análisis desarrollado en este estudio pone de manifiesto la importancia de continuar investigando la relación entre tecnología, derecho y derechos humanos en el contexto de la justicia penal contemporánea. La rápida evolución de las tecnologías digitales plantea desafíos constantes para los sistemas jurídicos, lo que exige una reflexión permanente sobre los mecanismos más adecuados para garantizar la seguridad pública sin comprometer las libertades fundamentales que constituyen la base de las sociedades democráticas.

El uso de spyware en el sistema penal acusatorio mexicano debe analizarse desde una perspectiva que combine la eficacia en la persecución del delito con el respeto irrestricto a los derechos humanos. Solo a través de marcos normativos claros, controles judiciales efectivos y una interpretación jurisprudencial comprometida con la protección de la dignidad humana será posible garantizar que las tecnologías de vigilancia digital se utilicen de manera legítima y compatible con los principios del Estado de derecho.

REFERENCIAS BIBLIOGRAFICAS

American Convention on Human Rights. (1969). American Convention on Human Rights. Organization of American States.

Amnesty International. (2021). Forensic methodology report: How to catch NSO Group's Pegasus. Amnesty International.

Constitución Política de los Estados Unidos Mexicanos. (1917). Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación.

Corte Interamericana de Derechos Humanos. (2009). *Caso Escher y otros vs. Brasil*. Sentencia del 6 de julio de 2009.

Corte Interamericana de Derechos Humanos. (2015). Caso Tristán Donoso vs. Panamá. Sentencia del 27 de enero de 2009.

Corte Interamericana de Derechos Humanos. (2018). Caso López Lone y otros vs. Honduras. Sentencia del 5 de octubre de 2015.

Deibert, R. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy*, 30(1), 25–39.

Deibert, R., Scott-Railton, J., & Marczak, B. (2020). Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries. Citizen Lab, University of Toronto.

Dworkin, R. (1977). Taking rights seriously. Harvard University Press.

Electronic Frontier Foundation. (2022). *Go*vernment hacking and surveillance: Legal and ethical challenge*s*. EFF Publications.

Ferrajoli, L. (2001). Derecho y razón: Teoría del garantismo penal. Trotta.

Foucault, M. (1977). Discipline and punish: The birth of the prison. Pantheon Books.

International Covenant on Civil and Political Rights. (1966). United Nations.

Kerr, O. S. (2010). *T*he Fourth Amendment and new technologies: Constitutional myths and the case for caution. Michigan Law Review, 102(5), 801–888.

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.

Marczak, B., Scott-Railton, J., McKune, S., Razzak, B., & Deibert, R. (2018). Hide and seek: Tracking NSO Group's Pegasus spyware. Citizen Lab Research Report.

Naciones Unidas. (2014). The right to privacy in the digital age. United Nations General Assembly.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Solove, D. J. (2007). "I've got nothing to hide" and other misunderstandings of privacy. San Diego Law Review, 44(4), 745–772.

Solove, D. J. (2021). Understanding privacy. Harvard University Press.

Suprema Corte de Justicia de la Nación. (2014). Derecho a la inviolabilidad de las comunicaciones privadas. Jurisprudencia constitucional.

Suprema Corte de Justicia de la Nación. (2018). Intervención de comunicaciones privadas y control judicial. Jurisprudencia constitucional.

Suprema Corte de Justicia de la Nación. (2020). Derechos fundamentales y tecnologías de vigilancia. Jurisprudencia constitucional.

Transparency International. (2021). Surveillance technologies and democratic accountability. Transparency International Report.

Westin, A. (1967). Privacy and freedom. Atheneum.

Zuboff, S. (2019). The age of surveillance capitalism. Public Affairs.