CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS, A.C.

CASO PEGASUS: EL ESPIONAJE EN MÉXICO

TESINA

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

PRESENTA

IVÁN GARCÍA ARGUETA

DIRECTORA DE LA TESINA: DRA. MARÍA SOLANGE MAQUEO RAMÍREZ

CIUDAD DE MÉXICO 2021

AGRADECIMIENTOS:

A mis papás por haber estado ahí en cada paso de mi vida y por enseñarme a no perder a mi niño interior.
A cada persona que confío en mí y que me acompaño en este camino.
Esto fue gracias y para ustedes.

ÍNDICE

1 INTRODUCCIÓN

La tecnología avanza a pasos cada vez más grandes y cada vez es más evidente que el derecho no puede actualizarse a tiempo. Desde lo que pasa con la inteligencia artificial hasta los cambios más simples como las videoconferencias causan estragos para asegurar que exista justicia de acuerdo con las circunstancias actuales.

En México existen intentos fallidos por querer legislar o intentar regular nuevas tecnologías. Recientemente, se les pidió a los bancos que cada vez que un individuo realizara una transferencia electrónica, abriera una cuenta o celebrara un contrato, su aplicación de banco registraría su localización GPS. ¿Para qué? Los bancos tendrán que recolectar masivamente estos datos y dárselos a la autoridad, en cuanto lo requiera, todo bajo la bandera del combate al lavado de dinero y el financiamiento al terrorismo.

Otro caso actual es la creación de un "Padrón Nacional de Usuarios de Telefonía Móvil" en el que la autoridad propone que cada SIM comprada sea registrada con los datos biométricos del comprador para combatir los delitos de extorsión y delincuencia organizada. La autoridad argumenta que con este padrón podrá combatir de una mejor manera este tipo de delitos a pesar de que la evidencia en intentos pasados del uso de este tipo de herramientas fue que fracasó e incluso la base de datos fue robada y vendida en el mercado negro.[1]

Ahora, se presenta un reto que fue ignorado y que es un tema que inevitablemente va a volver a estar presente en la agenda pública. El uso de programas de vigilancia que puedan convertir al teléfono móvil en una máquina de espionaje. Este tipo de *spyware* rebasa actualmente los alcances de nuestra legislación y debido a su poca regulación ha sido usado contra ciudadanos mexicanos que ni siquiera tenían una investigación formal que justificara su uso. Los riesgos de dejar libre el uso de este tipo de *spyware* es que los derechos de los ciudadanos sean vulnerados en especial el derecho a la privacidad y el derecho a la protección de datos.

[1] R3D, "Recolección de datos de geolocalización de datos en banca en línea es desproporcionada riesgosa e innecesaria," *R3D*, 23 de marzo de 2021, https://r3d.mx/2021/03/23/recoleccion-de-datos-de-geolocalizacion-en-banca-en-linea-es-desproporcionada-riesgosa-e-innecesaria/.

La cuestión es que hasta ahora ha sido un problema gubernamental, pero ¿qué pasará cuando este tipo de *spywares* no necesariamente sean vendidos sólo a gobiernos? La discusión que desató la polémica en México fue el caso Pegasus, se discutirá más adelante, detonó una discusión necesaria e importante pero que, lamentablemente, no trajo consigo ningún cambio sustancial en la vida de los ciudadanos mexicanos. La autoridad se limitó a decir que había supuestamente ordenado su eliminación de los dispositivos de la Procuraduría General de la República (PGR) aunque posteriormente por vía de solicitud de información se comprobó que no habían recibido las autoridades esa orden.[2]

El uso de herramientas de vigilancia en México ha sido documentado por organizaciones como R3D e internacionalmente por organizaciones como *Citizen Lab*.
Dentro de los problemas documentados sobre este tipo de *spyware* son que se aprovechan de vulnerabilidades que el teléfono tiene de fábrica, su uso contra personas que no tienen ninguna investigación judicial activa, el mal uso o inclusive el no uso de autorizaciones judiciales para la utilización de estas herramientas.

Tal como R3D ha documentado vía solicitudes de información entre 2016 y 2017, el 85% de las técnicas de investigación que involucran algún tipo de autorización judicial se realizaron sin una autorización previa debido a que argumentaron una situación de emergencia. Aunque los jueces no ratificaron más del 45% de acceso a los datos conservados por las empresas de telecomunicaciones ni el 85% de las localizaciones geográficas.

Hay un gran abuso de ese tipo de herramientas de vigilancia y hay un gran avance en su desarrollo por lo que no van a desaparecer pronto. Debido a que el uso de herramientas como Pegasus son tecnología novedosa no hay en sí ninguna legislación dentro de lo investigado que prevea una regulación. Por lo que se analizará su fundamentación constitucional que es la intervención de comunicaciones. Tanto en el marco mexicano como en el internacional.

La pregunta de investigación de la tesis es la siguiente ¿Existe una normativa clara y actualizada respecto a las herramientas de vigilancia que proteja el derecho a la privacidad y la protección de datos personales? La hipótesis de la tesina es que no existe una regulación clara y actualizada que contemple estándares de derechos humanos junto con un correcto tratamiento

[2] Georgina Zerega y Pablo Ferri, "El Estado Mexicano se atraganta con el caso Pegasus," *El País*, 6 de agosto de 2020, https://elpais.com/mexico/2020-08-06/el-estado-mexicano-se-atraganta-con-el-caso-pegasus.html.

de datos por lo que viola el derecho a la privacidad y el derecho a la protección de datos personales de los ciudadanos.

La metodología usada para la elaboración del documento fue la siguiente. Para la primera parte de la tesina se consultó fuentes primarias respecto al marco jurídico mexicano. La legislación revisada fue la constitución política de México así como las leyes especiales que consideraban la intervención de comunicaciones aunque no fueran propiamente del ámbito penal como la Ley Federal de Telecomunicaciones y Radiodifusión. Al ser un tema regulado por diversas fuentes normativas seleccione las que reglaban el proceso para la intervención de comunicaciones. La fuente principal fue el Código Nacional de Procedimientos Penales al ser la normativa que reglamentaba a profundidad este proceso; además, de ser la normativa que sería aplicable al mayor número de casos de intervención de comunicaciones.

Asimismo, para la selección de jurisprudencia fueron escogidas aquellas sentencias de la Corte que trataban sobre el derecho a la privacidad y la protección de datos personales. Prestando un énfasis a que estuvieran relacionadas con la intervención de comunicaciones y los datos que se obtienen a partir de ella. Los amparos 964/2015 y 937/2015 ofrecen la jurisprudencia más actualizada respecto a estos temas. De igual manera, ofrecen la postura de la Corte y cómo entiende el derecho a la privacidad y la protección de datos personales.

Conjuntamente, fueron consultadas fuentes secundarias como reportes de ONG que explican el uso de herramientas de vigilancia que ha utilizado el Estado mexicano. Los reportes ofrecen un panorama amplio y documental acerca de los problemas que surgen al utilizar este tipo de herramientas para la intervención de comunicaciones. Asimismo, fueron consultadas fuentes periodísticas para hacer un recuento histórico del espionaje que ha hecho México contra sus ciudadanos. Estas fuentes ayuda a crear una línea histórica de las veces han sido usado estos nuevas herramientas de vigilancia en la población mexicana.

En la segunda parte de la tesina, fueron consultadas fuentes académicas para un análisis profundo de ambos derechos. El criterio para la selección de estas fuentes fue escoger textos que desarrollaran cada derecho a profundidad y de preferencia bajo el supuesto de la intervención de comunicaciones. De igual manera fue consultada normativa mexicana que regulara el derecho en concreto. Asimismo, fue consultada jurisprudencia que ofreciera un análisis del derecho a la luz de la intervención de comunicaciones.

En esta parte fue hecho un ejercicio de derecho comparado por lo que se consultaron fuentes primarias para entender su concepción del derecho en el contexto angloamericano. Para realizar este ejercicio fueron seleccionados cuatro casos significativos entorno al derecho a la privacidad y la tecnología. El criterio utilizado para su selección que trataran sobre el derecho a la privacidad en su dimensión de la inviolabilidad de comunicaciones o la esfera privada del individuo y que estuvieran relacionados con las nuevas tecnologías de vigilancia.

En la siguiente parte, para el contraste entre ambas legislaciones utilice la legislación americana que protegiera el derecho a la privacidad y que protegiera los datos personales. Asimismo, para el marco angloamericano seleccione legislación enfocada en la intervención de comunicaciones y las capacidades del Estado para vigilar a sus ciudadanos. En el caso mexicano utilice legislación que regulará la intervención de comunicaciones y protegiera ambos derechos para contrastarla; igualmente, que pudiera compararse con la angloamericana en cuanto a los contenidos regulados.

Finalmente, fueron utilizadas fuentes primarias como resoluciones de la ONU y autoridades expertas en la materia para ofrecer directrices y posibles soluciones a esta falta de normativa clara y actualizada que garantice ambos derechos.

Dicho lo anterior el trabajo estará dividido en tres partes. En el primer capítulo, se explicará ¿Qué fue el caso Pegasus en México? ¿Cómo funciona y dónde está presente ¿Cómo se diferencia su utilización respecto de una intervención de comunicación? y ¿Cómo operan este tipo de programas con los datos recopilados por empresas de telecomunicaciones? El segundo capítulo tratará sobre dos derechos fundamentales para hacer frente a arbitrariedades en vigilancia ¿Qué es el derecho a la privacidad? ¿Cómo opera en el marco jurídico mexicano? Debido al avance jurisprudencial y su gran avance en la discusión pública de los temas de vigilancia será analizado el derecho a la privacidad en el marco jurídico angloamericano.

Asimismo, en el capítulo se desmenuzará el derecho a la protección de datos y su protección jurídica en México. Conjuntamente, se hará una revisión a profundidad cómo la protección de datos juega un papel fundamental en la colaboración entre instancias de seguridad y empresas de telecomunicaciones. A manera de cierre del capítulo se hará una prueba de proporcionalidad en el cual demuestra jurídicamente cómo estos dos derechos deben de ser ponderados cuando un juez autorice la utilización de herramientas como Pegasus.

Finalmente, se hará un ejercicio de derecho comparado entre la legislación mexicana y la legislación angloamericana. Se compararán sus similitudes y sus diferencias para tener un panorama más completo de cómo funcionan y operan este tipo de programas en ambos territorios. Para concluir, se ofrecerán directrices que podrían ayudar a regular el uso indebido de este tipo de herramientas y explicar cómo México podría resolver el problema de la vigilancia indebida antes de que sea demasiado tarde.

2 CAPÍTULO I - CASO PEGASUS: ¿QUIENES SON LOS ENEMIGOS DEL ESTADO?

2.1 Pegasus*:*

"Somos los nuevos enemigos del Estado" no es una frase de un narcotraficante, una nueva banda de secuestradores o de un nuevo cartel que confronta al Estado, sino del ex director del Instituto Mexicano para la Competitividad (IMCO) después de que él, su esposa y múltiples periodistas fueron atacados con un spyware llamado Pegasus donde el principal sospechoso del ataque es el Estado Mexicano.

De 2015 a 2017 periodistas, científicos y miembros de la sociedad civil sufrieron múltiples ataques provenientes de este spyware. El primer caso documentado fue respecto de los aliados en la imposición de un impuesto a las bebidas azucaradas en 2014. El Dr. Simón Barquera, investigador del Instituto Nacional de Salud Pública, Alejandro Calvillo, director de la revista "El Poder del Consumidor" y Luis Encarnación, líder de la coalición de ONG ContraPESO que tiene como objetivo la prevención de la obesidad. Los ataques comenzaron después de una acalorada conferencia de prensa en 2016 donde los actores defendieron el impuesto, pidieron su incremento y criticaron la manera en la que se estaba gastando el impuesto.[3]

El modus operandi de Pegasus es el siguiente y se repite en todos los ataques en México. El primer paso consiste en enviarle un *SMS* al destinatario. Este mensaje está personalizado para atraer la atención del destinatario con temas polémicos que incitan al usuario a abrir el mensaje. El segundo paso es incitar al usuario a abrir un *enlace* que lleva a un sitio web falso sobre algún medio. Al abrir el enlace el celular queda infectado por el *spyware* Pegasus. El patrón de los ataques es el que se repetirá a lo largo de los futuros casos de espionaje doméstico en México.

El caso que detonó el escándalo de espionaje doméstico fue el ataque masivo hacia periodistas y miembros de la sociedad civil, todos críticos del sexenio de Peña Nieto. Entre los afectados estaba el Centro Prodh una asociación dedicada a la defensa y promoción de los

[3] John Scott - Railton, Claudio Guarneri y Masashi Nishihata, "BITTERSWEET: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links" (Citizen Lab Research Report No. 8, University of Toronto, 2017), https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

derechos humanos. El Centro estuvo activamente involucrado en la documentación y defensa de los 43 normalistas de Ayotzinapa, la ejecución extrajudicial de civiles por parte del ejército en Tlatlaya y ayudó a defender a los sobrevivientes de tortura sexual durante el operativo de Atenco en 2006. Todos estos casos fueron sumamente mediáticos y crueles, con claras posturas en contra del Estado Mexicano.[4]

Otra víctima fue el equipo de trabajo de Aristegui Noticias. En 2014 revelaron en su investigación "La Casa Blanca de Peña Nieto" la existencia de un inmueble de siete millones de dólares que fue un escándalo en el sexenio de Peña Nieto. Los tres periodistas de la investigación, Carmen Aristegui, Rafael Cabrera y Sebastián Barragán, e incluso el hijo de Aristegui, recibieron ataques por parte de Pegasus mediante el mismo *modus operandi*: un *SMS* personalizado que contiene un enlace infectado que posteriormente se apodera sutilmente del celular.

Las últimas víctimas documentadas fueron el periodista Carlos Loret de Mola que durante esos años publicó varias columnas de opinión acerca de ejecuciones extrajudiciales en Tanhuato y posteriormente columnas de opinión cuestionando las irregularidades de la captura del peligroso narcotraficante el Chapo. Todo esto le valió múltiples ataques a su privacidad mediante *el modus operandi* de Pegasus. Asimismo, la organización Mexicanos Contra la Corrupción y la Impunidad (MCCI) reportó ataques contra figuras clave en la organización como Salvador Camarena y Daniel Lizárraga quienes ayudaron a la realización de reportajes en contra del gobierno de Peña Nieto como "El constructor de la Casa Blanca de EPN ocultó una fortuna en paraísos fiscales" y "El caso de las empresas fantasma de Veracruz".[5]

Finalmente, el IMCO reportó ataques a sus directivos Juan Pardinas y Alexandra Zapata. Este instituto ha publicado varios índices donde señalan que uno de los principales problemas de México es la corrupción de las autoridades; igualmente, sus directores han sido muy críticos sobre los escándalos de corrupción del sexenio de Peña Nieto.

Ahora bien, sabemos quienes son las víctimas de los ataques por parte de Pegasus, pero ¿Quién está detrás de Pegasus? ¿Quién pagó por el *software*? La empresa detrás de Pegasus es *NGO Group* es una empresa de origen israelí que se dice ser líder en la ciberguerra de móviles y teléfonos inteligentes. Según NGO es una compañía que trabaja solamente con gobiernos para

[4] R3D: Red en Defensa de los Derechos Digitales, "Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México", *R3D*, s.f., 9.
[5] R3D, *Gobierno Espía*, 58.

mejorar sus capacidades tecnológicas tanto ofensivas como defensivas en la ciberguerra.[6] Actualmente, es propiedad de una empresa de capital de inversión "*Francisco Partners Management LLC*" quien la adquirió en 2014 después de la aprobación del Ministerio de Defensa de Israel.

¿Cuál es la relación de NGO con México? Debido a una filtración masiva de emails de NGO y de su principal competidor en México "*Hacking Team*" revelaron que México había hecho contratos multimillonarios con la empresa y que la nación mexicana era el cliente más grande e importante de "*Hacking Team*" con una cartera de 14 Estados de la república mexicana que en conjunto habían pagado $6.3 millones de dólares desde 2010. Un reportaje hecho por MCCI reveló que un subordinado del exprocurador de justicia José Murillo Karam, Luis Fernando Ayala Puente, mediante la empresa Grupo *Tech Bull* SA de CV concretó la venta de NGO Pegasus a la PGR por 34 millones de dólares.[7]

La empresa NGO ha repetido en múltiples ocasiones que solo vende su software a gobiernos o agencias de gobierno por lo que no podría atribuirse el ataque a que un grupo de personas hubiera adquirido el producto. Se ha reportado por múltiples fuentes que México adquirió software de Pegasus por 20 millones de dólares y los emails filtrados de *Hacking Team* en los que explícitamente se dice que México tiene contratos en múltiples dependencias del gobierno.[8]

Finalmente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) determinó que la PGR violó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, al no cumplir con sus deberes de seguridad y el principio de responsabilidad por la utilización del *spyware* Pegasus.[9] Todo señala que los nuevos enemigos del Estado no son solo los narcotraficantes sino los periodistas y activistas.

---

[6] Bill Marczak and John Scott- Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender* (Citizen Lab Research Report No. 78, University of Toronto, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[7] Raúl Olmos, "SUBORDINADO DE MURILLO KARAM, LIGADO A GRUPO EMPRESARIAL QUE VENDIÓ PEGASUS A LA PGR," *mexicanos Contra la Corrupción e Impunidad*, 20 de febrero de 2017, https://contralacorrupcion.mx/pegasus-pgr/.

[8] "Hacking Team," Hacking Team Archive, Wikileaks, visitado el 12 de noviembre de 2020, https://wikileaks.org/hackingteam/emails/emailid/5391.

[9] INAI, "DETERMINA INAI QUE FGR, RESPECTO AL SOFTWARE PEGASUS, INCUMPLIÓ LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS," comunicado INAI/054/19, 20 de febrero de 2019, http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf.

A partir de esto surge una nueva interrogante ¿El gobierno puede utilizar este spyware para espiar a ciudadanos? La respuesta corta sería si, pudiera usarse invocando el artículo 16 constitucional el cual establece que ciertas autoridades autorizadas por la autoridad federal o ministerio público de la entidad podrán solicitar la intervención de cualquier comunicación privada.

La autoridad tendrá que fundar y motivar la solicitud, estableciendo el tipo de intervención, sujetos y duración. Los jueces de control resolverán de manera inmediata la solicitud garantizando los derechos de los indiciados, víctimas u ofendidos. Tiene que existir un registro de la comunicación del juez y el Ministerio Público. Las intervenciones autorizadas se ajustarán a los requisitos previstos en las leyes.

No obstante, debido a su naturaleza y su creación reciente deben existir límites claros respecto a la utilización de estas formas de intervención de comunicaciones. Por lo que surge la pregunta de investigación ¿Existe una normativa clara y actualizada respecto a las herramientas de vigilancia que proteja el derecho a la privacidad y la protección de datos personales?

Para responder esta pregunta tenemos que entender la normatividad mexicana, es decir, las reglas básicas del juego. ¿Qué puede hacer el gobierno? ¿Qué no puede hacer? ¿Cuáles son los límites? El principal problema es que el legislador no contempló reglas claras y actualizadas respecto al uso de estas herramientas que protegen los derechos humanos y que su utilización fuera idónea, necesaria y proporcional.

Este tipo de herramientas de vigilancia no cuentan con un conjunto de normas que las permitan operar de manera correcta y de acuerdo con estándares de derechos humanos. No hay un control sobre ¿Qué herramientas usa el gobierno mexicano? ¿Quién puede contratar estas herramientas? ¿Se le tiene que avisar a alguien? ¿Qué reglas tienen que contemplar los jueces para su utilización? ¿Qué significa fundar y motivar? ¿Cómo pueden asegurarse los jueces que la herramienta es proporcional, necesaria e idónea?

El sistema normativo mexicano no contempla en el centro los principios de proporcionalidad, necesidad e idoneidad. No está actualizada a los nuevos retos que presentan las nuevas tecnologías. Cuenta con contradicciones entre lo que señala la jurisprudencia y lo que señala la normativa actual. Asimismo, no contempla que el uso de estas herramientas se

hace en un ambiente opaco donde el ciudadano no puede acceder por medios ordinarios a la información sobre las herramientas de vigilancia que cuenta el gobierno.

No hay registros de los programas con los cuales cuenta el gobierno. No existe precisión sobre sus capacidades. Asimismo, los derechos de protección de datos personales quedan vulnerados pues no se cuentan con protecciones adecuadas para que los datos tan sensibles que extraen estas herramientas sean tratados de manera correcta.

Todo esto queda traducido en una falta de normativa clara y actualizada que pueda regular el uso de estas herramientas. Actualmente, operan en una zona gris donde no existen salvaguardas adecuadas y donde la normativa no contempló la existencia de herramientas mucho más especializadas. Por esta razón, la hipótesis sería que no existe una regulación clara y actualizada que contemple estándares de derechos humanos junto con un correcto tratamiento de datos por lo que viola el derecho a la privacidad y el derecho a la protección de datos personales de los ciudadanos.

2.2 Intervención de comunicaciones y programas de vigilancia

2.2.1 Fundamentos legales para intervenir comunicaciones

El fundamento constitucional para la intervención de comunicaciones es el artículo 16 constitucional, el cual establece en su párrafo décimo segundo:

"Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Publico de la entidad federativa correspondiente, podrá´ autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá´ fundar y motivar las causas legales de la solicitud, expresando, además, el tipo de intervención, los sujetos de la misma y su duración."[10]

Entonces, de acuerdo con el precepto constitucional la intervención es posible y solo permite que dos sujetos puedan solicitar la intervención de comunicaciones, a saber: "autoridades facultadas por la ley" y el "Ministerio Público de la entidad federativa correspondiente". Ahora bien ¿Cuáles son las autoridades facultadas por la ley? Esta pregunta la resuelve el Amparo en Revisión 964/2015 en el cual se establece cuáles son las autoridades que pueden intervenir en las comunicaciones y solicitar la geolocalización en tiempo real las cuales son: 1) El Procurador General de la República, así como los procuradores de las

[10] Constitución Política de los Estados Unidos Mexicanos, CP, art. 16, Diario Oficial de la Federación [DOF] 05-02-1917, últimas reformas DOF 28-05-2021 (Mex).

entidades federativas. 2) La ahora extinta policía federal. 3) La autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional (CISEN).

Ahora bien, no existe un criterio actualizado de la Corte que permita nuevamente vislumbrar a qué autoridades se refiere el artículo 16 constitucional. Además, de que las autoridades que fueron materia de la impugnación ya no existen como tal.

La PGR ahora es la fiscalía general de la República (FGR) como tal no tiene esa función explícita en su ley orgánica si no que menciona en el artículo 9 fracción X que "X. Solicitar y efectuar actos de investigación, dentro o fuera del territorio nacional, conforme al principio de libertad probatoria;". Al ser la intervención de comunicaciones un acto de investigación de acuerdo con el CNPP podría ordenarlo. De hecho, el CNPP prevé que el titular de la procuraduría sea una persona autorizada para solicitar la intervención de comunicaciones en su artículo 303.

En el caso de la Guardia Nacional que ahora asume las funciones de la extinta policía federal en sus transitorios sexto y séptimo.[11] En el artículo 100 de la Ley de la Guardia Nacional prevé que pueda solicitar la intervención de comunicaciones a la autoridad judicial el Comandante o titular de la Jefatura General de Coordinación Policial si se tienen indicios suficientes que se actualiza alguno o algunos de los delitos previstos en el artículo 103 de la ley.[12] Finalmente, el Centro Nacional de Inteligencia (CNI) sustituye al CISEN y ahora está adscrito a la Secretaría de Seguridad y Protección Ciudadana.

En teoría, el CNI sustituye al CISEN en sus funciones; sin embargo, en la Ley de Seguridad Nacional sigue contemplando al CISEN en sus funciones. Ahora, no está claro por lo menos en la Ley si el CNI tiene las mismas funciones que el CISEN.

El amparo resuelve tres problemas centrales: 1) La relación del derecho a la privacidad con el derecho a la protección de datos personales. En este caso la SCJN menciona que "la protección a los datos personales es una vertiente del derecho humano a la privacidad de las personas, que se despliega ante la necesidad de otorgar salvaguardas necesarias a los gobernados", por lo que es necesario que los usuarios tengan poder sobre sus datos personales para evitar intromisiones indebidas. 2) Menciona que requerir autorización judicial no es

[11] Ley de la Guardia Nacional [LGN], Diario Oficial de la Federación [DOF] 27-05-2019, últimas reformas DOF 27-05-2019 (Mex), formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019.
[12] Ley de la Guardia Nacional [LGN], Diario Oficial de la Federación [DOF] 27-05-2019, últimas reformas DOF 27-05-2019 (Mex), formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019.

necesario para intervenir en el derecho humano a la protección de datos personales. El razonamiento de la autoridad es que:

"no constituye un requisito que se encuentren autorizadas por autoridad judicial, pues como se ha precisado, el cabal cumplimiento a dicho derecho humano manda únicamente que tales limitaciones se encuentren previstas en ley, que persigan un fin legítimo, que sean instrumentalmente aptas para alcanzar ese objetivo -necesidad-, y finalmente, que resulten proporcionales -proporcionalidad en sentido estricto"[13]

Es decir, la autoridad investigadora puede perturbar el derecho mediante la realización de un *test* de proporcionalidad lo cual es correcto, puesto que la prueba de proporcionalidad nos permite ponderar la perturbación de un derecho con una medida intrusiva; no obstante, este test de proporcionalidad lo tiene que hacer un juez, no la autoridad. El juez tiene que ser un tercero imparcial en la resolución del caso y realizar la prueba. La autoridad no puede ser juez y parte, si no todas las intervenciones realizadas por ella serían legales y proporcionales.

3) La localización geográfica en tiempo real (GPS) no necesita de una autorización judicial, puesto que lo único que se trata de localizar es el teléfono que está asociado a una línea telefónica. Por lo que el perjudicado no es la persona que tiene en ese momento el teléfono sino el móvil asociado a esa línea telefónica El razonamiento de la Corte es cuestionable, puesto que es claro que el móvil no es un ente por sí mismo y quien recibe esa intromisión es la persona dueña de él pues puede ser localizada en donde se encuentre. Otro criterio debatible es que los metadatos de las comunicaciones por teléfono si las considera parte vital de la esfera de privacidad de la persona por lo que podrían revelar de ella, pero una cuestión tan intrusiva como la localización en tiempo real de una persona no lo considere invasivo.

Otro criterio importante y es el que prevalece actualmente es el Amparo en Revisión 937/2015 en el que la Corte analiza la constitucionalidad de las fracciones I y II de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR). En el cual la Corte reitera lo que estableció en la Acción de Inconstitucionalidad 32/2012 sobre que la geolocalización de equipos de comunicación móvil no vulnera el derecho a la privacidad. Lo cual es un criterio cuestionable, por las razones anteriormente expuestas y que la geolocalización de un equipo móvil puede revelar información intima, en tiempo real de la persona que tiene el móvil.

Si bien la medida es específicamente contra el dispositivo no puede ignorarse que el móvil es una parte importante del día a día de las personas y que en la mayoría de los casos está

[13] Amparo en Revisión 964/2015, Segunda Sala de la Suprema Corte de Justicia [SCJN].

en su posesión. Si sabes la localización del dispositivo muy probablemente puedes saber la localización de la persona.

Ahora bien, un acierto del Amparo en Revisión es que considera que efectivamente los metadatos pueden revelar datos íntimos e importantes de la vida de las personas pues a través de ellos pueden crearse perfiles precisos de las personas.

Asimismo, reconoce que la recolección de estos datos tiene un propósito constitucional válido pues ayuda a tareas de seguridad pública para la prevención del delito y protege el derecho a la seguridad personal de la población. El punto clave de la resolución de la Corte es que establece que una cosa es el almacenamiento de estos datos por parte de los concesionarios y otra es la entrega de los datos a la autoridad.

Es en esta tesitura que la Corte menciona que debido a la sensibilidad de los datos y su capacidad para desarrollar un perfil preciso de la persona la solicitud de acceso por parte de las autoridades debe hacerse en términos del 16 constitucional debido a que esa una injerencia constitucionalmente válida a la privacidad de las personas.[14] La solicitud solo podrá hacerse por la autoridad judicial federal, a petición de la autoridad federal facultada o el titular del ministerio público de la entidad federativa correspondiente.

Por lo que autoridad tiene que fundar y motivar su solicitud, precisar que datos serán solicitados y el periodo por el cual se requiera la información. A partir, de la tesis derivada de este amparo en revisión se hacen obligatorio los requisitos jurídicos que deberán cumplirse para la solicitud y entrega de la información retenida por los concesionarios de telecomunicaciones.[15]

Asimismo, este criterio de la Corte se reitera en una tesis aislada de los Tribunales Colegiados de Circuito.[16] En la cual recalca el criterio de la Corte y establece que la entrega de

[14] Amparo en Revisión 937/2015, Segunda Sala de la Suprema Corte de Justicia [SCJN].
[15] COMUNICACIONES PRIVADAS. LA SOLICITUD DE ACCESO A LOS DATOS DE TRÁFICO RETENIDOS POR LOS CONCESIONARIOS, QUE REFIERE EL ARTÍCULO 190, FRACCIÓN II, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN, DEBE REALIZARSE EN TÉRMINOS DEL ARTÍCULO 16 CONSTITUCIONAL Y SÓLO LA AUTORIDAD JUDICIAL PODRÁ AUTORIZAR LA ENTREGA DE LA INFORMACIÓN RESGUARDADA, Segunda Sala de la Suprema Corte de Justicia [SCJN], Gaceta del Semanario Judicial de la Federación, Décima Época, tomo I, Julio de 2016, Tesis 2a. XXXV/2016, Página 776. (Mex).
[16] SOLICITUD MINISTERIAL DE ENTREGA DE DATOS CONSERVADOS POR LOS CONCESIONARIOS DE TELECOMUNICACIONES. SU AUTORIZACIÓN ES COMPETENCIA EXCLUSIVA DEL PODER JUDICIAL DE LA FEDERACIÓN (INTERPRETACIÓN CONFORME DEL ARTÍCULO 303 DEL CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES), Tribunales Colegiados de Circuito [TCC], Gaceta del

los datos conservados por los concesionarios de telecomunicaciones la cual está prevista en el art. 303 del Código Nacional de Procedimientos Penales "es un acto de investigación que invade el ámbito de protección de las comunicaciones privadas"[17]. Lo cual es un acierto debido a la sensibilidad de estos datos y de establecer que estos actos deben estar previstos en ley y con estándares constitucionales rigurosos pues constituyen actos de investigación. Por lo tanto, afectan a la esfera jurídica de la persona y su derecho a la privacidad y a la protección de datos personales.

Dado este contexto constitucional y jurisprudencial es importante tener claro en qué legislación está prevista la intervención de comunicaciones. La siguiente tabla resume eso y deja claro que no solamente está regulado en una ley sino en un compendio de leyes con supuestos específicos y particulares para cada normativa.

Tabla 1. Mapeo normativo sobre intervención de comunicaciones en México.[18]

Ley	Artículo
Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro	Art. 24
Código Nacional de Procedimientos Penales	Arts. 252, 291-303
Ley Federal Contra la Delincuencia Organizada	Arts. 16 -28
Ley de la Guardia Nacional	Arts. 100 - 106

Semanario Judicial de la Federación, Décima Época, Tomo IV, Diciembre de 2017, Tesis I.8o.P.18 P, Página 2267 (Mex).

[17] SOLICITUD MINISTERIAL DE ENTREGA DE DATOS CONSERVADOS POR LOS CONCESIONARIOS DE TELECOMUNICACIONES. SU AUTORIZACIÓN ES COMPETENCIA EXCLUSIVA DEL PODER JUDICIAL DE LA FEDERACIÓN (INTERPRETACIÓN CONFORME DEL ARTÍCULO 303 DEL CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES), Tribunales Colegiados de Circuito [TCC], Gaceta del Semanario Judicial de la Federación, Décima Época, Tomo IV, Diciembre de 2017, Tesis I.8o.P.18 P, Página 2267 (Mex).

[18] Existen disposiciones tales como los "Lineamientos De Colaboración En Materia De Seguridad Y Justicia" los cuales regulan la manera en que interactúan los concesionarios de telecomunicaciones con las autoridades jurisdiccionales respecto a las intervenciones de comunicaciones.

Ley Federal de Telecomunicaciones y Radiodifusión	Arts. 189 - 190
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Arts. 80-82

Fuente: Elaboración propia.

2.2.2 Datos recopilados por la intervención de comunicaciones

Ahora, los datos que recaba una intervención de comunicaciones común y los datos recabados por programas de *spyware* no son necesariamente los mismos. En la intervención de comunicaciones está delimitado la información que pueden recabar. El CNPP establece una definición de lo que comprende esta figura lo que nos permite entender el alcance de una intervención de comunicaciones. En su artículo 291 establece lo siguiente:

> "La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real."[19]

Entonces, lo que se puede intervenir es ya sea un dispositivo móvil y los programas que permitan esta comunicación y el intercambio de datos. La definición es sumamente amplia y contempla numerosos datos que podrían ser sumamente sensibles y requieren un tratamiento especial. Por ejemplo, si se controla el micrófono remotamente podrían revelarse datos sensibles. Asimismo, con el control de la cámara para la toma de fotografías pueden revelarse datos sensibles. El concepto de "información" es tan amplio que podría recabarse contraseñas, datos bancarios, contactos sin ninguna distinción.

Lo que se recaba principalmente son los metadatos que son "datos sobre las comunicaciones de una persona, por ejemplo: los números telefónicos de origen y destino de una comunicación; la hora, fecha y duración de la misma; los datos de identificación de la tarjeta

[19] Código Nacional de Procedimientos Penales, CNPP, art. 291, Diario Oficial de la Federación [DOF] 05-04-2014, últimas reformas DOF 19-02-2021 (Mex).

SIM (IMSI) y del dispositivo (IMEI); e incluso los datos de localización de las antenas a las cuales se conecta un dispositivo móvil."[20] Básicamente como menciona el comisionado de privacidad de Ontario son las "migajas digitales" que toda persona deja al usar dispositivos digitales pues es la información generada por la comunicación de nuestros dispositivos con los servicios de telecomunicaciones.[21]

Si bien pueden parecer inofensivas estas migajas digitales y que la autoridad puede tener información limitada respecto de la persona investigada; la realidad es que los metadatos pueden revelar una cantidad importante de información sensible sobre la persona. Por ejemplo, en 2014 la Universidad de Stanford analizó los metadatos de 546 voluntarios y encontró información sensible de varios candidatos. Entre los datos encontrados fueron que una persona padecía esclerosis múltiple, otra persona planeaba abortar y varios datos sensibles de múltiples personas.[22] Afortunadamente, los metadatos fueron clasificados como parte del derecho de la inviolabilidad de las comunicaciones puesto que el contenido de ellas, es decir, los metadatos podían "extraer conclusiones muy precisas sobre la vida privada de las personas."[23]

El amparo 964/2015 dejó precedentes claros, aunque contradictorios, al considerar que los metadatos son parte del derecho de inviolabilidad de comunicaciones. Sin embargo, no incluyó la localización GPS como parte de este derecho.

2.2.3 Datos recopilados por Pegasus

Ahora bien, es claro que una intervención de comunicaciones tiene sus límites y alcances; sin embargo, los datos recabados por Pegasus requieren un control y un cuidado mucho más meticuloso. Al igual que normativa clara y actualizada que proteja estos datos. Lo que hace Pegasus es vulnerar completamente la seguridad del dispositivo para infectarlo. Es

[20] R3D, *El Estado de Vigilancia: Fuera de Control* (México: Red en Defensa de los Derechos Digitales, 2016).
[21] Craig Forcese. "Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives," in *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, ed. Michael Geist (University of Ottawa Press, 2015).
[22] Jonathan Mayer y Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata," *Web Policy*, 12 de marzo de 2014, http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.
[23] Amparo en Revisión 964/2015, Segunda Sala de la Suprema Corte de Justicia [SCJN].

decir, no se necesita que la empresa de telecomunicaciones te proporcione herramientas para obtener los metadatos o la localización GPS.

El programa funciona de la siguiente manera: primero, el programa puede infectar de dos maneras el dispositivo: *zero-click vector* y *one-click vector*. En *one-click vector* el usuario tiene que acceder a un *link* que es enviado por *SMS* para que el celular abra el navegador y descargue el *spyware* al celular y en *zero-click vector* no hay necesidad de entrar a ningún *link,* sino que con el solo envío de un mensaje *WAP* se puede infectar el teléfono. Este último no es tan común debido a que las empresas de telecomunicaciones constantemente bloquean este tipo de mensajes.

En el caso Pegasus en México se utilizó el primer método que involucra mandar SMS sugestivos con un *link* que infecta el teléfono. Lo que provoca el software Pegasus, por lo menos en el caso del iPhone, es hacerle un *jailbreak* en el que modifica totalmente la manera en que funciona el dispositivo. En el momento que se instala es totalmente sutil, es decir, la víctima no puede ni detener la infección, ni mucho menos darse cuenta de que su celular se ha convertido en una máquina de espionaje.

La información que puede obtener el programa de Pegasus rebasa toda expectativa de privacidad que podría tener el usuario intervenido. Ya no son las migajas sino el plato completo al cual tiene acceso Pegasus. Dentro de las funciones del spyware destacan las siguientes: i) activación del micrófono en cualquier momento; ii) activación de las cámaras que posea el dispositivo; iii) Extraer datos de SMS y correos electrónicos; iv) Grabar en tiempo real llamadas telefónicas y por servicios como *WhatsApp, Telegram, Facebook,* etc.; v) Conocer en tiempo real la ubicación del dispositivo; vi) Acceder a los contactos, contraseñas, historial de navegación, redes sociales, calendario entre otros datos; vii) Extraer cualquier archivo que se encuentre en el dispositivo y, viii) En caso de riesgo de ser detectado autodestruirse para no dejar rastro en el teléfono.[24]

Los datos que puede recabar el *spyware* de Pegasus son alarmantes. Si bien, este tipo de herramientas podrían ser de gran ayuda para detener el crimen organizado debido a sus múltiples herramientas con las que cuenta. La realidad demuestra que estas herramientas no cuentan con una regulación robusta que se adapte a las nuevas tendencias de vigilancia digital

[24] Marczak and Scott - Railton, *"The Million Dollar Dissident,"* 15.

y que en lugar de usarse para criminales se usa para los nuevos enemigos del Estado: los periodistas y activistas.

2.3 Proceso judicial para intervenir comunicaciones vs proceso judicial para la utilización de programas de vigilancia estatal

Surge la interrogante ¿Cuál es el proceso judicial para la intervención de comunicaciones y cuál es el proceso judicial para la utilización de *spyware*? Hay una diferencia fundamental respecto a las dos que es la relación que tienen las autoridades con las empresas de telecomunicaciones. En la intervención de comunicaciones las autoridades tienen que tratar directamente con las empresas de telecomunicaciones, pero en la utilización de Pegasus no es necesario.

Respecto a la intervención de comunicaciones hay dos grandes filtros que hacen que la solicitud siga un proceso más transparente, seguro y cuidando que la intervención no sea arbitraria. No obstante, este proceso tiene grandes deficiencias y opacidades las cuales deberían ser atendidas con prontitud para evitar que el Estado ejerza una vigilancia estatal sin control.

El proceso judicial varía ligeramente dependiendo de la legislación consultada; sin embargo, la que contiene la regulación más completa y que puede ilustrar de mejor manera cómo es el proceso jurídico para que una autoridad solicite intervenir comunicaciones de un ciudadano es el Código Nacional de Procedimientos Penales (CNPP). Por esta razón la legislación que será la base para analizar la intervención de comunicaciones será la que está contenida en el CNPP.

En la siguiente sección se realizará un análisis del proceso jurídico para intervenir comunicaciones por parte de una autoridad y será contrastado con el proceso jurídico que tendría que hacer una autoridad para utilizar *softwares* de vigilancia masiva. El CNPP establece en su artículo 252, fracción III que requiere autorización judicial previa del juez de control es la intervención de comunicaciones privadas y correspondencia.

La solicitud debe hacerse al juez federal competente y el juez tiene seis horas para resolver la solicitud. Se necesita una autorización judicial tanto para intervenir comunicaciones, como para extraer información del dispositivo como documentos de texto, documentos de audio, imagen o video. La solicitud debe reunir los siguientes requisitos: “i) estar fundada y

motivada; ii) Precisar la persona o personas que estarán sujetas a la medida; iii) Señalar el lugar o lugares donde se realizará; iv) Señalar el tipo de comunicación intervenida; v) Establecer la duración de la intervención, las líneas intervenidas, números o aparatos a intervenir y, vi) Señalar la empresa concesionaria del servicio de telecomunicaciones".[25]

La duración de la intervención de comunicaciones no podrá exceder seis meses. El juez es el que limitará todas estas variables, podrá establecer límites y valorar si es necesario este tipo de intervención. La autoridad judicial es la que realiza el test de proporcionalidad y decide si la intervención de comunicaciones es una medida acorde para los fines perseguidos.

Ahora bien, toda intervención de comunicación debe ser registrada para que sea ofrecida como medio de prueba. Es importante este punto porque debido a la tesis:

"INTERVENCIÓN DE COMUNICACIONES PRIVADAS SIN AUTORIZACIÓN JUDICIAL. LAS GRABACIONES DERIVADAS DE UN ACTO DE ESA NATURALEZA CONSTITUYEN PRUEBAS ILÍCITAS QUE POR MANDATO EXPRESO DEL ARTÍCULO 16 CONSTITUCIONAL CARECEN DE TODO VALOR PROBATORIO".[26]

La cual establece que cualquier prueba obtenida sin autorización judicial mediante la intervención de comunicaciones no tendrá valor probatorio. Aunado a esto puede derivar una responsabilidad penal o administrativa para el servidor público responsable de la violación.

Al concluir la intervención, debe informarse al Ministerio Público y al Juez que se le solicitó la intervención. En caso de solicitar la localización geográfica en tiempo real y solicitud de entrega de datos conservados se requiere igualmente de una autorización judicial contrario a lo que resolvió en el Amparo 964/2015 en el cual establecía que no era necesaria la autorización judicial para solicitar la localización *GPS*. Igualmente, en términos del CNPP, la solicitud debe fundamentarse y expresar los motivos por lo que sería necesario saber la localización *GPS* en tiempo real de una persona o la entrega de los datos conservados.

Las concesionarias juegan un papel fundamental en la intervención de comunicaciones. Puesto que tienen que ayudar a la autoridad para facilitar la medida de investigación. No solo ayudan, sino que también ofrecen un segundo filtro para que quede claro el alcance, la persona,

[25] Código Nacional de Procedimientos Penales, CNPP, art. 292, Diario Oficial de la Federación [DOF] 05-04-2014, últimas reformas DOF 19-02-2021 (Mex).

[26] INTERVENCIÓN DE COMUNICACIONES PRIVADAS SIN AUTORIZACIÓN JUDICIAL. LAS GRABACIONES DERIVADAS DE UN ACTO DE ESA NATURALEZA CONSTITUYEN PRUEBAS ILÍCITAS QUE POR MANDATO EXPRESO DEL ARTÍCULO 16 CONSTITUCIONAL CARECEN DE TODO VALOR PROBATORIO, Pleno de la Suprema Corte de Justicia [SCJN], Semanario Judicial de la Federación y su Gaceta, Novena Época, tomo XXVII, abril de 2008, Tesis P. XXXIII/2008, página 6.

la duración de la intervención y su objeto y propósito. La Ley Federal de Telecomunicaciones en sus artículos 189 a 190 reglamentan las obligaciones de las concesionarias en materia de seguridad y justicia.

En general, los concesionarios de telecomunicaciones están obligados a atender todo mandamiento por escrito, fundado y motivado por la autoridad competente. Los concesionarios tienen que colaborar con las autoridades para la localización geográfica en tiempo real de los equipos de comunicación móvil. Asimismo, deben conservar un registro y control de comunicaciones hechas por la línea donde deben conservarse datos tales como: nombre, tipo de comunicación, servicios de mensajería o multimedia empleados, datos necesarios para rastrear e identificar el origen y destino de las comunicaciones, fecha y hora de la comunicación, ubicación digital (GPS) entre otros.

El concesionario tiene que almacenar esos datos durante veinticuatro meses, los primeros doce meses se le tienen que entregar a la autoridad de manera inmediata y los siguientes doce meses pueden transcurrir hasta cuarenta y ocho horas para su entrega. Finalmente, deben de contar con un área responsable disponible las 24 horas del día y los 365 días del año, para atender los requerimientos de información, localización geográfica e intervención de comunicaciones privadas.

La materia está regulada de manera aún más específica en los Lineamientos de Colaboración en Materia de Seguridad y Justicia. Los lineamientos proporcionan información valiosa para la ciudadanía pues establecen formatos que contienen información con la que pueden hacer controles ciudadanos o de autoridades respecto del uso de estas herramientas.

Lo importante es que esta información sea pública para que cualquier ciudadano pueda ver de qué manera interactúan las autoridades con las concesionarias y cómo se protegen sus datos personales. Si bien, estos formatos son públicos y es una obligación de la concesionaria publicarlos semestralmente, se han encontrado muchas irregularidades en su publicación y en los datos presentados.[27]

Ahora bien, cada vez que una autoridad facultada pide a la concesionaria la localización por *GPS* y la entrega de los datos la autoridad tiene que llenar una solicitud donde sea clara la siguiente información: “1) Nombre completo del servidor público, cargo e institución a la que pertenece, fecha en la que se publicó en el DOF su autorización como sujeto obligado, número

[27] R3D, *El Estado de Vigilancia*, 45-70.

de teléfono o IMEI y cuál es el objeto del requerimiento (entrega de datos conservados, localización geográfica en tiempo real o ambas). Asimismo, tienen que anexar la autorización judicial por parte del juez cuando sea necesaria."[28]

Ahora bien, existe una normativa clara de las obligaciones en transparencia que tienen que entregar tanto como concesionarias como autoridades. La normativa para las concesionarias está en los Lineamientos de Colaboración en Materia de Seguridad y Justicia expedida por el IFT. En el transitorio décimo octavo menciona que los concesionarios deberán entregar dos informes semestrales uno en enero y otro en julio cada año en el que contenga la siguiente información: Número total y por autoridad, así como la facultad de requerimientos de información de localización y de registro de comunicaciones, desglosando cuantas fueron recibidas, aprobadas y no entregadas mensualmente.

No solamente tienen que presentar informes acerca del número de solicitudes, sino que tienen que presentar otro informe acerca de los protocolos de seguridad que utilizaron para el desarrollo o implementación de las plataformas electrónicas por las que la autoridad solicita información. Es decir, hay una constante vigilancia de que los datos tratados por estas empresas se manejan de manera correcta y de acuerdo con estándares de seguridad internacionales. Toda esta información no solamente tiene que ser entregada a la autoridad en telecomunicaciones, sino que es pública y debería de estar en sus portales de transparencia.

También, la autoridad deberá entregar dos informes semestrales cada año, uno en enero y otro en julio, donde señale: i) Cuántas veces requirió la localización geográfica en tiempo real y de registro de datos y, ii) El número de registros de datos de comunicaciones cancelados y suprimidos una vez cumplida su finalidad. Por lo menos, en la parte normativa hay obligaciones entre concesionarias y autoridades sobre los datos de los usuarios y en teoría deberían de estar publicando esta información semestralmente tal como marca la ley.

El proceso para la intervención de comunicaciones en términos del CNPP es claro. La utilización del *spyware* Pegasus en este proceso no es tan clara. La autorización para la intervención de comunicaciones debe seguir la normativa establecida en de los artículos 291 a 302. Este proceso ya ha sido explicado en la sección anterior.

[28] Lineamientos de Colaboración en Materia de Seguridad y Justicia [LCMSJ], Diario Oficial de la Federación [DOF] 21 de junio de 1996, últimas reformas DOF 2-12-2015 (Mex.), formato PDF, http://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/dofpiftext111115159.pdf.

Ahora bien, si existe evidencia que la fiscalía general de Jalisco ha utilizado este tipo de *spyware* en dos ocasiones. Este caso será explicado en una sección posterior. Sin embargo, es necesario confirmar que, aunque una no exista reglas del todo claras y específicas nuestro marco constitucional prevé que deberán aplicarse las reglas constitucionales y jurisprudenciales respecto a la intervención de comunicaciones privadas. No obstante, no solo estas medidas pueden ayudar a regular y ofrecer un marco normativo robusto respecto a la utilización de este tipo de *spyware* si no que podrían incluirse otras medidas que se detallarán en el último capítulo.

Es importante mencionar que al ser una medida invasiva el juez que autorice su utilización deberá utilizar controles constitucionales más estrictos y con mucho más rigor para autorizar su utilización. La cuestión es que estas nuevas formas de vigilancia no estaban previstas en la jurisprudencia y el marco legal mexicano, puesto que es una tecnología reciente. Es por eso por lo que debe apostarse por nuevos criterios que den certeza a ambas partes (Estado y ciudadano) que la utilización de estas herramientas se hará conforme a criterios actualizados y claros.

2.4 Asimetrías y similitudes de ambos procesos judiciales.

El legislador previó una cooperación entre las dos partes y que gracias a esta cooperación surge información y datos públicos a los que la ciudadanía puede acceder. Lo preocupante es que la utilización de *spyware* como Pegasus o Galileo por parte de *Hacking Team* no necesitan de la ayuda de las concesionarias para intervenir en las comunicaciones, ni para la entrega de metadatos ni para la localización *GPS.*

El software permite tener eso y más sin la necesidad de solicitarle nada a la concesionaria y así agilizar más labores de investigación. Lo cierto es que en ninguna ley consultada hay alguna mención de estos *spyware*, no hay regulación específica para la utilización de estos programas.

Es una tarea pendiente del Estado mexicano legislar acerca de estas nuevas formas de vigilancia estatal. ¿Quién puede contratar estos spyware? ¿Quién los puede utilizar? ¿En qué casos puede justificarse su uso? ¿Con qué legislación pueden regularse? Todas son preguntas en las que no hay respuestas claras puesto que en principio no hay ningún impedimento para

que el gobierno pueda comprar estos softwares. Al tratarse de softwares de vigilancia para la "prevención del delito" podríamos guiarnos por lo que menciona el artículo 16º constitucional que sean las mismas autoridades que puedan intervenir comunicaciones las que puedan utilizar estos softwares.

La utilización de este *spywares* deberían usarse sólo en casos límite o de seguridad nacional o bien cuando pueda probarse que la intervención de comunicaciones no es suficiente. La legislación actual no es suficiente para regular una nueva manera de ejercer la vigilancia debido a que la regulación de la intervención de comunicaciones no está lo suficientemente actualizada para prever las diferentes violaciones a la privacidad y a la protección de datos. El spyware puede activar la cámara, micrófono, GPS, todo al mismo tiempo que extrae datos y recaba información de los contactos del teléfono por lo que el CNPP queda corto en su regulación.

A simple vista puede observarse que no existen estos mecanismos de rendición de cuentas que expuse anteriormente. No se tienen que entregar reportes, informes, a ninguna autoridad como la de telecomunicaciones porque no requiere información de las concesionarias. Entonces ¿Quién vigila al vigilante? ¿Cómo podemos asegurarnos que efectivamente el Estado está usando estos programas para fines correctos?

2.5 México y el uso de herramientas de vigilancia

¿Sabemos de la existencia del spyware de Pegasus, pero hay más spywares en el territorio mexicano? ¿Cuántos hay? ¿Quién los tiene? Gracias a una investigación de R3D podemos saber una aproximación del panorama de los programas de vigilancia doméstica en México.[29] Hay dos empresas que actualmente están disputándose el mercado mexicano*: NSO Group* y *Hacking Team.*

Sabemos de las empresas por una filtración masiva de correos y documentos internos de la empresa *Hacking Team* en 2015. La información que a continuación se expone fue recabada por R3D: de los 35 países en los que opera *Hacking Team*, México ocupa el lugar número uno como el cliente más grande de la firma. Como comparación México ha gastado €5,800,000 millones de euros ($141,520,000 millones de pesos) y el segundo cliente más

[29] R3D, *El Estado de Vigilancia*.

grande es Italia con €4,000,000 millones de euros. En el año 2015 los siguientes Estados tenían relaciones comerciales con *Hacking Team*: Baja California, Campeche, Chihuahua, Durango, Estado de México, Guerrero, Jalisco, Nayarit, Puebla, Querétaro, Tamaulipas y Yucatán.

Asimismo, dependencias como la SEDENA, el extinto CISEN, la extinta Policía Federal, la PGR (ahora FGR) y finalmente Pemex. El último siendo un caso anómalo pues no es una institución de seguridad pública entonces ¿Para qué establecer relaciones comerciales con *Hacking Team*? Ahora de todas las dependencias y Estados, Pemex es la que menos dinero ha gastado en contratos con *Hacking Team* con una cifra de €321,120 mil euros gastados frente a SEDENA que ha gastado €3,200,000 millones de euros.

Como podemos ver cualquier institución o Estado que tenga el poder adquisitivo para adquirir el *spyware* puede hacerlo. Un ejemplo claro de esto es el caso de Jalisco en 2015 cuando la autoridad primero afirmó que no había adquirido ningún *software* de esta naturaleza. Posteriormente, rectificó que si lo adquirió pero que solo lo usarían en materia de secuestros para que después saliera a la luz que este *software* había sido instalado en la Secretaría de Gobierno. Los funcionarios de la Secretaría de Gobierno fueron capacitados para su utilización y se comprobó que el principal cliente no era Fiscalía General del Estado de Jalisco sino la Secretaría de Gobierno del Estado de Jalisco.[30]

Lo preocupante es el proceso judicial para la utilización de estos *softwares* puesto que debido a solicitudes de información hechas por R3D para conocer si la fiscalía general del Estado de Jalisco había solicitado autorización judicial para utilizar este *software* reveló que solo ha solicitado autorización dos veces una en 2014 y otra en 2015. R3D plantea dos hipótesis: la fiscalía general del Estado de Jalisco ha utilizado este *software* sin autorización judicial, es decir, de manera ilegal o el Gobierno de Jalisco adquirió *software* con valor de €748,003.00 euros para utilizarlo en dos ocasiones.

Ambas hipótesis son alarmantes puesto que puede que estén utilizando el *software* de manera ilegal sin ningún tipo de control judicial o que han gastado aproximadamente 40 millones de pesos en conjunto para no utilizarlo ni una sola vez. En el caso de las procuradurías del Estado de México, Yucatán, Durango, Campeche, Tamaulipas gracias a solicitudes de información de R3D confirmó que ninguna pidió autorización judicial para la utilización de

[30] Arturo Ángel, "El Sabueso: ¿Jalisco compró el sistema de Hacking Team sólo para investigar secuestros?," *Animal Político*, 24 de julio 2015, https://www.animalpolitico.com/elsabueso/el-sabueso-jalisco-compro-galileo-solo-para-investigar-secuestros-y-sin-conocer-a-hacking-team/.

este *spyware* para la intervención de comunicaciones. El caso de Jalisco no es aislado tanto el Estado de Puebla y Querétaro adquirieron programas de vigilancia valuados en millones de euros y solo han utilizado menos de 10 veces por lo que es un considerable para el presupuesto público.

En el caso de NGO dueño de Pegasus la información se obtuvo de la misma filtración masiva de correos de *Hacking Team* donde relatan cómo la SEDENA estaba buscando contratar Pegasus para sus agentes y que previamente había sido estafada en un contrato multimillonario en el cual le vendieron *spyware* apócrifo. Asimismo, la empresa fundada por un subordinado del ex procurador de justicia José Murillo Karam, *Tech Bull* S.A. de C.V comentaba en un correo a *Hacking Team* que tenían de clientes a la SEDENA, PGR, CISEN, Policía Federal y muchas procuradurías estatales. En el caso de la PGR fue documentado por *New York Times* y Reforma que la procuraduría había adquirido spyware por 15 millones de dólares. [31]

En conclusión ¿Cómo regulamos todas estas herramientas? ¿Cómo confiamos que la actuación de la autoridad fue de acuerdo con la ley? ¿Cómo sabemos que la autoridad no activará la cámara para la grabación de video cuando mencionó que solo extraería correos electrónicos? El problema es complejo y la regulación debe estar a la altura. El INAI determinó que la PGR "carecía de una bitácora de uso respecto del tratamiento de datos personales vinculado con el software Pegasus y además no acreditó que contaba con un sistema de gestión y con un documento de seguridad; así como haber llevado a cabo el borrado seguro del sistema en comento, tras su desinstalación"[32]

Entonces, la PGR no tenía un registro de quienes habían sido las personas a las cuales se les investigó ni contaba con sistemas de gestión ni documentos de seguridad que salvaguarden la protección de los usuarios. Lo que más extraña es la actuación de la PGR si estos *spywares* tienen la función de prevenir el delito ¿Por qué no hacer públicos los contratos? Si la utilización del spyware no es ilegal ¿Por qué negar la adquisición del *spyware* para luego

[31] Redacción, "Adquiere la PGR equipo para espiar," *Reforma*, 12 de septiembre de 2016, https://www.reforma.com/aplicacioneslibre/articulo/default.aspx?id=937450&md5=6796275797392efc0223b450c4b2d0e2&ta=0dfdbac11765226904c16cb9ad1b2efe&lcmd5=daff83a6dbd92c568ac692898d5f4c2b.

[32] INAI, "DETERMINA INAI QUE FGR, RESPECTO AL SOFTWARE PEGASUS, INCUMPLIÓ LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS," comunicado INAI/054/19, 20 de febrero de 2019, http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf.

comprobarse contratos adicionales?[33] Si ya se pagaron millones de dólares para la licencia del producto ¿Por qué desinstalar el programa de las oficinas de la PGR en medio de una investigación del INAI?

Asimismo, cabe resaltar los contratos de software espía adquiridos con fondos de la Iniciativa Mérida durante el gobierno de Felipe Calderón. El gobierno mexicano había adquirido de dos empresas espionaje software espía, Verin y Narus, para combatir el narcotráfico y delincuencia organizada durante los sexenios de Felipe Calderón y Vicente Fox. Estas empresas han trabajado con la *National Security Agency* (NSA) según datos filtrados por Edward Snowden en 2013. [34]

Los contratos para la adquisición de software espía fue analizado por Noticias MVS quien obtuvo una copia de estos contratos. Estos fueron firmados por el entonces director del CISEN, Eduardo Medina Mora. Cabe resaltar que los vendió una filial de Verint en México llamada Sogams SA de CV la cual en su objeto social señalaba "compra, venta y distribución de equipo de cómputo, comunicaciones y su mantenimiento" con un domicilio en la Ciudad de México en la Colonia San Rafael en el cual no parece que sea la empresa encargada de contratos millonarios.

En el CISEN existía (o existe) un sistema de espionaje instalado por esta empresa desde el año 2003 por el cual fue firmado un contrato por 1 millón 849 mil 200 pesos. La contratación se dio en el marco de la iniciativa Mérida y fue una imposición del gobierno estadounidense a México.

Asimismo, en 2007 en el portal de la Administración Pública estadounidense fue anunciado un contrato por dos millones de dólares para instalar en México equipo que tenía la capacidad de "intervenir chats, correos electrónicos, llamadas de teléfonos móviles y fijos, y redes internas de comunicación."[35] De igual manera, existñian contratos para comprar equipo que pudiera intervenir llamadas de la red de Telmex, Telcel, Unefon, Iusaccel y Prodigy. Todos estos contratos estaban en los portales de EUA.

---

[33] INAI, "DETERMINA INAI QUE FGR, RESPECTO AL SOFTWARE PEGASUS, INCUMPLIÓ LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS," comunicado INAI/054/19, 20 de febrero de 2019, http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf.

[34] Redacción, "México compró equipos de espionaje a empresas vinculadas con la NSA de EU," *Aristegui Noticias*, 8 de enero de 2014, https://aristeguinoticias.com/0801/mexico/mexico-compro-equipos-de-espionaje-a-empresas-vinculadas-con-la-nsa-de-eu/.

[35] Redacción, "México compro equipos."

La empresa Sogams igualmente aparecía en la lista de proveedores de los Estados de Hidalgo, Sonora y Chihuhua. De igual manera, el CISEN reconoció que Sogams era una distribuidora de Verint en México. Por medio de SOGAMS, la empresa Verint "vendió equipo de espionaje a la Policía Federal Preventiva (PFP), a Petróleos Mexicanos (Pemex), al Servicio de Administración Tributaria (SAT), así como al Centro de Investigación y Seguridad Nacional (Cisen), por un monto de 3 millones 228 mil pesos."[36] Hasta la fecha no hay responsables sobre la compra de estos contratos en México.

[36] Redacción, "México compro equipos."

3 CAPÍTULO II: DERECHO A LA PRIVACIDAD Y DERECHO A LA PROTECCIÓN DE DATOS: LOS PILARES FRENTE A LA ARBITRARIEDAD

3.1 Derecho a la privacidad

3.1.1 Definición

El derecho a la privacidad es un derecho profundo y con diversas dimensiones. Uno de los primeros precedentes del derecho a la privacidad es el ensayo de Samuel Warren y Louis Brandeis "*The Right to Privacy*". Las preocupaciones de los autores en ese tiempo era la difusión de fotografías por medio de periódicos que podrían dañar la privacidad de las personas.[37] Había una gran preocupación de cómo la ley podía proteger a los ciudadanos del desarrollo de nuevas tecnologías como las fotografías. La privacidad siempre ha sido una preocupación con el desarrollo de nuevas tecnologías.

El derecho a la privacidad tiene múltiples dimensiones pues así lo han establecido varios teóricos del derecho y cortes en su jurisprudencia y doctrina.

Por ejemplo: para la CIDH el derecho a la privacidad puede entenderse en cuatro dimensiones: "1) El derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas. 2) El derecho a gobernarse por reglas propias definidas con base en un proyecto de vida individual. 3) La protección de todos los datos que se produzcan en un espacio reservado, es decir se prohíbe la divulgación o circulación de la información capturada, sin consentimiento del titular.4) La protección a la vida privada protege el derecho a la propia imagen."[38]

Para Pozen en su *artículo* "*Privacy-Privacy Tradeoffs*" La privacidad tiene seis dimensiones: "1*) The right to be alone. 2) Limited access to the self. 3) Secrecy. 4) Control over personal information. 5) Personhood or the protection of one 's personality and 6) Intimacy*."[39] Ambas autoridades no ofrecen un análisis radicalmente diferente; al contrario, el análisis denota que la privacidad podría componerse en dos grandes bloques: 1) La vida privada que incluye la

[37] Samuel D. Warren y Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, No. 5. (Dec. 15, 1890): 193-195, http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C.

[38] María Solange Maqueo, y Alessandra Barzizza Vignau, *Democracia, privacidad y protección de datos personales* (Ciudad de México: Instituto Nacional Electoral, 2019), 21.

[39] David E. Pozen. "Privacy - Privacy Tradeoffs," *The University of Chicago Law Review* 83, No. 1 (Invierno 2016), 221-247.

intimidad y el derecho a tener un proyecto de vida propia. 2) El derecho a contar con una esfera jurídica que proteja de cuestiones arbitrarias que podrían dañar nuestro derecho.

Para fines de la tesis el derecho a la privacidad será entendido como el derecho que tiene toda persona a tener una protección contra injerencias que pudieran revelar aspectos íntimos de su vida. Como todo derecho no es un derecho absoluto sino tiene que estar sujeto a un test de proporcionalidad para ser limitado y por medio de un juez. Tal como Solange y Barzizza señalan en su texto "Democracia, privacidad y protección de datos personales" el derecho a la privacidad "no ampara una absoluta imposibilidad de realizar ciertas intromisiones por parte de la autoridad o de terceros en el ámbito privado de las personas".[40]

Toda intervención en el derecho tiene que ser validada constitucional y convencionalmente. Además, la intervención tiene que ser fundamentada y que no sea arbitraria. Es decir, tiene que cumplir una serie de requisitos que sean razonables, proporcionales y necesarios. En una intervención de comunicaciones tal y como lo prevé la ley existe un requerimiento a una autoridad jurisdiccional, una previa ponderación por parte del juez, diversos formatos que especifican con quién, por cuánto tiempo y que se pretende encontrar en el uso de la intervención de comunicaciones.

Tal como fue expuesto en el primer capítulo el uso de estas nuevas tecnologías de espionaje hace que sea muy fácil para la autoridad evitar el contacto con una autoridad jurisdiccional y con una empresa de telecomunicaciones para intervenir en el teléfono de un ciudadano.

3.1.2 El derecho a la privacidad en el marco legal mexicano

Ahora bien, es importante saber ¿Cómo se entiende este derecho en el marco jurídico mexicano?

Comprender cómo entendemos el derecho a la privacidad hace que podamos construir una mejor defensa para diseñar mecanismos y legislación adecuada para regular de manera efectiva estas nuevas herramientas de vigilancia. Nuestra constitución, a pesar de un texto que se modifica con gran frecuencia, no ha incluido ninguna mención expresa del derecho; no

[40] Solange, María y Barzizza, "Democracia, privacidad y protección de datos personales," 45.

obstante, esto no quiere decir que no se encuentre en el texto constitucional. Al contrario, este está presente en el artículo 16 constitucional.

"Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento."[41]

La SCJN ya se ha pronunciado respecto del fundamento constitucional del derecho de la privacidad y en su Amparo en Revisión 134/2008 establece que se encuentra en el primer párrafo del artículo 16 constitucional.[42]

Asimismo, estableció en la tesis derivada de ese juicio que el derecho a la privacidad no solamente se limita a la injerencia física sino que "puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida."[43]

En el marco mexicano este derecho está construido de una manera que podemos entenderlo con las múltiples dimensiones que los teóricos y autoridades de DH han señalado. No solo se limita a un espacio físico, si no, va más allá de él por lo que el derecho a la privacidad se extiende por las dimensiones que se señalaron anteriormente.

Asimismo, la SCJN ha reconocido que el derecho a la privacidad es un derecho el cual su limitación es excepcionalísima y la autoridad siempre tiene que señalar la razón de su limitación. Por ello, la autoridad deberá probar que tiene "elementos objetivos y razonables para justificar válidamente la afectación a la libertad y seguridad personal." Esto quiere decir que en cualquier intervención por parte de la autoridad debe ir fundamentada. En México existe un grave problema de medidas de vigilancia excesivas y que no han dado ningún resultado.

[41] Constitución Política de los Estados Unidos Mexicanos, CP, art. 16, Diario Oficial de la Federación [DOF] 05-02-1917, últimas reformas DOF 28-05-2021 (Mex).
[42] Amparo en Revisión 134/2008, Segunda Sala de la Suprema Corte de Justicia [SCJN].
[43] DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, Segunda Sala de la Suprema Corte de Justicia [SCJN], Semanario Judicial de la Federación y su Gaceta, Novena Época, tomo XXVII, mayo de 2008, Tesis 2a. LXIII/2008, página 229 (Mex).

Tal y cómo lo señala R3D puesto que "únicamente el 8.76% de las averiguaciones previas en las que se ha utilizado alguna medida de vigilancia entre 2013 y 2015 se ha ejercido la acción penal. Lo cual sugiere que aproximadamente el 90% de las personas que podrían haber sido vigiladas con fines de investigación penal no han sido acusadas de ningún delito ante un juez."[44] Esto quiere decir que las medidas de vigilancia no están siendo debidamente aplicadas y puede que no se justifique su necesidad ni razonabilidad.

Para finalizar dicho derecho está contemplado en diversos tratados jurídicos los cuales México ratificó y es parte: la Declaración Universal de Derechos Humanos (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Convención sobre los Derechos del Niño (artículo 16) y la Convención sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y sus Familiares (artículo 14).[45]

Ahora bien, respecto a la jurisprudencia de la Corte Interamericana de Justicia la cual es vinculante para México. Es importante mencionar lo siguiente, el derecho a la privacidad está previsto en el artículo 11 de la Convención Americana y los artículos V y X de la Declaración Americana.

El artículo 11 establece que: 1. toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.[46]

Asimismo, el artículo V de la Declaración Americana establece "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar." que es el derecho a la protección a la honra, la reputación personal y la vida privada y familiar. El artículo X establece "Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia." En este derecho está comprendido el derecho a la inviolabilidad y circulación de la correspondencia. [47]

[44] R3D, *Gobierno Espía*, 58.
[45] Solange, María, y Alessandra Barzizza, *Democracia, privacidad y protección de datos personales*, (Ciudad de México: Instituto Nacional Electoral, 2019), 45.
[46] Convención Americana sobre Derechos Humanos (Pacto de San José). 22 de noviembre de 1969.
[47] Declaración Americana de los Derechos y Deberes del Hombre. 1948.

Ahora el derecho a la privacidad tiene diferentes dimensiones las cuales la Comisión Interamericana ha señalado como cuatro por lo menos:

"a) el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas; b) el derecho a gobernarse por reglas propias según el proyecto individual de vida de cada uno; c) el derecho al secreto respecto de lo que se produzcan en ese espacio reservado con la consiguiente prohibición de divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona; y d) el derecho a la propia imagen."[48]

En este caso la dimensión del derecho a la privacidad es la que indica en el inciso a) la cual protege de invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad.

Asimismo, ha aclarado que la correspondencia está protegida por el art. 11 de la Convención; asimismo, la jurisprudencia ha incluido las comunicaciones telefónicas y la que se da por medio de nuevas tecnologías como el Internet.[49] Aunado a esto en los Casos Tristán Donoso vs Panamá y Escher y otros vs Brasil, la Corte Interamericana reconoció que si bien estas no comunicaciones no están cubiertas de forma explícita si se encuentran protegidas.[50]

3.1.3 El derecho a la privacidad en el marco jurídico estadounidense

Debido a la extensa jurisprudencia que tiene Estados Unidos de América (EUA) sobre el derecho a la privacidad y su relación con las nuevas tecnologías de intervención de comunicaciones considero que es importante observar cómo entienden el derecho a la privacidad en EUA. Se hará revisión de una serie de casos emblemáticos que han marcado el derecho a la privacidad en el contexto digital.

Es importante mencionar que los casos se centran en la intervención de comunicaciones y no en los programas de vigilancia como Pegasus. Debido a que es una tecnología nueva no hay muchos precedentes jurídicos en el mundo sobre su uso; sin embargo, a través del derecho comparado podemos vislumbrar idea sobre cómo regular este nuevo tipo de tecnologías.

El concepto de privacidad para el contexto de EUA en este texto lo entendemos como lo entiende la Cuarta enmienda es "*the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no*

[48] CIDH. *Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión.* OEA/Ser.L/V/II.149. (Diciembre 31, 1999).
[49] OEA. *Estándares para una Internet Libre, Abierta e Incluyente Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.* OEA/Ser.L/V/II. (Marzo 15, 2017)
[50] Caso Tristán Donoso vs. Panamá. Caso 12.360. Inter-Am. C.H.R. (2009). Caso Escher vs. Brasil. Caso 12.353. Inter-Am. C.H.R. (2009)

Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Es decir, el enfoque a analizar sobre este derecho de privacidad es a no ser molestado en nuestra esfera personal y protegernos contra cualquier arbitrariedad que no tenga una causa probable o algún fundamento en la ley. Es importante esta distinción porque el derecho a la privacidad es sumamente amplio.

Por ejemplo: En EUA la primera enmienda se ha catalogado como "*Privacy of beliefs*" que básicamente menciona que el Congreso no podrá hacer ninguna ley que establezca alguna religión o que prohíba el ejercicio de una. En este caso se garantiza que cada persona pueda ejercer su propia religión individual y que el gobierno no interfiera con sus creencias. Otro ejemplo sería que el "*Fourteenth Amendmen*t" establece "*No State shall… deprive any person life, liberty, or property without due process of law*" y que la *Supreme Court of the United States* (SCOTUS) lo ha entendido cada vez más como una enmienda que puede interactuar con la crianza de los hijos, procreación, matrimonio y el tratamiento médico.[51] Este *fourteenth amendment* expone otra dimensión de la privacidad que la podríamos enmarcar en la privacidad que una persona tiene para la toma de decisiones personales. Por eso es de vital importancia tener en claro siempre el concepto dinámico de privacidad y sus múltiples dimensiones. Al hablar sobre el derecho a la privacidad en EUA en esta tesis se hará referencia a la Cuarta enmienda y enfocado en el entorno digital.

Para empezar el fundamento constitucional del derecho a la privacidad se encuentra en la cuarta enmienda. En ella se establece lo siguiente: "*the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*."[52] Tiene una gran similitud con nuestro artículo 16 constitucional; sin embargo, la cuarta enmienda ha sido discutida y profundizada gracias a múltiples casos. Por ejemplo, durante mucho tiempo para probar que había sido violentado tu derecho a la cuarta enmienda tenías que ofrecer evidencia sólida que efectivamente probará que habían invadido tu

[51] "The Right to Privacy," Exploring Constitutional Conflicts, visitado el 26 de enero de 2020, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

[52] "Fourth amendment," Fourth Amendment, visitado el 2 de junio de 2021, https://www.law.cornell.edu/constitution/fourth_amendment.

privacidad. Ahora, ya no es así, solo tienes que probar que tienes una expectativa de privacidad y que ha sido violentada arbitrariamente por el gobierno.

Ahora bien, la Cuarta enmienda puede aplicarse a multitudes de medidas de vigilancia, pero en este texto nos enfocaremos a las medidas que utilizan algún medio electrónico para su ejecución. En este caso EUA entiende la vigilancia electrónica como "*the nonconsensual acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or electronic communication, under circumstances in which a party to the communication has a reasonable expectation of privacy."*[53]

Ahora bien, hay múltiples tipos de vigilancia electrónica como el uso de micrófonos ocultos, videograbaciones, geolocalización, monitoreo tráfico de datos e internet. Si bien, pueden usarse uno, dos o tres tipos para las tareas de seguridad ¿Qué pasa con Pegasus que puede usarlos todos al mismo tiempo? ¿Dónde ponemos el límite?

3.1.3.1 Katz v United States

El concepto de expectativa de privacidad surge del caso que resolvió la SCOTUS en el cual Katz era un corredor de apuestas que usaba un teléfono público para correr las apuestas. La policía interviene el teléfono público que usaba argumentando que como era un teléfono público no había una expectativa de privacidad, pues era un bien público. Al final, la SCOTUS determina que si bien, era un espacio público la cuarta enmienda no solo protege lugares sino personas y que Katz tenía una expectativa de privacidad.[54] Es decir, Katz usaba una cabina de teléfono pensando que está en un lugar seguro que no debería estar sujeto a alguna invasión de privacidad.

A partir de este caso, el concepto de expectativa de privacidad se vuelve vital para entender la cuarta enmienda. De hecho, el juez Harlan propone una prueba para saber si existe o no una expectativa razonable de privacidad. Consiste en dos premisas fundamentales: 1) El individuo exhibe una expectativa (subjetiva) de privacidad. 2) Esta expectativa es reconocida por la sociedad. Si ambas premisas se cumplen y la acción hecha por el gobierno interviene en alguna de ellas entonces se ha violado la Cuarta enmienda.

---

[53] "Electronic Surveillance," Electronic Surveillance, visitado el 9 de febrero de 2020, https://www.law.cornell.edu/wex/electronic_surveillance.
[54] Charles Katz v. United States, 389 U.S. 347 (1967).

Por ejemplo, si la sociedad tiene una expectativa de privacidad que las fotos que se encuentran en su teléfono son suyas o que las contraseñas que almacenan en su teléfono están dentro de una expectativa de privacidad. La sociedad considera razonable que los contenidos en tu teléfono son privados y están lejos de una intervención arbitraria. Entonces, si el gobierno decide usar un programa de vigilancia doméstica para extraer fotos y contraseñas de mi celular sin una orden judicial previa violaría claramente la expectativa de privacidad.

Si se usa el *spyware* Pegasus para extraer datos de nuestro celular sin una orden judicial previa que justifique una medida tan intrusiva entonces hay violaciones al derecho a la privacidad. El problema de *spywares* como Pegasus es que ofrecen absolutamente toda la información, es decir al usarlo tienes acceso a todo aspecto del celular.

Si una autoridad adquiere una orden judicial para obtener datos de geolocalización usando Pegasus por los próximos siete días ¿Cómo sabemos que no va a activar la cámara del celular o que va a extraer fotos íntimas del celular? Es ahí la razón por la que no se puede equiparar una intervención de comunicaciones con la utilización de spyware de vigilancia.

3.1.3.2 Jones v United States

Otro caso importante para entender el derecho a la privacidad es *United States v Jones* en 2012. En el cual Antoine Jones fue investigado por el Federal Bureau of Investigation (FBI) por tráfico de droga. El FBI junto con la policía pidieron al juez una orden judicial para instalar un GPS en su coche. El juez autorizó dicha medida, pero pidió que fuera instalada en los siguientes 10 días; sin embargo, fue instalada hasta el día 11. Por lo que la orden judicial ya no era válida para el caso.

El dispositivo estuvo en el coche de Antoine por 28 días y con los datos generados por el dispositivo lo detuvieron. Un corte de distrito determinó que la información obtenida del GPS cuando estaba estacionado en su casa no podía usarse porque había una expectativa de privacidad; no obstante, la información obtenida cuando usaba calles y carreteras sí, debido a que no había una expectativa de privacidad al ser espacios públicos. Posteriormente, un circuito en D.C determinó que toda la información obtenida por el GPS violaba la Cuarta Enmienda. La Corte determina que efectivamente al ser una búsqueda conforme a la Cuarta Enmienda debe tener una orden judicial.

Lo más relevante del caso es la discusión que tiene la SCOTUS acerca del uso de dispositivos GPS y cómo afectan el derecho a la privacidad. La opinión que ofrece una mejor claridad sobre el problema es la del Juez Sotomayor. En su opinión establece que no se necesita presencia física para que ocurra una violación a la privacidad y con el nuevo desarrollo de tecnología es posible que los límites en la privacidad se vuelvan borrosos pero el test de Katz continúa siendo útil.

El punto clave es reconocer lo que puede revelar la tecnología GPS como lo señala opinión "*GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."*[55]

Efectivamente, solo a través de la localización podemos saber detalles íntimos de la persona y a quién realmente se está vigilando es al conductor del automóvil, este solo es un medio. La afectación a la privacidad es para la persona. Este criterio contrasta fuertemente con el sostenido por la SCJN en la cual no alcanza a reconocer que, si bien el GPS localiza al celular, el que sufre la invasión a la privacidad es la persona y no el dispositivo.

3.1.3.3 Kyllo v United States

Otro caso importante para entender cómo funciona el derecho a la privacidad frente avances tecnológicos es el presente caso. En 1991 el agente William Elliott tenía la sospecha que el ciudadano Danny Kyllo cultivaba marihuana en su departamento. Para cultivar esta planta es necesario luz de alta intensidad que generalmente provocan un aumento en la temperatura del cuarto. Por lo que el agente con su compañero instaló cámaras térmicas del otro lado de la calle para identificar si existía un aumento de la temperatura en el departamento de Kyllo. Las cámaras captaron un aumento en la temperatura en el departamento por lo que podría indicar que efectivamente Kyllo podría estar cultivando marihuana. Finalmente, el agente obtuvo la orden de cateo que pidió al Juez. Al entrar al domicilio encontraron un cultivo de aproximadamente 100 plantas de marihuana por lo que Kyllo fue arrestado.

[55] United States v. Jones, 615 F. 3d 544 (2012).

Kyllo combatió la sentencia diciendo que el uso de cámaras térmicas violaba la cuarta enmienda al ser una busqueda y una violación a su expectativa de privacidad. La Corte de Apelaciones estableció que Kyllo no tenía expectativa de privacidad pues nunca realizó alguna acción para ocultar el calor que irradiaba su casa. Igualmente, la Corte estableció que las imágenes obtenidas por las cámaras no revelaban ningún aspecto intimo de su vida.

Posteriormente, el caso llegó a la SCOTUS bajo la pregunta sobre si el uso de cámaras térmicas desde una calle pública a una casa privada para detectar aumentos de temperatura constituía una búsuqeda en el sentido de la cuarta enmienda. La Corte resalta que con el avance de la tecnología el grado de privacidad es afectado bajo los términos establecidos en la Cuarta enmienda. Por lo tanto, la Corte determina que obtener por medio de tecnología especial cualquier información respecto del interior de una casa que no podía obtenerse sin la intrusión a un área constitucional protegida constituye una búsqueda pues la tecnología no está disponible al público. [56]

Es decir, cualquier uso de tecnología especial lejos del poder la ciudadanía que sea usada para intervenir en un espacio protegida es considerada una búsqueda. Esta regla se traslada tecnologías nuevas o que están gestandose por lo que crea una regla que perdura a pesar del avance de la tecnología. Un punto importante es la protección que otorga la Cuarta enmienda al hogar no está ligada a la calidad o cantidad de información obtenida. Si la información obtenida es relevante o no, copiosa o escueta, la protección es la misma.

Por lo tanto, el uso de nuevas tecnologías en espacios protegidos por la Cuarta enmienda si invaden alguna expectativa de privacidad deben requerir una orden antes de ser ejecutados. No importando si la tecnología podía obtener información precisa o amplia del sujeto al que será aplicada la medida.

Es un acierto el razonamiento de la Corte al crear reglas amplias que protegan la privacidad de los ciudadanos frente al uso de nuevas tecnologías cada vez más especializadas y precisas. Esto revela directrices a las que México podría orientarse creando reglas que protejan ampliamente espacios que ellos consideren privados.

3.1.3.4 Carpenter v United States

[56] Kyllo v. United States, 533 U.S. 27 (2001).

Finalmente, el último caso y el más reciente respecto a la privacidad es uno que contrasta fuertemente con lo que pasa en México y la relación con las empresas de telecomunicaciones. En invierno de 2010 ocurrieron una serie de robos en Detroit, Michigan y Ohio. El Federal Bureau of Investigation (FBI) obtuvo los números de los posibles implicados y pidieron órdenes judiciales para obtener "*cell site location information*" (CSLI). Para entender este concepto es necesario aclarar que todos los celulares se conectan con una antena llamada "cell site". La conexión a la antena se hace de manera constante y sin que medie algún tipo de autorización por parte del usuario. Cada conexión con la antena crea un "*cell site location information* (CSLI). Toda esta información creada por las empresas de telecomunicaciones se encuentra regulada en el *Stored Communications Act.*

Ahora bien, el gobierno pidió a la empresa de telecomunicaciones darle estos CSLI sobre el teléfono de Carpenter y esta le otorgó aproximadamente 12, 898 CSLI de los anteriores 127 días. El principal argumento de Carpenter era que lo que el FBI necesitaba era una orden judicial de búsqueda o en inglés "*warrant*" para obtener estos datos. La Corte de Distrito desestima esta demanda y señala que gracias a la información saben que Carpenter participó en la serie de robos.

Posteriormente, el sexto circuito confirma la decisión de la Corte de Distrito puesto que a su parecer no había una expectativa razonable de privacidad, puesto que cuando una persona firma un contrato con la empresa de telecomunicaciones cede su información a las empresas de telecomunicaciones.[57] Finalmente, la SCOTUS decidió que era necesario un warrant bajo la Cuarta Enmienda.

La decisión de la SCOTUS impactaría en gran medida en cómo se concebía el derecho a la privacidad en el contexto digital. ¿Puede la policía acceder a la información que tienen las empresas de telecomunicaciones sobre ti? Sí, por supuesto. Puede ayudar como una medida sumamente eficaz para prevenir o detener crímenes inclusive podría ayudar a la localización de personas desaparecidas. Surge la pregunta ¿Se necesita orden judicial o warrant para acceder a estos datos? Por supuesto, salvo en casos sumamente excepcionales.

Los metadatos como los CSLI generan una imagen clara y profunda como se estableció en el capítulo 1. El Juez Roberts Jr. hace un comentario importante "*We decline to grant the*

[57] Carpenter v. United States. 819 F. 3d 880 (2018).

state unrestricted access to a wireless carriers database of physical location information."[58] La cantidad que manejan las empresas de telecomunicaciones es enorme y su alcance es aún mayor.

3.2 El derecho a la protección de datos

3.2.1 Definición

El derecho a la protección de datos personales es un derecho relativamente nuevo por su naturaleza. Conforme el ser humano fue progresando y la tecnología mejoraba era evidente que surgieran problemas con los datos personales. La Unión Europea (UE) ha sido un ente que ha aportado legislación importante en materia de datos personales. El Reglamento General de Protección de Datos (Reglamento 2016/679) o GDPR, por sus siglas en inglés, es el más reciente instrumento de la UE. Anteriormente, existía la Directiva de Protección de Datos o Directiva 95/46/CE creada en 1995.

La legislación en materia de datos personales en EUA está comprendida en una serie de normativa local y federal pero no hay una sola ley que rija la protección de datos personales.[59] Por ejemplo, existe la *Health Insurance Portability and Accountability Act (HIPAA)* para datos personales en materia de salud. Otro ejemplo, sería el *Gramm – Leach – Bliley Act (GLBA)* Existen leyes locales como *California Consumer Privacy Act (CCPA)* o *The New York SHIELD Act* las cuales regulan este tema de manera local. No obstante, no hay alguna ley federal o directiva general como en otros países. Esto genera que no exista una protección amplia al derecho y que muchas veces empresas puedan violentar el derecho. [60]

La discusión no es menor pues diversos autores y cortes han entendido que los datos personales al pertenecer dentro del campo de la intimidad de la persona están protegidos por el derecho a la privacidad. Si bien es razonable y comprensible ese análisis, este texto apoya la idea que el derecho a la protección de datos personales es un derecho autónomo al derecho a la

[58] Carpenter v. United States. 819 F. 3d 880 (2018).
[59] Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally White and Case, *Data Protection Law in the USA* (Advocates for International Development Lawyers Eradicating Poverty Agosto 2013), https://www.neighborhoodindicators.org/sites/default/files/course materials/A4ID_DataProtectionLaw%20.pdf.
[60] Josiah Wolfson, "The Expanding Scope of Human Rights in a Technological World—Using the Inter-American Court of Human Rights to Establish a Minimum Data Protection Standard across Latin America," *The University of Miami Inter-American Law Review* 48, No. 3 (Spring 2017): 204.

privacidad. El argumento central de este razonamiento es que los datos personales simplemente son, no dependen de una expectativa de privacidad o del contexto en el que se den, sino que el procesamiento, el tratamiento y su protección se da simplemente por su condición de ser.[61]

La protección de datos personales depende de su manejo, almacenamiento, distribución, transmisión, entre otros aspectos. Es decir, al nosotros al afectar alguna parte del ciclo de vida de los datos personales estamos violentando el derecho a la protección de datos personales. Eso no depende de si había o no una expectativa de privacidad o del contexto, eso simplemente representa que dentro de la cadena de protección de datos personales fue perjudicada una parte.

Esto provoca que la protección a los datos personales sea mucho más amplia y progrese de acuerdo con los avances tecnológicos. La doctora Lynskey hace hincapié a que todo dato que hace identificable o podría hacer identificable a una persona sería materia de protección de datos personales. Es decir, no entraría a discusión si el concepto de dato personal depende del contexto. Por ejemplo, si se dice que un dato es personal porque invade un aspecto de la privacidad se tendría que tomar en cuenta el contexto. En cambio, si se toma al dato personal como un derecho propio no es necesario tomar el contexto o ponderar. El dato personal simplemente es o no es de acuerdo con la legislación en materia de datos personales.[62]

En la medida de que la tecnología avanza se requiere legislación que entienda cómo se comportan los datos, cómo deben de almacenarse, su tratamiento específico de acuerdo con el dato. Por lo que si la ley en materia de datos menciona que el género es un dato personal no debe de cuestionarse si es o no debido a que hay una ley que claramente estipula que esa categoría debe tomarse como dato personal.

La doctora Lynskey aporta argumentos importantes a esta visión. La protección de datos personales como derecho autónomo puede ayudar a reducir la discriminación y el robo de identidad. La discriminación es reducida al exigir que el tratamiento de datos sea de una manera anónima y libre de identificadores que podrían poner en riesgo a la persona.[63] Esto se logra por medio de legislación que establezca que el tratamiento de datos en ciertos contextos sea totalmente anónimo. Lynskey hace mención del panóptico del que hablaba el filósofo Jeremy

[61] Orla Lynskey, "DECONSTRUCTING DATA PROTECTION: THE 'ADDED-VALUE' OF A RIGHT TO DATA PROTECTION IN THE EU LEGAL ORDER," *The International and Comparative Law Quarterly* 63, No. 3 (Julio 2014): 584.
[62] Lynskey, "DECONSTRUCTING DATA PROTECTION," 584.
[63] Lynskey, "DECONSTRUCTING DATA PROTECTION," 584.

Bentham, esto es, una estructura que todo lo ve sin que sepa la persona que está siendo observada.

Siguiendo con el segundo argumento de la doctora Lynskey es que el derecho a la protección de datos reduce las asimetrías de poder entre el usuario y aquel que se encuentra en posesión del dato personal. Debido al mercado emergente de datos personales las compañías usan estos datos personales para venderlos a quien ofrezca una buena cantidad de dinero.

Si una aplicación que pone filtros en nuestro rostro al tomarnos selfis recolecta nuestras caras y ofrece esta información a instituciones policiacas ¿Qué puede prevenir esto? Legislación y por supuesto una correcta aplicación de la ley. La materia de datos personales es una materia que debe modificarse y legislarse constantemente siempre cuidando la protección del usuario y fomentando la innovación.

Si se tiene claro quién es el encargado de cuidar nuestros datos personales y quién será el responsable de su tratamiento entonces hay una rendición de cuentas clara que le da al usuario herramientas para prevenir esta asimetría de poder.[64] Finalmente, el derecho a la protección de datos personales incorpora el derecho que tiene el ciudadano a acceder, rectificar, cancelar y oponerse a la utilización de sus datos personales y a que los datos sean tratados con altos estándares de calidad en su almacenamiento, tratamiento, protección y las demás salvaguardas para su correcta utilización.

3.2.2 El derecho a la protección de datos en el marco jurídico mexicano

México no contaba con un reconocimiento expreso del derecho a la protección de datos hasta hace unos años.[65] No quiere decir que México no reconocía este derecho previamente puesto que en el ámbito federal desde 2002 a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental ya se vislumbraba una cierta protección a los datos personales. En el dictamen que surge de la reforma constitucional de 2009 se expresa que el derecho a la protección de datos personales surge como un límite al derecho de acceso a la información.

[64] Lynskey, "DECONSTRUCTING DATA PROTECTION," 584.
[65] DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, Diario Ofical de la Federación [DOF] 01-06-2009 (Mex.).

Asimismo, establece que debido a la evolución de las tecnologías era necesario establecer un derecho que se adaptara y protegiera a los usuarios en el mundo digital y no digital. [66] Un acierto es que se preveía que la protección de datos personales fuera en dos ejes: una protección para los datos personales en posesión de entes privados y en posesión de entes públicos.

En México existen dos ordenamientos en esta materia aplicable a sujetos distintos. El primero es la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) para todas las personas físicas o morales privadas que no sean sociedades de información crediticia o personas que se dediquen a recolectar y almacenar datos personales para uso personal. El segundo ordenamiento es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) la cual aplica para autoridades establecidas en el artículo 1.[67]

La distinción entre particulares y sujetos obligados facilita saber el tipo de reglas que le aplican a cada uno de los sujetos. Asimismo, quedan bien delimitadas las obligaciones y derechos que tiene cada sujeto por lo que no hay ambigüedad sobre el marco normativo al que está sujeto el particular o el sujeto obligado.

México cuenta con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) el cual es un órgano constitucional autónomo. El cual es el órgano garante de los derechos de acceso a la información y el derecho a la protección de datos personales.[68] Su antecesor fue el Instituto_Federal de_Acceso a la Información (IFAI) creado el 24 de diciembre de 2002.[69] Tenía la naturaleza jurídica de un organismo descentralizado, no sectorizado con una personalidad jurídica y patrimonio propio. Debido a

---

[66] "ÍNDICE DEL PROCESO LEGISLATIVO CORRESPONDIENTE A LA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 01 DE JUNIO DE 2009" Constitución 1917 - 2017, visitado el 20 de febrero de 2021, https://www.constitucion1917-2017.pjf.gob.mx/sites/default/files/CPEUM_1917_CC/procLeg/187%20-%2001%20JUN%202009.pdf

[67] **Artículo 1 (LGPDPPSO) -** Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

[68] Constitución Política de los Estados Unidos Mexicanos, CP, Diario Oficial de la Federación [DOF] 05-02-1917, últimas reformas 28-05-2021(Mex.).

[69] Decreto del Instituto Federal de Acceso a la Información Pública, Diario Oficial de la Federación [DOF] 24-12-2002 (Mex.), formato HTML, https://www.dof.gob.mx/nota_detalle.php?codigo=716452&fecha=24/12/2002.

que existía una disparidad entre las leyes de acceso a la información puesto que seguían diferentes modelos planteados por la Ley Federal de Transparencia y Acceso a la Información.[70] Se reformó el segundo párrafo del artículo 6to constitucional el cual estableció el estándar mínimo del ejercicio del derecho y sienta los principios de la política de transparencia gubernamental.[71]

Posteriormente, el 1 de junio de 2009 se reformó el artículo 16 constitucional el cual reconoció de manera expresa el derecho a la protección de datos personales, así como los derechos ARCO (Acceso, rectificación, cancelación).[72] Asimismo, las facultades del congreso de la unión fueron reformadas el 30 de abril de 2009 para poder legislar en materia de protección de datos personales en posesión de particulares.[73]

Posteriormente, el 7 de febrero de 2014 se le otorgó a este ente, el carácter de un órgano constitucional autónomo el cual lo reconoció como un "organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley."[74]

Aunado a esto, el 4 de mayo de 2015 fue publicada en el DOF la Ley General de Transparencia y Acceso a la Información Pública lo cual reforzó las capacidades y facultades del INAI además de darle una gran relevancia el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.[75]

---

[70] José Antonio Caballero et al., *El Futuro del Instituto Federal De Acceso A La Información Pública y Protección De Datos Personales: Consideraciones Sobre Su Autonomía Constitucional* (Distrito Federal: Instituto de Investigaciones Jurídicas, 2012), 3, https://archivos.juridicas.unam.mx/www/bjv/libros/7/3196/2.pdf.

[71] Caballero et a., *El Futuro del Instituto Federal de Acceso a la Información*, 4.

[72] Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación [DOF] 01-06-2009 (Mex.).

[73] Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación [DOF] 30-04-2009 (Mex.), formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5089047&fecha=30/04/2009.

[74] DECRETO por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia. Diario Oficial de la Federación [DOF] 07-02-2014 (Mex.), formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014.

[75] DECRETO por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. Diario Oficial de la Federación [DOF] 04-05-2015 (Mex.)., formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015.

Lo cual fue un paso importante ya que funciona como un contrapeso al poder además de contar conocimientos técnicos y especializados en la materia. De esta manera no dependería de lo que estableciera el Gobierno en turno al ser una institución técnica, reguladora y especializada.[76]

El marco normativo del INAI tiene diversas disposiciones dentro de las cuales destacan: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPP)Ley General de Transparencia y Acceso a la Información Pública (LGTA) y Ley Federal de Transparencia y Acceso a la Información Pública (LFTA).

Entre las principales facultades del INAI son garantizar el derecho a la protección de datos personales en posesión de sujetos obligados, conocer y resolver los recursos de revisión y recursos de inconformidad que interpongan los titulares, promover acciones de inconstitucionalidad y controversias constitucionales y resolver los procedimientos de verificación para concretar si fueron violadas disposiciones de leyes aplicables en la materia.

La jurisprudencia e informes de la doctrina interamericana ha señalado que es fundamental que existan regímenes de protección de datos los cuales deben regular "el almacenamiento, procesamiento, uso y transferencia de datos personales sea entre entidades estatales como respecto de terceros."[77]

Asimismo, ofrece en su informe del comité jurídico interamericano: "Privacidad y protección de datos personales" una definición de datos personales la cual menciona que "abarca la información que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o indirecta, especialmente por referencia a un número de identificación o a uno o más factores referidos específicamente a su identidad física, fisiológica, mental, económica, cultural o social." Aunado a lo anterior, hace especial énfasis en que esto involucra a los datos o bits que son conocidos como metadatos pues al analizarlos revelan información íntima sobre la persona.[78]

---

[76] Leticia Raquel Real Rodríguez, "Desmantelar el INAI," *Nexos*, 14 de enero de 2021, https://anticorrupcion.nexos.com.mx/desmantelar-el-inai/.

[77] OEA. *Estándares para una Internet Libre, Abierta e Incluyente Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos*, OEA/Ser.L/V/II. (Marzo 15, 2017)

[78] OEA. *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, OEA/Ser.Q. (Marzo 26, 2015)

Respecto al tema central de la tesis es necesario identificar cómo funciona la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y cómo funciona en el texto de seguridad y vigilancia. En el presente caso, el análisis estará enfocado en el uso de datos personales por sujetos obligados. Siguiendo el marco normativo mexicano el derecho a la protección de datos personales se encuentra en el artículo 16 constitucional:

"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."[79]

Del derecho a la protección de datos personales se desprenden los derechos al acceso, rectificación, cancelación de estos y su oposición, estos son conocidos como los Derechos ARCO.

Asimismo, vemos que el derecho a la protección de datos personales no es un derecho absoluto, sino que hay límites cuando se trata de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros. En el Caso Pegasus el Estado no logró nunca justificar que alguno de estos límites fue usado para vulnerar la protección de datos personales. Era casi imposible justificar el uso de Pegasus en el dispositivo móvil de un menor de edad o de los papás de los normalistas desaparecidos por el Estado.

A falta de una legislación especial la ley aplicable sería la LGPDPPSO para el uso de Pegasus. Puesto que Pegasus fue usado por una instancia gubernamental y hasta ahora la evidencia señala que quien está en posesión de este spyware es el Estado Mexicano.[80]

---

[79] Constitución Política de los Estados Unidos Mexicanos, CP, art. 16, Diario Oficial de la Federación [DOF] 05-02-1917, últimas reformas DOF 28-05-2021 (Mex.).

[80] El uso de estos spywares no debería ser ilegal y no estoy sugiriendo que el Estado mexicano debería abstenerse de utilizar estas herramientas por completo. El Estado mexicano puede y debería usar estas herramientas en casos excepcionales en donde su uso esté debidamente justificado y sea una medida proporcional, razonable e idónea. Tal como lo expuse anteriormente México sufre una guerra contra el narcotráfico y los narcotraficantes han sido bastante difíciles de capturar o siquiera localizar. Si se usara Pegasus contra el móvil de un narcotraficante importante o algún allegado podría saberse dónde está localizado, grabar las conversaciones, grabar las llamadas y obtener de sus contactos nuevos teléfonos a los cuales podría usarse Pegasus. Poco a poco por medio de estas tecnologías podría ir descubriendo la verdadera red del narcotráfico e ir desmantelando. El problema es que la legislación actual no prevé aún limitaciones al uso de este tipo de tecnologías y por su capacidad tan intrusiva en el derecho tiene que revisarse muy claramente ¿Quién está en posesión de estos datos? ¿Cómo aseguramos que solo se revisen los datos requeridos en la orden judicial? ¿Cómo serán almacenados estos datos y si por su naturaleza no entran en la categoría de datos sensibles? El uso legal de Pegasus es el último paso puesto que previamente tiene que existir una adecuación normativa y sobre todo resultados que justifiquen que el Gobierno

3.2.2.1 Colaboración entre instancias de seguridad y empresas de telecomunicaciones

Ahora bien, la colaboración entre las autoridades y los concesionarios está prevista en la LGPDPPSO en su capítulo II "De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia" y en la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) en su capítulo "De las Obligaciones en materia de Seguridad y Justicia del Título Octavo de Colaboración con la Justicia.

En el artículo 189 de la LFTR se establece que los concesionarios, autoridades y proveedores de servicio de aplicaciones y contenidos están obligados a atender todo mandamiento escrito y fundado por la autoridad. El artículo 190 de la LFTR prevé que deberán colaborar con las instancias de seguridad en la localización geográfica en tiempo real de los equipos celulares. Debe conservar un registro de las comunicaciones que realice cada línea donde se establezcan datos como: el nombre, tipo de comunicación (oral o texto), datos para identificar el origen de las llamadas, la ubicación digital entre otros datos. Todos estos datos serán entregados a las autoridades previa orden judicial fundada y motivada.

Existe una discusión importante acerca de si es suficiente este tipo de legislación, es decir, si no hay un exceso en el plazo de conversación de la información, falta de precisión en cuanto a las motivaciones, la falta de precisión en las motivaciones de la autoridad, etc.[81]

La LFTR prevé parámetros que deben seguir los concesionarios para el resguardo y transferencia de estos datos personales. Existen parámetros técnicos que tiene que seguir las concesionarias y autorizadas en telecomunicaciones, pero para las instancias de seguridad no se prevén estos mecanismos. Los Lineamientos de Colaboración en Materia de Seguridad y Justicia son una herramienta para cubrir los casos en materia federal; sin embargo, en la justicia local también existen situaciones de cooperación que los lineamientos no alcanza a prever.[82]

El principal problema con la protección de datos personales es el mal uso que se le puede dar a los límites al derecho. Si la autoridad con el fin de obtener siempre los datos personales de los usuarios utiliza la seguridad ¿Cómo prevenimos que se cometan abusos con la bandera

mexicano ha hecho un buen uso de la intervención de comunicaciones, ha respetado el proceso judicial y ha dado resultados.

[81] Mónica Estrada Tanck, "De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia," en *Ley General de Datos para la Protección de Datos en Posesión de Sujetos Obligados Comentada*, ed. INAI, 244 (Ciudad de México: INAI, 2018).

[82] Estrada, "De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia." 247.

de la seguridad? La maestra Estrada señala que deben "establecerse regulaciones que acoten estas atribuciones y determinen (…) que su ejercicio debe respetar los principios de protección de datos (...) el principio de licitud y el principio de la proporcionalidad."

La LGPDPPSO prevé en su artículo 80 que la obtención y tratamiento de datos personales por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales. ¿Qué son necesarios y proporcionales?

Tal y como la maestra Estrada lo señala si hay una investigación para la persecución de un delito hace sentido, pero ¿Qué pasa cuando se utiliza el argumento de seguridad nacional? En el Caso Pegasus si la autoridad hubiera señalado que era necesario intervenir en los móviles de Carmen Aristegui y Rafael Cabrera por seguridad pública ¿Qué hubiera decidido la autoridad?

El artículo 81 establece que las autoridades en el tratamiento de datos personales usarán bases de datos para el almacenamiento de los datos y que solo una autoridad competente con previa autorización podrá intervenir en las comunicaciones. ¿Cuándo se requiere o no una autorización judicial?

Conforme la tecnología avanza deben de establecerse criterios claros que puedan tanto a concesionarios como a los usuarios saber con claridad los límites de la autoridad. En el artículo 82 de la LGPDPPSO establece que estas bases de datos creadas deben tener un estándar de seguridad alto para garantizar integridad, disponibilidad y confidencialidad de la información ¿Cómo aseguramos que efectivamente pasa esto?

En el CNPP en su artículo 300 establece que la autoridad tendrá que borrar los registros que rebasen la autorización judicial respectiva, no sean útiles, se declare sobreseimiento entre otros supuestos.

Valdría la pena considerar los principios de responsabilidad demostrada en materia de datos personales. La responsabilidad demostrada es el principio que establece que la autoridad deberá ser responsable por cumplir de manera efectiva con las medidas implementadas en materia de protección de datos. En el presente caso, la autoridad que esté en posesión de los datos, por ejemplo el ministerio público deberá cumplir con todas las medidas de protección de datos personales que marca la LGPDPPSO.

La OCDE en su documento *The OCDE Privacy Framework s* señala que el principio de responsabilidad demostrada es parte de los principios clave que deben aplicarse en la legislación nacional de cada país.[83] La OCDE establece que el principio debe ir acompañado por sanciones ilegales en caos de incumplirlas y principios de rendición de cuentas.

Por lo que en el caso de la información manejada por las autoridades en posesión de datos personales obtenidas por herramientas de vigilancia como Pegasus deberían respetar este principio. Debe existir una rendición de cuentas por parte de la autoridad de acatar este principio. Por ejemplo, en el caso de la PGR el INAI señaló su falta de cumplimiento de las obligaciones en materia de datos personales en el Caso Pegasus. Un paso adelante para la protección de datos personales podría ser revisar el cumplimiento de los Ministerios Públicos de las Entidades para comprobar si efectivamente están haciendo un correcto uso en materia de datos personales.

Asimismo, podría considerarse la implementación de los principios de borrado seguro por parte las autoridades que manejen este tipo de datos. El INAI en su "Guía para el Borrado Seguro de Datos Personales" establece que el borrado seguro es "la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima."[84]

El cumplimiento de este principio es de vital importancia puesto que las herramientas de vigilancia como Pegasus pueden extraer una gran cantidad de datos personales del dispositivo infectado. Por consiguiente, sería importante que las autoridades consideraran implementar las recomendaciones del INAI en esta materia.

Finalmente, el derecho a la protección de datos personales es un derecho de reciente creación y no muchos países latinoamericanos tienen una legislación robusta en la materia.[85] Sin embargo, lo que más nos tardemos en legislar y en adaptarnos a las nuevas tecnologías, mayor es el estado de indefensión de los usuarios.

Este estado de indefensión por lo menos en el caso mexicano podría atribuirse a una falta de normativa actualizada y clara respecto a la protección de datos personales frente a estas

---

[83] OCDE, *The OCDE Privacy Network* (OECD Publishing, 2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[84] INAI, *Guía para el Borrado Seguro de Datos Personales* (México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, junio de 2016), http://inicio.inai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf.

[85] Wolfson "The Expanding Scope of Human Rights in a Technological World," 43.

nuevas herramientas de vigilancia. La novedad y la rapidez a la que evolucionan estos mecanismos de vigilancia hace que la normativa no pueda avanzar al mismo paso.

Por supuesto, podríamos considerar otro factor como la interacción de familias jurídicas como el derecho anglosajón y el continental el cual cada uno pretende proteger los datos personales de las personas bajo su modelo. En el caso del modelo continental como es el caso de México la jurisprudencia y las leyes no han llegado aún a plantearse estos nuevos retos. La razón detrás puede ser que estos mecanismos no habían sido usados en territorio mexicano o que quizás no se había planteado el debate sobre las herramientas si no sobre la práctica de intervenir de comunicaciones. Hay un énfasis actual en la intervención de comunicaciones pero no en qué herramientas se usan para la intervención.

En México se ha hecho un gran avance en la legislación de datos personales; por ejemplo, ya se adhirió al Convenio 108 del Consejo Europeo y a su Protocolo Adicional Relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos el 12 de junio de 2018.[86] Además, el Estado mexicano ha expresado su intención de suscribirse al Convenio 108 Modernizado del Consejo Europeo. La intención de suscribirse al Convenio 108 Modernizado haría que México armonizara su legislación en materia de datos personales con estándares altos en protección de datos.

La jurisprudencia de este derecho es aún poca y no hay casos tan emblemáticos como en EUA. Hay tesis aisladas que señalan que el Estado debería proteger aún más el derecho ante las nuevas herramientas tecnológicas y los riesgos que estas presentan por sus características.[87]

Las autoridades tienen que ser transparentes y ofrecer una rendición de cuentas acerca del uso y la compra de este tipo de herramientas de vigilancia. No existen registros en los ciudadanos puedan encontrar información de los contratos que ha celebrado México respecto a la adquisición de estas nuevas herramientas. Si este *spyware* fuera vendido a grupos de

[86] DECRETO por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente, Diario Oficial de la Federación [DOF] 12-06-2018 (Mex.).

[87] PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS, Tribunales Colegiados de Circuito [TCC], Gaceta del Semanario Judicial de la Federación, Décima Época, tomo III, Septiembre de 2009, Tesis I.10o.A.6 CS, página 2200 (Mex.).

delincuencia organizada ¿Qué pasaría? No existen reglas claras por parte del gobierno para la adquisición de este tipo de *spywares*.

En el Caso de Pegasus ya existe un pronunciamiento del INAI en el cual por medio de su resolución INAI/054/19[88] determinó que la PGR incumplió con la LGPDPPSO pues no contaban con un sistema de gestión ni documentos de seguridad para el tratamiento de datos personales. Asimismo, dio vista a la Auditoría Superior de la Federación (ASF) para que verificará los bienes adquiridos por la PGR respecto a Pegasus y si se había cometido alguna irregularidad en su contratación.

También, pidió que se presentará una denuncia ante el Ministerio Público Federal para determinar si se habían cometido los hechos constitutivos del delito de ejercicio ilícito de servicio público, previsto en las fracciones IV y V del artículo 214 del Código Penal Federal. Tampoco existen noticias acerca de la investigación y de si se han hallado responsables. Finalmente, se le pidió a la PGR publicar en su portal los contratos de Pegasus hecho que tampoco ha ocurrido.

3.3 Test de proporcionalidad

3.3.1 Constitucionalidad de los fines perseguidos

Conociendo a profundidad cómo operan estos dos derechos y cómo se relacionan entre sí los denomino los pilares frente a la arbitrariedad. Si una autoridad pretende intervenir usando Pegasus tendría que justificar que el uso de Pegasus justifica no utilizar en su totalidad estos dos derechos.

Previamente, fueron señalados los límites que presentan estos dos derechos y hasta dónde nos protegen en el marco jurídico mexicano. Debido a que la autoridad no utilizó el *spyware* de manera legítima ni en una investigación la ponderación de derechos no puede hacerse de una manera correcta usando como base el Caso Pegasus. Si se hubiera realizado una solicitud al juez probablemente el juez notaría que no hay bases ni motivos para creer que los

[88] INAI, "DETERMINA INAI QUE FGR, RESPECTO AL SOFTWARE PEGASUS, INCUMPLIÓ LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS," comunicado INAI/054/19, 20 de febrero de 2019, http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf.

periodistas y activistas cometan o hayan cometido un ilícito. Ni mucho menos se justificaría el uso de una medida tan restrictiva.

Entonces, será desarrollado un caso hipotético donde la autoridad pretenda utilizar el *spyware* de Pegasus en el caso de un secuestro. La policía obtuvo el celular del secuestrador debido a que realizó la extorsión a la familia por medio de un celular. La policía considera que en este caso la intervención de comunicaciones común es insuficiente por lo tardado que sería el proceso y que el secuestrador ha enviado a los padres un supuesto dedo de la víctima.

El juez tiene que poner sobre la mesa los hechos, los principios y los derechos en juego. Primero, los derechos afectados por la medida serían el derecho a la privacidad y a la protección de datos personales del posible secuestrador. (P1) La restricción a estos derechos sería por medio de la herramienta Pegasus (M). El bien colectivo que trata de salvaguardar el Estado con esta medida es la seguridad pública y la integridad de la víctima (P2) Por lo que el Estado a través de la intervención de comunicaciones con Pegasus (M) busca salvaguardar la seguridad pública y proteger los derechos de la víctima.

3.3.2 Examen de idoneidad

El siguiente paso es hacer un examen de idoneidad. Es decir, analizar "la relación entre el medio seleccionado por el Estado y el derecho o fin que este busca promover a través de la implementación del medio."[89]

La persona que supuestamente tiene secuestrada a la persona sufrirá una afectación a sus derechos de privacidad y protección de datos personales, por la medida escogida por la policía (Uso del *spyware* Pegasus) para mantener la seguridad pública y la integridad de la víctima. En este caso el juez tiene que ponderar si la medida (M) es la idónea para cumplir P2.

Ahora dentro del rango de acciones que tiene la autoridad se encuentran las siguientes: 1) Usar elementos policiacos para vigilar un área y observar actividad sospechosa. 2) Utilizar la intervención de comunicaciones normal y pedirle a la concesionaria la localización en tiempo

[89] Laura Clérico, *Derechos y Proporcionalidad: Violaciones por acción, insuficiencia y por regresión. Miradas locales, interamericanas y comparadas* (Querétaro: Instituto de Estudios Constitucionales del Estado de Querétaro, 2018), 37.

real de la persona. 3) Utilizar el *spyware* Pegasus para obtener control de las funciones del celular y asegurar la mayor cantidad de datos posibles del celular.[90]

3.3.3 Examen de Necesidad

En este caso el juez tiene que realizar un "examen de medios alternativos menos lesivos o de necesidad" Determinar si existe una medida igual de idónea para cumplir con P2 y que restrinja mucho menos los derechos del posible secuestrador P1. La primera medida si bien es la que menos restringe los derechos del presunto culpable no es la más idónea. La cantidad de recursos gastados es importante y nada garantiza que la zona que patrullan sea en la que está la víctima. La segunda medida es la intervención de comunicaciones normal en la que la autoridad le pide a la concesionaria la localización en tiempo real del celular.

La medida afecta los derechos (P1) no obstante, si la autoridad sólo exige la localización en tiempo real del celular podría justificarse para proteger (P2). Si la autoridad pidiera la localización y las llamadas y mensajes de texto que ha enviado el número celular si ocasiona un perjuicio aún mayor a (P1). En la idoneidad de la medida es cuando entra en juego diversos factores a tomar en cuenta como la tardanza en la que puede incurrir la concesionaria y las horas vitales que se pierden en lo que el juez autoriza y la concesionaria entrega los datos.

Dado los hechos del caso el secuestrador ya ha amenazado a la familia con la entrega de un supuesto dedo de la víctima. La vida de la víctima corre mucho más peligroso pues el secuestrador muestra un alto grado de hostilidad hacia la víctima. La opción dados los hechos parece ser el uso de Pegasus.

Si es usado Pegasus podría ser una medida más que idónea porque es capaz de extraer una cantidad de datos enorme del celular de la persona. La afectación a P1 es mayor que con todas las medidas. El juez al no haber una legislación ni reglas claras sobre su utilización tiene que sacrificar los dos derechos del secuestrador con la esperanza que la medida funcione.

Se usa el término sacrificar porque la medida no tiene un marco normativo claro y la protección a los datos personales ha sido insuficiente tal y como lo expuso el INAI con la PGR.

[90] Recordemos que el spyware de Pegasus es una medida de vigilancia sumamente intrusiva tal y como lo expuse en el capítulo 1. Pegasus tiene acceso a los mensajes, los correos, las contraseñas de wifi, los contactos, los archivos del celular, las cámaras, el micrófono, la localización entre otras medidas.

Entonces ¿Qué podría hacer el juez en ese margen de tiempo tan apretado? Si el juez desconoce de las capacidades de vigilancia de Pegasus ¿Cómo tomará una decisión informada? ¿Qué ocurre si la policía nota que si acceden a la cámara podrían obtener fotos del lugar donde se encuentra el secuestrador? Podría efectivamente ser una medida idónea para saber la localización del secuestrador e incluso la víctima, pero eso indica que en todo momento la privacidad queda comprometida.

Si el celular obtiene audio o foto de un momento íntimo del secuestrador y posteriormente esos datos son filtrados por un mal manejo podría violentar aún más la protección a los derechos personales. Peor aún podrían filtrarse recabados por la policía con ayuda de Pegasus puesto que en México no es extraño que se filtren datos.

El peligro del desconocimiento del funcionamiento de estas nuevas tecnologías puede causar graves problemas. Si el juez supiera que el *spyware* de Pegasus es una herramienta de vigilancia, pero no entendiera toda a la capacidad de injerencia podría dictar una sentencia que estableciera "Se autoriza el uso del programa Pegasus para la investigación 1614". ¿Esto quiere decir que la policía tendría acceso a todas las herramientas que ofrece Pegasus?

Sería un pase en blanco para la autoridad para ocupar Pegasus al máximo de sus capacidades. La medida afecta no solamente los datos personales de la persona si no que la autoridad puede extraer la lista de contactos de la persona y posteriormente aplicar Pegasus a cada uno de los celulares bajo el argumento de la "seguridad pública". Se entraría nuevamente en un círculo vicioso en el cual la policía podría argumentar ante el juez "Queremos intervenir estos teléfonos pues creemos que podrían ser cómplices en la realización de un delito".

Posteriormente, el juez podría aplicar este mismo examen y determinar que se utilice Pegasus completamente o que solo se utilicen ciertas herramientas del programa. La policía en caso de la autorización completa nuevamente procede a extraer números y repetir el mismo proceso. ¿Cómo proteger los datos que se obtienen del uso de herramientas como Pegasus? ¿Cómo vigilamos al vigilante que no exceda de lo permitido?

3.3.4 Examen de proporcionalidad

Supongamos que el juez conoce a profundidad cómo funciona Pegasus y los alcances del *spyware* por lo que permite la medida, pero con ciertas limitaciones: el programa solo se

usará para obtener la localización en tiempo real, la obtención de los mensajes en plataformas de comunicación como *WhatsApp, Messenger* y SMS y el micrófono. Es decir, la persona que utilice el programa no podrá acceder a las fotos, los archivos, la cámara, entre otras cosas. El juez limita el alcance de la medida y la afectación de los derechos; sin embargo, no hay ningún mecanismo que nos asegure que efectivamente la policía revisará solo estos datos.

Un riesgo más de no regular propiamente estas nuevas herramientas. En este punto el juez tiene que decidir que la medida, a pesar de que sea sumamente intrusiva, sea lo menos restrictiva posible y que la herida se haga con un bisturí en lugar de con un machete.

Entonces, ahora chocan los derechos de la privacidad y la protección de datos personales (P1) contra la obligación de mantener la seguridad pública y salvaguardar la integridad de la víctima (P2). Ahora ¿existe una regla que privilegie un derecho sobre otro? Si bien no hay una regla que se aplique a este caso en específico si existen limitaciones a ambos derechos constitucionales en las que señalan que estos derechos pueden ser limitados por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros.

Es decir, pueden ser limitados estos derechos si entran en alguno de estos supuestos. No obstante, es importante que los derechos sean limitados con una justificación clara y más si se pretende usar herramientas tan invasivas. Usar estas limitaciones podría causar problemas en que la autoridad usará el argumento de "seguridad pública" o "seguridad nacional" como una justificación para actuar en todo momento.

La autoridad debe proporcionar al juez información que permita establecer que efectivamente la limitación aplica en este caso. Por eso la labor del juez es vital y sobre todo que los jueces estén capacitados en estas nuevas tecnologías de otra manera causaría una afectación grave a los derechos de las personas.

Ahora bien, en este caso no solamente es la seguridad pública lo que está siendo afectada sino los derechos de la víctima son los que están siendo gravemente perjudicados. Por lo que debe ser tomado en cuenta en la ponderación de los derechos. La vida de la víctima juega un rol vital en este examen de proporcionalidad. Para el Estado es importante que la integridad de la víctima se conserve intacta y que se ejecuten todas las medidas necesarias para su protección.

Entonces, el juez al decidir que efectivamente para proteger a la integridad de la víctima y la seguridad pública deben limitarse los derechos a la privacidad y a la protección de datos

por medio de la utilización de Pegasus de manera limitada, existe una ponderación de derechos en forma. El juez debería crear una regla-resultado de ponderación tal y como Laura Clérico señala estas reglas resultado vincularía a las reglas a quien realiza una ponderación y en este sentido, limitaría su discrecionalidad.[91] Se utilizaría para crear una red de reglas resultados de la ponderación en materia de derecho a la privacidad y la protección de datos.

La regla en este caso quedaría de la siguiente manera: si se trata de la injerencia en los derechos de privacidad y protección de datos personales de una persona que pueda ser el probable secuestrador entonces la restricción a los derechos no es excesiva por medio de Pegasus si: (1) La utilización de Pegasus se limita en su capacidad solo para las tareas que beneficien claramente la investigación del delito. (2) No existe un medio alternativo igual de idóneo, pero menos lesivo dentro de los medios presentados a la autoridad. (3) la restricción a los derechos de privacidad y protección de datos es plausible dado que se pretende salvaguardar la integridad de la víctima lo más pronto posible por los hechos fácticos del caso y mantener la seguridad pública.

[91] Clérico, *Derechos y Proporcionalidad*, 55.

3.4 CAPÍTULO III - LEGISLACIÓN SOBRE VIGILANCIA E INTERVENCIÓN DE COMUNICACIONES EN ESTADOS UNIDOS Y MÉXICO: COMPARACIÓN, CONTRASTE Y ANÁLISIS

El propósito de este capítulo es hacer un ejercicio de derecho comparado para comprender el marco normativo de EUA, cómo construyen el derecho a la privacidad y el derecho a la protección de datos, cómo han regulado los programas de vigilancia y analizar los aciertos y errores de su regulación a estos programas. Posteriormente, serán contrastados con el marco normativo mexicano donde serán analizadas las similitudes y diferencias entre estas dos regulaciones distintas. Serán analizados los aciertos del sistema jurídico mexicano y las áreas que puede fortalecer.

Como fue explicado en el capítulo anterior se ha escogido Estados Unidos por su amplia jurisprudencia del derecho a la privacidad y su interacción con las nuevas tecnologías de seguridad y espionaje. Las decisiones de la SCOTUS son un referente en cómo interactúan estos dos derechos con nuevas tecnologías de vigilancia.

3.5 Estados Unidos de América:

3.5.1 Marco Normativo:

El marco normativo por analizar estará compuesto por legislación que trata sobre vigilancia y herramientas que permiten intervenir las comunicaciones de una persona.

El concepto de privacidad para el contexto de EUA en este texto lo entendemos como lo entiende la Cuarta enmienda es "*the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*[92] Es decir, nos enfocamos particularmente en este derecho de privacidad a no ser molestado en

[92] "Fourth Amendment," Fourth Amendment, Cornell Law School, visitado el 15 de mayo de 2021, https://www.law.cornell.edu/constitution/fourth_amendment#:~:text=The%20right%20of%20the%20people,and%20the%20persons%20or%20things

nuestra esfera personal y protegernos contra cualquier arbitrariedad que no tenga una causa probable o algún fundamento en la ley.

Una nota importante de la concepción de privacidad en EUA privilegia a la seguridad nacional sobre otros criterios. EUA tiene una historia legislativa en la cual ha emitido normativa que limita derechos fundamentales para ofrecer mayor seguridad a los ciudadanos. Por ejemplo, el *Patriot Act* después del ataque a las torres gemelas. En el cual en aras de proteger la seguridad del país había que limitar ciertos derechos; en específico, la primera y cuarta enmienda.[93] Bajo la bandera de la seguridad nacional EUA ha emitido regulación que podría comprometer gravemente derechos de sus ciudadanos.

3.5.2 Freedom Act

Para comprender esta ley debe analizarse el contexto en el que fue creada y las razones que justificaron su creación. Creada como una respuesta a los escándalos de espionaje revelados por Edward Snowden, ex agente de la Central Intelligence Agency (CIA). En los que se reveló que la *National Security Agency* (NSA) espiaba no solamente a países extranjeros sino a toda la población estadounidense a través de la recolección masiva de metadatos.[94] Los metadatos son huellas digitales que pueden revelar aspectos sumamente íntimos de la vida de la persona. Ahora, el gobierno de EUA por medio de programas masivos de vigilancia había estado recolectando toda esta información de los ciudadanos.

Son *spywares* sumamente potentes que son capaces de almacenar la información de millones de personas y hacer un perfil de cada uno. Cada programa sirve para cuestiones diferentes, por ejemplo: PRISM funcionaba como un software que permitía recolectar información de sitios como *Facebook, Twitter, Google y Apple.*[95] PRISM puede recolectar el historial de búsquedas, contenido de correos electrónicos, archivos, *chats*, fotografías según

[93] "SURVEILLANCE UNDER THE USA/PATRIOT ACT," ACLU, visitado el 16 de marzo de 2021, https://www.aclu.org/other/surveillance-under-usapatriot-act.
[94] Reuters, "NSA surveillance exposed by Snowden was illegal, court rules seven years on," *The Guardian*, 3 de septiembre de 2020, https://www.theguardian.com/us-news/2020/sep/03/edward-snowden-nsa-surveillance-guardian-court-rules.
[95] Timothy B. Lee, "Here's everything we know about prism to date," *Washington Post*, 12 de junio de 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

presentaciones filtradas de la NSA.[96] *Dishfire* el cual es un software que permite analizar aproximadamente 200 millones de mensajes de texto al día. El programa extrae toda la información posible de estos mensajes con el objetivo de obtener los itinerarios de viaje, contactos, historial de transacciones y toda información útil para identificar a la persona.[97]

Otro programa es *Mystic* que permite la grabación y almacenamiento de llamadas no sólo domésticas sino internacionales.[98] Las posibilidades son enormes pues el programa podría estar grabando las conversaciones de mandatarios mexicanos sin que ellos lo supieran. La lista de programas que tiene en su posesión la NSA es enorme y con una capacidad de vigilancia igual a la retratada en 1984 de George Orwell.[99]

Ahora bien, estos programas tenían un fundamento legal puesto que operaban bajo el Patriot Act. El Uniting *and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* o *Patriot Act* como es coloquialmente conocido es una ley creada a raíz de los ataques de septiembre 11 en 2001.

La ley comprende una amplia gama de temas dentro de los cuales existen unas normas que tenían una caducidad. La razón de la caducidad era que en el momento parecían medidas justificadas, pero en el futuro podrían ser no tan necesarias. Esta caducidad fue postergada en dos ocasiones hasta el 31 de mayo de 2015.

Una de estas normas era la sección 215 que era conocida como la "*Business records provisión*" la cual le daba el poder al gobierno pedir a los negocios sus datos si sospechaban que alguien estaba involucrado en actos terroristas. Esta sección 215 es la que el gobierno usó para justificar la recolección de millones de datos de los usuarios. [100]

---

[96] "NSA Prism program slides," *The Guardian*, 1 de noviembre de 2013, https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[97] James Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," *The Guardian*, 16 de enero de 2014, https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

[98] Barton Geliman, " NSA surveillance program reaches 'into the past' to retrieve, replay phone calls," *Washington Post*, 18 de marzo de 2014, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

[99] Yolanda Quintana, "Todos los programas de espionaje de la NSA desvelados por Snowden," *elDiario.es*, 19 de marzo de 2014, https://www.eldiario.es/turing/vigilancia_y_privacidad/nsa-programas-vigilancia-desvelados-snowden_1_4974573.html.

[100] Dara Lind, "Everyone's heard of the Patriot Act. Here's what it actually does," *Vox*, 2 de junio de 2015, https://www.vox.com/2015/6/2/8701499/patriot-act-explain.

Otra sección que expiró fue la sección 206 conocida como "*roving wiretap*" permitía que el gobierno interviniera físicamente cualquier dispositivo que la persona usará solo con una autorización de la *Foreign Intelligence Surveillance Court (FISC).* Finalmente, la sección 207 conocida como "*lone wolf*" la cual le permite al gobierno vigilar a alguien si sospecha que está involucrado en actividad terrorista, aunque la persona no pertenezca a un grupo terrorista.[101]

Debido a que algunas disposiciones del *Patriot Act* estaban a punto de expirar y la polémica desatada por las filtraciones hechas por Edward Snowden se tomó la decisión de crear el *US Freedom Act of "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act."* La cual establece tres cambios esenciales con respecto al antiguo *Patriot Act.* 1) Prohibición a la recopilación masiva de datos por parte del Gobierno.[102] 2) Reforma y hace más transparente a *la Foreign Intelligence Surveillance Cour*t (FISC)[103] 3) Permite a compañías informar al público que entregaron a las autoridades de inteligencia sus datos.

La recopilación masiva de datos queda fuertemente limitada primero en la sección 103. *"PROHIBITION ON BULK COLLECTION OF TANGIBLE THINGS."* En la cual modifica el United States Code *"50 U.S. Code § 1861 - Access to certain business records for foreign intelligence and international terrorism investigations"* en el cual menciona que cada si se pretende recolectar información física la "*application*" que la autoridad tiene que someter al juez debe señalar un "*specific selection term*" es decir se tiene que especificar un individuo o una unidad no puede seleccionarse toda la información de una compañía.[104]

Esto limita enormemente la capacidad para una recolección masiva y general de datos. Reforzando esta visión de limitar la recolección masiva de datos queda también limitada en la sección 201 "*PROHIBITION ON BULK COLLECTION."* En esta nuevamente se introduce el concepto de "*specific selection term*" para limitar que pueda hacerse una recolección masiva de datos por medio de "*Pen register y trap and trace devices*".[105]

---

[101] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 18 USC 1 (2001).
[102] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 18 USC 1 (2001).
[103] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 18 USC 1 (2001).
[104] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 18 USC 1 (2001).
[105] Según el USC los *Pen Registers* son device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication

Asimismo, se establece que el fiscal general debe asegurarse que se usen la políticas y procedimientos que protejan la información obtenida por estos mecanismos, así como el manejo, colección, retención y uso de la información obtenida.

De igual manera, en la sección "*SEC. 301. LIMITS ON USE OF UNLAWFULLY OBTAINED INFORMATION"* establece que ninguna información obtenida que sea identificada por una Corte como deficiente podrá ser usada como evidencia en ninguna corte, órgano administrativo, autoridad y órgano legislativo; aunque, hay una excepción a esto y es que la autoridad puede subsanar las deficiencias de la información obtenida.

Finalmente, en el título V *National Security Letter Reform* se reforma dentro del USC la sección de *COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS*. En la que se establece que la orden para solicitar los datos tiene que ir especificada a una persona, teléfono o cuenta. Es decir, no puede ser a una multitud de dispositivos lo que limita la recolección masiva de datos.

Esta misma disposición se aplica para el *ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES* del derecho a la privacidad en el cual la orden para obtener los datos estará limitada a un cliente, cuenta o entidad. Las empresas o servicios de telecomunicaciones que van a proporcionar esta información reciben una orden que certifica que la falta de una prohibición expresa para difundir la información podría causar: i) un peligro a la seguridad nacional de Estados Unidos; ii) Podría perjudicar una investigación criminal, terrorista o de contrainteligencia; iii) Intervención en las relaciones diplomáticas y, iv) Poner en riesgo la vida o integridad de una persona. Aunque si no se certifica la orden entonces las empresas o servicios de telecomunicaciones pueden difundir la información (sobre que la autoridad les requirió los datos de una persona) a tres sujetos: i) Las personas con quien es necesario colaborar para cumplir con la orden; ii) Un abogado para obtener un consejo legal o asistencia y, iii) Otras personas que haya permitido el director del *Federal Bureau of Investigation* (FBI).[106]

---

is transmitted, provided, however, that such information shall not include the contents of any communication y los Trap and Trace devices son: a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

[106] Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act, 50 USC 1801(2015).

El *Freedom Act* contempla reformas a la FISC dentro de las cuales destacan la sección 401 "*APPOINTMENT OF AMICUS CURIAE*" en la cual señala que los jueces de las Cortes pueden designar hasta 5 personas/organizaciones como *amicus curiae* quienes tendrán el propósito de asistir a la Corte en la resolución de órdenes o para analizar casos que puedan requerir una interpretación significativa de la ley.

Toda persona u organización deberán ser personas con experiencia en temas de privacidad, comunicaciones, tecnología o cualquier área que pueda ser relevante para el tema. Los *amicus curiae* tendrán acceso a toda la información necesaria para dar su opinión, inclusive podría tener acceso a información clasificada siempre y cuando no comprometa la seguridad nacional. Dentro de las obligaciones que tienen estos *amicus curiae* son las siguientes: i) Proporcionar argumentos legales que protejan la privacidad y las libertades civiles; ii) Información respecto a la manera en la que fue obtenida la información; iii) Argumentos legales sobre algún otro tema importante para la resolución del caso.

Para hacer más transparente el trabajo de la FISC el director nacional de inteligencia y el fiscal general pueden pedir que se desclasifique una resolución, orden u opinión emitida por el F*oreign Intelligence Surveillance Court* of Foreign *Intelligence Surveillance Court of Review*.

Por supuesto, la limitante a esta facultad son documentos que podrían comprometer la seguridad nacional. Aunque tanto el director nacional de Inteligencia puede por medio del fiscal general liberar un resumen de los puntos más importantes, el contexto en el que se decidió y los criterios que se tomaron para tomar la decisión.[107]

3.5.3 Communications Assistance for Law Enforcement Act (CALEA)

La CALEA es una ley publicada en 1994 que tenía como objetivo asegurar que todas las empresas de telecomunicaciones tuvieran las capacidades tecnológicas para cumplir con las órdenes por parte de las autoridades en cuestión de intervención de comunicaciones.

[107] Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act, 50 USC 1801(2015).

Dentro de la sección 103 "*Assistance Capability Requirements*" El cual establece que todos las empresas de telecomunicaciones necesitan asegurarse que sus instalaciones, equipo y servicios que ofrecen al público puedan cumplir con tres cosas: i) Poder aislar y permitir que el Gobierno (previa autorización de la Corte) pueda interceptar una comunicación vía cable o electrónica dentro de la zona de servicio; ii) Permitir la identificación de la información de la comunicación intervenida; iii) Permitir que esta información sea compartida con las autoridades y, iv) Realizar las intervenciones de manera que los afectados no se den cuenta de esta acción y no se viole alguna otra comunicación.[108] Es importante aclarar que si bien se exige que tengan la tecnología y capacidades adecuadas para atender estos requerimientos, no se les exige ni se les prohíbe un diseño en específico.

Un punto importante es que el fiscal general determina el número de intervenciones simultáneas que puede hacer la autoridad. Entonces, si el fiscal general señala que son 50 intervenciones simultáneas la empresa de telecomunicaciones debe tener la capacidad para sostener ese número de intervenciones. Además, establece que la empresa de telecomunicaciones debe asegurarse que la intervención de comunicaciones sólo pueda ser activada por medio de una orden judicial u otra autorización legal.

Conjuntamente, sólo ciertas personas pueden cumplir con la orden judicial y siguiendo las regulaciones establecidas por la *Federal Communications Commission* (FCC). Para garantizar que exista un estándar de calidad y de uniformidad dentro de las tecnologías y equipamiento aquellos que producen estas herramientas tienen que seguir los lineamientos establecidos por el FBI. Inclusive se prevé que el fiscal general tenía la autoridad de pagar y ayudar a las empresas de telecomunicaciones con los costos que significaba tener este tipo de tecnologías. [109]

3.5.4 Electronic Communications Privacy Act (ECPA)

Es una legislación clave y esencial para comprender cómo funciona la intervención de comunicaciones en EUA y ha sido ampliamente reformada y modificada por el CALEA, el

[108] Communications Assistance for Law Enforcement Act, 47 USC 1001 (1994).
[109] Communications Assistance for Law Enforcement Act, 47 USC 1001 (1994).

Patriot Act y los *FISA Amendments Acts*. Analizaré la legislación que está contenida en el US Code que es la vigente de esta ley.

Para empezar, tiene que estar claro ciertas definiciones y cómo entienden en EUA la intervención de comunicaciones. Una intervención de comunicaciones según la legislación angloamericana es *"the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."*[110] Ahora bien por wired communication se refiere a:

"any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce."[111]

Las comunicaciones orales las entiende como: *"any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;"* [112]

Otro concepto clave es "*electronical, mechanical or other devic*e" que se entiende como "*any device or apparatus which can be used to intercept a wire, oral, or electronic communication"*. Finalmente, el concepto de lo que entienden por "electronic communication" que es *"any transfer of signs, signals, writing, images, sounds, data, or intelligence of any*

[110] En la sección 18 *U.S. Code § 3127 - Definitions for chapter* establece cuál es la definición para los "*devices*" que pueden ayudar a la intervención de comunicaciones. Primero, el "pen register" la ley lo entiende como "*a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;"* Posteriormente, el concepto de "*trap and trace device*" que la ley lo entiende como "*device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication*;"
En la sección "*18 U.S. Code § 3117 - Mobile tracking devices*" establece la definición de otro dispositivo capaz de seguir el rastro de un teléfono móvil "*an electronic or mechanical device which permits the tracking of the movement of a person or object*."
[111] Definitions for chapter, 18 U.S.C § 3127.
[112] Definitions for chapter, 18 U.S.C § 3127.

nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[113]

Un punto interesante es que el USC prohíbe la venta, manufactura, promoción o posesión de cualquier dispositivo electrónico o mecánico que pueda usarse para intervenir en comunicaciones de manera ilegal. La persona que cometa alguna de estas acciones será acreedora a una multa y a años de prisión.

La venta de este tipo de tecnología solo está regulada de manera que solo puedan vender los que están autorizados y solo puedan adquirir este tipo de productos aquellos que están autorizados.[114] Existe una prohibición para usar la información obtenida de una manera indebida y sin seguir los lineamientos establecidos en la legislación. Esta información no puede usarse en ninguna audiencia, juicio, procedimiento jurisdiccional, administrativo o legislativo.[115]

Respecto a las personas autorizadas para solicitar a una autoridad jurisdiccional la intervención de comunicaciones; el USC establece en el apartado 2516 que las autoridades serán las siguientes: *The Attorney General, Deputy Attorney General, Associate Attorney General or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General* y todas ellas requerirán la autorización de un juez federal. Ahora bien, la intervención de comunicaciones se prevé para una amplia variedad de delitos y ofensas que están contempladas dentro de la sección 2516.[116]

Cada autorización para la intervención de comunicaciones debe contar con lo siguiente según la sección 2518 del *U.S. Code Procedure for interception of wire, oral, or electronic communications*: i) La identidad de la autoridad que está solicitando la intervención y la autoridad que autoriza esa solicitud; ii) Los hechos y circunstancias por las que justifican la intervención deben incluir: a) detalles del delito que está cometiendo o podrá cometer; b) una Authorization for interception de la naturaleza y localización del lugar de donde serán

[113] Definitions for chapter, 18 U.S.C § 3127.
[114] Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited, 18 U.S.C § 2512.
[115] Prohibition of use as evidence of intercepted wire or oral communications, 18 U.S.C § 2515.
[116] Prohibition of use as evidence of intercepted wire or oral communications, 18 U.S.C § 2515.

intervenidas las comunicaciones;[117] c) la descripción del tipo de comunicación que serán intervenidas y, d) la identificación de la persona (si conocen al sujeto) que va a cometer o cometió la ofensa o de quien sus comunicaciones vayan a ser intervenidas. iii) una justificación del por qué otras medidas de investigación fallaron o no fueron usadas antes de solicitar la intervención de comunicaciones; iv) Establecer el periodo de tiempo que va a durar la intervención y si requiere que siga siendo intervenidas las comunicaciones por riesgo a que vuelvan a ocurrir los hechos que dieron pie a la solicitud; v) Una lista de todas las veces que el solicitante ha pedido a una autoridad jurisdiccional la intervención de comunicaciones así como los hechos y circunstancias alrededor del caso y la resolución del juez y vi) Si se solicita la extensión de una autorización previa de intervención de comunicaciones los resultados obtenidos a partir de la autorización previa o una explicación de la falta de resultados.[118]

El juez tendrá que autorizar la solicitud tomando en cuenta los siguientes puntos: a) Existencia evidencia suficiente y hay una causa probable de que el individuo vaya a cometer ilícitos o los haya cometido; b) Hay una causa probable de que la intervención de comunicaciones pueda revelar información de los ilícitos cometidos; c) Ya se han intentado otras medidas de investigación pero no tuvieron éxito o eran demasiado riesgosas y, d) Hay una causa probable de que las comunicaciones intervenidas son usadas para comunicarse para la comisión del delito o vayan a ser usadas para la comisión del delito.

Cada orden autorizada por el juez debe contener: a) la identidad de la persona (si se conoce) de quién será intervenidas sus comunicaciones; b) la naturaleza y la ubicación de los

[117] Authorization for interception of wire, oral, or electronic communications, U.S.C § 2516.
Existen varias limitantes a este requisito en la sección 11(a) y 11(b): (a)in the case of an application with respect to the interception of an oral communication—
(i)the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General; (ii)the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and (iii)the judge finds that such specification is not practical; and (b)in the case of an application with respect to a wire or electronic communication— (i)the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General; (ii)the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility; (iii)the judge finds that such showing has been adequately made; and (iv)the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.
[118] Procedure for interception of wire, oral, or electronic communications, 18 U.S.C § 2518.

medios de comunicación a los que se concede la autorización para interceptar, o el lugar en que se concede dicha autorización; c) La descripción de la comunicación que será intervenida y del delito que está relacionado con la medida; d) La identidad de la agencia que está permitida para intervenir comunicaciones así como de la persona autorizando la orden y, e) El periodo de tiempo el cual será autorizada la medida y si la medida debe terminar en cuanto se logre la intervención o debe continuar. [119]

Asimismo, el U.S Code en la sección 2518 menciona que toda orden debe autorizar la intervención de comunicaciones no puede durar más del tiempo establecido para la realización del objetivo con un máximo de 30 días.

Se puede extender el periodo de tiempo por otros 30 días. La prórroga puede extenderse siempre y cuando el juez lo autorice y debe ser siempre para cumplir con los objetivos. El juez tiene la facultad de solicitar que se le de un reporte en la periodicidad que él señale sobre los avances de las investigaciones.

La sección 2518 del U.S. Code establece que los casos en los que puede ser intervenida las comunicaciones antes que el juez apruebe la orden son en los siguientes supuestos: a) Primero tiene que haber una situación de emergencia que involucre: i) Un riesgo inminente de peligro de muerte o una herida física seria a cualquier persona: ii) actividades de conspiración que puedan poner en peligro la seguridad nacional y, iii) actividades de conspiración que sean características de las organizadas por el crimen organizado.[120]

Todas estas situaciones deben ameritar que no se pida una orden judicial antes sin la diligencia debida. Si se realiza la intervención sin orden judicial debe terminar cuando se haya obtenido la información buscada o cuando la orden sea rechazada por el juez. En el caso de no obtener la autorización judicial toda información que haya sido interceptada será tratada como si se hubiera obtenido en contra de las disposiciones de la ley.

Asimismo, la sección 2518 del U.S Code señala que la información obtenida tiene que ser resguardada protegiendo la privacidad del sujeto y además se le tienen que hacer llegar al juez. El juez las conservará por diez años en caso de no existir una orden judicial que le pida eliminarlas o que se hubieran obtenido de manera contraria a la ley. En caso de que el juez haya denegado la orden o que haya expirado la orden judicial, el juez hará un registro sobre: i) los

[119] Procedure for interception of wire, oral, or electronic communications, 18 U.S.C § 2518.
[120] Procedure for interception of wire, oral, or electronic communications, 18 U.S.C § 2518.

hechos que dieron pie a la petición; ii) la fecha en que fue aprobada o desaprobada la orden judicial. iii) Si se concretó o no una intervención de comunicaciones. El juez podría informarle a la persona que se pretendía o se concretó la intervención este registro que realizó.

Otra disposición establecida en la sección 2518 del U.S Code es que cualquier persona agravada por la intercepción puede en cualquier juicio, audiencia o procedimiento ante alguna corte, departamento, oficial, agencia, organismo u autoridad en Estados Unidos puede intentar limitar o promover que la intercepción sea considerada contraria a la legislación bajo las siguientes razones: i) La comunicación fue intervenida de manera ilegal; ii) La orden de autorización o aprobación bajo la cual se realizó la intervención de comunicaciones es insuficiente y; iii) La intervención no acató la orden judicial del juez. Asimismo, el gobierno de EUA puede apelar la demanda que ratifique la limitación, haya sido declarada ilegal o haya sido rechazada para lo cual tienen 30 días para interponerla.[121]

Finalmente, la ley prevé en *18 U.S. Code § 2517 - Authorization for disclosure and use of intercepted wire, oral, or electronic communications* que cualquier autoridad investigadora o policía puede compartir los contenidos de la intervención contra autoridad o policía solo si esa información le será útil a quien reciba la información compartida. La información según la ley debe ser usada hasta el punto donde sea apropiada para el desempeño de sus funciones.

3.5.5 The Privacy Act

En materia de protección de datos personales EUA no tiene una legislación federal como tal. Tiene diversa legislación en materia de datos personales como *el Gramm - Leach - Bliley Act* (GLBA) que protege la información financiera. El *Health Insurance Portability and Accountability Act* (HIPAA) para proteger la información de los datos de salud y seguro de vida de los usuarios. El *Children 's Online Privacy Protection Act* (COPPA) para proteger los datos personales de los menores de 12 años. El *Federal Trade Commission Act* que dentro de su jurisdicción protege los datos personales que manejan las entidades comerciales. En este caso nos enfocaremos en el *Privacy Act* creado en 1974 que regula principalmente los derechos y restricciones en los datos que las agencias gubernamentales sobre los ciudadanos.

[121] Procedure for interception of wire, oral, or electronic communications, 18 U.S.C § 2518.

Dicha ley fue creada como respuesta a las bases de datos creadas por el gobierno sobre los datos de los ciudadanos y cómo estas bases podrían impactar en su privacidad. Un punto clave de esta legislación es que solamente aplica para las agencias gubernamentales federales.

La única excepción a esto es el número de seguridad social que puede aplicar para gobiernos federales, estatales y locales. Cada Estado tiene sus propias leyes especiales para proteger los datos personales de los usuarios tanto en materia de comercio como en materia de datos que tiene el gobierno en su poder. En este caso *el Privacy Act* aplica para los departamentos que dependen del ejecutivo, los militares, las agencias independientes regulatorias y las corporaciones administradas por el gobierno. Por ejemplo, agencias como el FBI se encuentran reguladas dentro de esta legislación. Dentro de la legislación puede verse que para EUA entienden que la protección de datos personales está comprendida dentro del derecho de "*right to privacy*".

Tal como lo expone en *el Statement of Purpose* "the *right to privacy is a personal and fundamental right protected by the Constitution of the United States. in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use and dissemination of information by such agencies.*"[122]

Uno de los puntos centrales de la legislación son los *Public Notice Requirements* los cuales tienen el objetivo de prevenir que el gobierno pueda almacenar de manera secreta los datos personales de los ciudadanos. Para esto cada entidad gubernamental debe publicar los detalles de sus sistemas de registros en un registro federal. Cada entrada en este registro debe mencionar los usos que le va a dar a la información; además, cada cambio significativo a los usos que se le dará a la información tiene que notificar a un Comité legislativo llamado "*Committee on Government Operation*s".

Toda esta información está contenida en el U.S Code § 552a - Records maintained on individuals. El contenido normativo del Privacy Act está contenido en este código. El cual menciona que cada individuo tiene acceso a los registros que tiene o pudiera tener la entidad sobre él. La persona puede revisar los datos, obtener copias cobre ellos y además si se encuentran incompletos o tienen algún error puede pedir que sean enmendados.[123] Existe todo

[122] Privacy Act of 1974, 5 U.S.C. § 552a (1974).
[123] Privacy Act of 1974, 5 U.S.C. § 552a (1974).

un proceso litigioso para esta petición en el cual la autoridad puede negar la petición de alterar los registros y la persona el derecho de apelar la decisión. Primero se puede litigar por la vía administrativa y en caso de insatisfacción de la persona puede llevarlo a la vía jurisdiccional.

Asimismo, en la sección 552a – Records maintained on individuals subsección (b) existen reglas específicas para la divulgación de la información por parte de las agencias gubernamentales. La entidad solo puede compartir esta información si cuenta con permiso del individuo o si puede cumplir una de las doce posibles condiciones enmarcadas en la subsección (b) "*Conditions of Disclosure*".[124] Asimismo, debe guardar un registro de todas las veces que ha compartido los datos personales de la persona con otras agencias por un periodo de cinco años o de por vida. Un punto importante es que, si la información se compartió para temas de seguridad o para la investigación de un delito, la persona no puede pedir si sus registros han sido compartidos.

En la sección 552a – Records *maintained on individuals*, subsección (e) *Agency Requirements* hace especial énfasis en la aplicación del principio de minimización de datos por lo que la agencia sólo podrá almacenar la información que sea relevante y necesaria para su propósito. Cada vez que recopila información la autoridad tiene que informarle al ciudadano tres cosas: 1) que ley u orden le permite recopilar la información; 2) los usos que pudieran darle a esa información y 3) las consecuencias de no dar la información pedida. [125]

Hay una fuerte regulación a los "*matching programs*" que según la definición establecida por la sección 552a, apartado (a) definitions son programas por computadora que comparan las bases de datos para identificar datos claves de individuos dentro del sistema de registros.[126] Este tipo de programas puede usarse para compartir información entre agencias gubernamentales. En general la legislación prohíbe este tipo de programas; sin embargo, las agencias pueden obtener un permiso para utilizar este tipo de programas según la sección 552a, apartado (r) *Report on New Systems and Matching Program*.[127]

Ambas agencias que compartirán información tienen que asegurarse que la receptora o la mensajera de la información cumplen con la regulación necesaria. Cada agencia que utilice este tipo de programas deberá tener un "*Data Integrity Board*" que se encargue de vigilar que

[124] Privacy Act of 1974, 5 U.S.C. § 552a (1974).
[125] Records maintained on individuals – (b) Conditions of disclosure, 5 U.S.C. § 552a.
[126] Records maintained on individuals – (b) Conditions of disclosure, 5 U.S.C. § 552a.
[127] Records maintained on individuals – (r) Report on New Systems and Matching Programs, 5 U.S.C. § 552a.

la agencia está cumpliendo con el *Privacy Act* y la demás legislación aplicable pues así lo establece la sección (u) *Data Integrity Boards* de la sección 552a. Las excepciones para la persecución de delitos y seguridad son bastante amplias por razones como que es contraproducente que los posibles criminales puedan acceder a la información que tiene la autoridad en su poder.[128]

Una de las disposiciones más criticadas del *Privacy Act* es que dentro de las condiciones en las que una autoridad puede revelar información de la persona a otras agencias hay una condición llamada "*routine use*" la cual según la "subsección (a) (7) significa "*the use of such record for a purpose which is compatible with the purpose for which it was collected*."[129] La cual es una categoría sumamente amplia que no ofrece una definición delimitada sobre lo que podría ser "*routine use*" y podría dar pie a arbitrariedades por parte de la autoridad.

3.6 Análisis y comparación del marco jurídico estadounidense contra el marco jurídico mexicano

3.6.1 Introducción

Ahora, es momento de realizar un análisis de la legislación estadounidense y contrastar con el marco jurídico mexicano. El marco normativo angloamericano está compuesto por una legislación enfocada en la protección a la seguridad nacional para salvaguardar la seguridad de sus ciudadanos.

Una de las acciones más cuestionables sobre las medidas implementadas por el gobierno estadounidense son los programas descubiertos por las filtraciones hechas por Edward Snowden. Los programas que ellos tienen se podrían asemejar a una fábrica donde con insumos de los ciudadanos están creando perfiles sumamente precisos sobre su identidad.

Hay que hacer una diferencia fundamental entre lo que pasa en el caso mexicano vs el caso estadounidense. En el caso de México apenas fue revelado que existen programas de vigilancia masiva comprados por el gobierno. Es importante esta diferencia pues cuando

[128] Records maintained on individuals – (u) Data Integrity Boards, 5 U.S.C. § 552a.
[129] Records maintained on individuals – (a) definitions, 5 U.S.C. § 552a.

hablamos de programas de vigilancia masiva son distintos a los programas de vigilancia como Pegasus.

Los programas que Estados Unidos tiene en su poder es realizar lo que Pegasus realiza, pero de manera continua y de manera ininterrumpida. Sería como tener un radar que de manera constante y repetida no deja de vigilar. Un ojo que todo lo ve. Parte de la lucha y de lo que se pretende en la lucha de la sociedad civil estadounidense es regular estrictamente a estos programas de vigilancia masiva o ponerle fin.[130]

Bajo la sección 702 EUA ha pretendido hacer constitucional la recopilación masiva de datos de estadounidenses y extranjeros. Puesto que la sección 702 se pretendía que se usará contra extranjeros puesto que estaba dentro del *Foreign Intelligence Surveillance Act* (FISA). El gobierno de EUA ha defendido que esto se usa para extranjeros y para comunicaciones de extranjeros a estadounidenses.

La realidad es que se ha usado contra la población estadounidense y gobiernos extranjeros. Inclusive el Estado mexicano según datos revelados por Snowden y publicados por el *diario Spiegel* ha sido víctima de estos ataques. En 2013 fue revelado que la NSA había obtenido acceso ilegal al correo electrónico del expresidente Calderón.[131]

En cambio, en México existe evidencia que el gobierno mexicano ha contratado programas de vigilancia y recolección masiva de datos tal como lo reveló la investigación del diario El País.[132] Además, tenemos en posesión herramientas de vigilancia como Pegasus que podrían replicar alguna de las funciones de los programas que tiene en su uso la NSA. En EUA han estado regulando algunas de las funciones por medio de casos clave como he expuesto anteriormente en el segundo capítulo, pero ¿En México cuál sería la solución?

---

[130] Patrick Toomey, "The NSA Continues to Violate Americans' Internet Privacy Rights," *ACLU*, 22 de agosto de 2018, https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

[131] Von Jens Glüsing, Laura Poitras, Marcel Rosenbach y Holger Stark, "NSA Accessed Mexican President 's Email," *Spiegel International*, 20 de octubre de 2013, https://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

[132] Zorayda Gallegos, "La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles," *El País*, 14 de abril de 2021, https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html.

3.6.2 Freedom Act vs Marco normativo mexicano

Una de las piezas claves de EUA es el *Freedom Act* que prohíbe en el papel la recopilación masiva de datos en materia de seguridad. En México no hay una prohibición expresa por parte de alguna legislación en materia de protección de datos que prohíba la recolección masiva de datos para seguridad. El tratamiento de datos personales debe obedecer a una causa legítima y este derecho según el artículo 6 de la LGPDPSO sólo puede ser limitado por razones de seguridad nacional, en términos de la ley de la materia, disposiciones de orden público, seguridad y salud pública o proteger derechos de terceros. El ejemplo más reciente en México a la fecha es la recolección masiva de datos de localización geográfica por parte de las instituciones financieras. [133]

En materia de seguridad cuando una autoridad pide una intervención de datos el CNPP señala en su artículo 293 que la autoridad debe indicar la persona o personas, pero no establece ningún límite respecto si pudiera pedir la intervención de 100 personas. Conforme la tecnología avance podría México adquirir este tipo de programas de vigilancia masiva que pudieran intervenir las comunicaciones de un amplio número de personas.

En EUA por lo menos en materia de seguridad limitaron que la autoridad pudiera pedir los datos de un amplio número de personas bajo el concepto de "specific selection term" en el cual establece que cuando una autoridad exige a la empresa o a la autoridad judicial tiene que especificar a individuos identificables y no una caer en una generalidad.

La diferencia sustancial entre ambos marcos normativos es definitivamente que en México existen leyes especiales para la protección de datos personales, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Son dos leyes que establecen las pautas generales bajo las cuales la autoridad tiene que realizar el tratamiento de datos personales y cómo interactúan las labores de seguridad en la protección de datos personales; al igual México forma parte del Convenio 108 y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos.[134]

---

[133] R3D, "Recolección De Datos De Geolocalización En Banca En Línea Es Desproporcionada, Riesgosa E Innecesaria," *R3D*, 23 de marzo de 2021, https://r3d.mx/2021/03/23/recoleccion-de-datos-de-geolocalizacion-en-banca-en-linea-es-desproporcionada-riesgosa-e-innecesaria/.

[134] DECRETO por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre

La LGPDPPSO en su artículo 6 establece que el derecho a la protección de datos personales sólo podrá limitarse por razones de seguridad nacional, en los términos de la ley en la materia disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. En el *Freedom Act* se prevé que la información que sea obtenida de manera ilegal no pueda ser utilizada en ningún tipo de procedimiento o juicio ante alguna autoridad. Si bien, en el CNPP no se establece esta prohibición de manera expresa que la información obtenida de manera ilegal no puede ser utilizada de manera ilegal.

Si establece en su artículo 300 que la información deberá ser destruida si no se relaciona con los delitos investigados, cuando no se haya dado la autorización y cuando esta información rebase los términos de la autorización judicial respectiva. Uno de los puntos clave del *Freedom Act* es que contempla que la FISC pueda colaborar con personas de la sociedad civil o académicos para la resolución de casos. En la utilización de programas como Pegasus debería de usarse en casos límite y en casos donde el juez amerite que es necesaria la utilización de un programa de esta naturaleza. El uso de estos programas debería ser el último recurso por su capacidad para intervenir en la esfera de la privacidad y la protección de datos personales.

Es en esta tesitura que podría considerarse que el juez en la resolución de la orden judicial pueda solicitar un *amicus curiae* de la sociedad civil, academia y personas con algún interés en la decisión. No obstante, resulta complicado debido a la urgencia y eficacia de la decisión que debe tomarse en el momento.

En México no tenemos previsto este tipo de mecanismos de *amicus* curiae para apoyar en la toma de decisiones del juez en caso de intercepción de comunicaciones. Es una herramienta compleja que requeriría una apresurada respuesta por parte de la sociedad civil. ningún tipo de colaboración con sociedad civil ni que la autoridad pueda solicitar opiniones diversas para la resolución de casos.

Se reconoce que por la necesidad de urgencia es complicado que la autoridad solicite este tipo de opiniones; sin embargo, creo que para investigaciones donde hay un trabajo una averiguación previa y que se solicita la intervención de comunicaciones como parte de las actividades de investigación podría ser relevante la intervención de la sociedad civil.

---

de 2001, respectivamente." Diario Oficial de la Federación [DOF] 12-06-2018 (Mex.), formato HTML, https://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018.

En el Freedom Act se prevé que el fiscal general o el director nacional de inteligencia pueda desclasificar una decisión u opinión emitida por la FISC. Si bien en México las resoluciones del poder judicial son en su mayoría abiertas al público tener transparencia sobre los criterios que se toman en cuenta, la fundamentación y motivación de las órdenes judiciales es necesario.[135] Es importante saber cómo entienden los jueces los derechos de privacidad y derecho a la protección de datos para que podamos hacer un ejercicio de construcción entre jueces con sociedad civil y academia.

3.6.3 Electronic Communications Privacy Act v Código Nacional de Procedimientos Penales (CNPP)

El ECPA sería su equivalente a nuestra intervención de comunicaciones prevista en el CNPP; sin embargo, tiene diferencias que son relevantes si se contrastan con el marco normativo mexicano.

En el marco estadounidense se definen cuatro conceptos: 1) intervención de comunicaciones; 2) comunicaciones por cable; 3) comunicaciones orales y, 4) comunicaciones electrónicas. En el USC establece que la intervención de comunicaciones se entenderá como: *"the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."* La podemos descomponer en tres partes la primera parte "*the aural or other acquisition of the contents*" la cual señala que puede ser comunicación que escuchen o que recaben. Posteriormente, señala los medios por los cuales se puede obtener esta información "*wire, electronic or oral communication*" que los podríamos clasificar en tres.[136]

Finalmente, menciona "*through the use of any electronic, mechanical or other device*" lo que quiere decir los medios por los cuales puede obtener la información. Si el gobierno de

[135] ACUERDO del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas." Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Diario Oficial de la Federación [DOF]15-04-2016 (Mex.).

[136] La definición de estos conceptos ya fue descrita en la sección anterior.

EUA utilizara software como Pegasus probablemente lo fundamentaría en esta última sección bajo el concepto de "*electronic*".

Por otro lado, el marco normativo solo aporta la siguiente definición para la intervención de comunicaciones:

"La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real."[137]

La definición establece lo siguiente "abarca todo sistema de comunicación o programas que sean resultado de la evolución tecnológica." Es una definición amplia que permite qué tipo de programas o sistemas pueden ser intervenidos, al tener un amplio rango la definición podría considerarse que se pretendía que no solamente se abarcara sistemas de comunicación comunes como la comunicación oral o por teléfono si no que el legislador pretendió hacerlo más amplio para lograr que las nuevas aplicaciones/plataformas puedan ser intervenidas.

Este tipo de redacción solo otorga más preguntas que respuestas ¿Podría considerar que la aplicación de *Facebook* es un programa? Entonces ¿la autoridad podría declarar que se otorgue una autorización para entrar a mi cuenta de *Facebook*? Son incógnitas que debieran ser analizadas y resueltas por parte del legislador.

Ahora bien, la segunda parte de la definición es la siguiente: "informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real." La definición es sumamente amplia para que la autoridad no tenga excusa en obtener diferentes tipos de datos tales como video, audio, mensaje o metadatos.

Un punto importante que podemos observar en ambas legislaciones es que si bien en la legislación de EUA se establece el término "devices" los cuales pueden ser utilizados. No es claro si un *spyware* como Pegasus podría considerarse un "*device*" que ayude a la intervención de comunicaciones. Un gran acierto de la legislación estadounidense es que prohíbe la venta y comercialización de programas ilegales que puedan intervenir en comunicaciones privadas.

[137] Código Nacional de Procedimientos Penales, CNPP, art. 291, Diario Oficial de la Federación [DOF] 5-04-2014, últimas reformas DOF 19-02-2021(Mex.).

Conforme avanza la tecnología y las capacidades de los internautas no sería difícil que existieran copias ilegales de programas como Pegasus circulando en la red. Todo ese tipo de comercio tiene que ser detenido y regulado puesto que no abogo por una prohibición expresa del uso de estos programas, pero sí ayudaría tener un patrón y registro de ¿Quién lo vende? ¿A quién lo vende? ¿Por cuánto tiempo? ¿En qué dispositivos fue instalado el programa? Todo esto profundizaré más en la siguiente sección de la solución. México no tiene ninguna definición acerca de los dispositivos usados para lograr una intervención de comunicación.

Pegasus puede ir más allá de la definición de intervención de comunicación pues no solamente se enfoca en las comunicaciones si no en los archivos o datos que el usuario guarda que no necesariamente tiene que ver con una comunicación. Es necesaria la definición de las herramientas que pueden ser usadas para estos fines. En el marco normativo estadounidense se establece una prohibición clara y tajante sobre que la información obtenida de manera ilegal o bajo algún procedimiento que no involucre una autorización no puede ser utilizada en ninguna circunstancia en ningún proceso judicial o administrativo.

Si bien en México toda prueba o información usada en contra de un individuo que haya sido obtenida de manera ilegal no tiene valor probatorio e incluso la tesis que analicé en el primer capítulo señala esta prohibición creo que no estaría de más que esta prohibición fuera ley y no una tesis aislada.

Ahora en EUA las autoridades que pueden pedir una intervención de comunicaciones están bien delimitadas y señaladas dentro de la ley. En cambio, en el marco normativo mexicano como analicé en el primer capítulo no hay absoluta certeza de quiénes pueden solicitar esta intervención de comunicaciones. La SCJN en el Amparo en Revisión 904/2015 tuvo que intervenir para dar luz al artículo 16 constitucional que establecía “Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.”

Las autoridades facultadas por la ley eran el Procurador General de la República, así como los procuradores de las entidades federativas, la ahora extinta policía federal y, la autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional (CISEN). Ahora bien, todos estos sujetos ya no existen, pero heredaron las facultades que tenían sus predecesores como las señala el capítulo primero.

Otra diferencia sustancial es que la legislación estadounidense establece el tipo de delitos y las circunstancias bajo las cuáles una intervención de comunicaciones está justificada. Si bien la crítica a este sistema es que su lista de delitos y circunstancias es inmensa en la que prácticamente está permitido para la gran mayoría de los delitos. El hecho de que esté listado en una ley podría ser un paso adelante para evitar la arbitrariedad en la intervención de comunicaciones. En México no existe ninguna lista de delitos o circunstancias que ameriten el uso de estas tecnologías.

Podría ser necesario que exista claridad en qué tipo de delitos y circunstancias puede ser usado este tipo de herramientas y sobre todo me parece indispensable cuando se trate de usar programas como Pegasus. Esto ofrece certeza a los ciudadanos para saber en qué momento puede autorizarse una intervención de comunicaciones y en qué momento podrían ser vigilados bajo programas de vigilancia como Pegasus.

Posteriormente, el proceso para solicitar una intervención de comunicaciones en el marco normativo estadounidense es bastante similar, pero hay diferencias importantes. Dentro de la solicitud que la autoridad hace al juez se encuentran dos puntos que tiene que acreditar la autoridad: i) una justificación del por qué otras medidas de investigación fallaron o no fueron usadas antes de solicitar la intervención de comunicaciones y ii) Una lista de todas las veces que el solicitante ha pedido a una autoridad jurisdiccional la intervención de comunicaciones así como los hechos y circunstancias alrededor del caso y la resolución del juez según la sección 2518 del U.S Code *Procedure for interception of wire, oral, or electronic communications.*

Estos dos puntos son importantes y en la legislación mexicana no se encuentran presentes. La autoridad no requiere legalmente mencionar expresamente las razones por las que otras medidas de investigación fallaron o no fueron idóneas para la realización de la investigación.

Sería importante que explique la autoridad mexicana la razón por la que necesita intervenir comunicaciones y posteriormente la razón por la que cree que Pegasus es la herramienta idónea. Pegasus o cualquier otro programa de vigilancia debe ser la herramienta más poderosa y de última instancia. Si la intervención de comunicaciones es una tijera, el uso de spyware como Pegasus es una motosierra. Ninguna es ilegal pero su uso siempre tiene que estar justificado.

Asimismo, es importante que haya un registro de todas las veces que un solicitante pide a la autoridad la intervención de comunicaciones, los hechos y circunstancias del caso, así como la resolución del juez. Esto le brinda aún más certeza al juez pues la autoridad que pide la intervención ha hecho un buen uso de este tipo de herramientas y el contexto en que las ha pedido. Esto permite distinguir si la persona ha hecho un buen uso de este tipo de herramientas y si ha sido consistente con las motivaciones detrás de su uso.

En México la legislación no le pide al juez que valore una serie de hechos como sí sucede en la legislación estadounidense. En México solo está la obligación de que el juez vea que esté fundada y motivada la solicitud. En Estados Unidos el juez tiene que valorar cuatro puntos como lo describí en la anterior sección: a) Existencia evidencia suficiente y hay una causa probable de que el individuo vaya a cometer ilícitos o los haya cometido; b) Hay una causa probable de que la intervención de comunicaciones pueda revelar información de los ilícitos cometidos; c) Ya se han intentado otras medidas de investigación pero no tuvieron éxito o eran demasiado riesgosas y, d) Hay una causa probable de que las comunicaciones intervenidas son usadas para comunicarse para la comisión del delito o vayan a ser usadas para la comisión del delito.

Se puede observar una característica importante de cómo influye su construcción sobre la Cuarta Enmienda y el concepto que explicamos anteriormente sobre “probable cause”. En la legislación estadounidense es notorio que para que el juez pueda aceptar que una injerencia a este derecho debe cumplirse ciertas condiciones. En cambio, en la ley mexicana el juez no tiene que cumplir por ley ciertos requisitos; sin embargo, el test de proporcionalidad debe hacerse y se espera que el juez sea en este punto el que valore si las circunstancias ameritan la intervención.

Si bien cada juez debe resolver conforme a su criterio y la ley, sería recomendable establecer pautas claras sobre lo que el juez debe superar en esta materia podría ayudar a que la intervención de comunicaciones sea cuando sea necesario. Sobre todo, con la nueva afluencia de tecnologías mucho más capaces en la materia de vigilancia los jueces deberían de tener conocimiento de ellas y la manera en que pueden permear en el derecho de privacidad de la persona.

Ahora bien, el contenido de la orden judicial en el marco normativo de EUA es prácticamente el mismo que con el contenido que se prevé en el artículo en el 293 del CNPP.

Aunque hay una diferencia sutil pero importante entre el marco normativo estadounidense y el mexicano. En el marco angloamericano señala en el primer requisito que *"(a) the identity of the person, if known, whose communications are to be intercepted;*" Se reconoce que no se intercepta un número o que el objeto de la intervención son aparatos tecnológicos como un teléfono, un número celular, sino que es la persona y sus comunicaciones.

La persona va al centro de la intervención. Es sutil pero poderoso puesto que esto ha ido construyéndose a través de las sentencias previamente analizadas. Los datos que puede revelar los metadatos o los archivos intervenidos en una intervención de comunicaciones son absolutamente reveladores y no se puede separar a que el afectado es el celular.

La Corte en las decisiones previamente analizadas no deja claro si efectivamente las intromisiones a la esfera de privacidad de la persona afectan al móvil intervenido o a la persona dueña de este. Asimismo, la legislación mexicana tampoco ofrece una claridad absoluta sobre quién está al centro de la intervención.[138] La jurisprudencia de la SCJN ha sido cuestionable puesto que hay un conflicto entre lo establecido por la Corte sobre que la localización por GPS no ameritaba una autorización judicial por dirigirse al móvil y lo establecido en el CNPP que si pide autorización judicial.

Si bien en el artículo 303 sobre el CNPP referente a la "Localización geográfica en tiempo real y solicitud de entrega de datos conservados" menciona que se requiere una autorización judicial. Aunque nunca se hace mención que los números telefónicos pertenezcan a una persona y por lo tanto su derecho a la privacidad pueda ser afectado. La persona y su privacidad queda en un segundo plano, cuando debería ser el primer plano.

Respecto de la duración de la intervención es bastante amplia la duración de la intervención establecida en el CNPP puesto que señala en el artículo 292 que la intervención junto con sus prórrogas no podrá exceder de seis meses. En cambio, en el marco estadounidense

[138] Artículo 293. Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas. En la autorización, el Juez de control determinará las características de la intervención, sus modalidades, límites y en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración.
Artículo 294. Objeto de la intervención. Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.
En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su
Defensor. El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

establece que la intervención inicia por 30 días para posteriormente ir prorrogando por menos de 30 días hasta que se cumplan los objetivos. Ambas legislaciones, a mi juicio, ofrecen un amplio margen discrecional respecto a las prórrogas, si bien en el caso mexicano si se establece un límite definitivo en seis meses, puede ampliarse si se llegaran a encontrar nuevos elementos que lo justifiquen.

Posteriormente, el marco normativo estadounidense establece ciertas excepciones en las que la intervención de comunicaciones se realizará y posteriormente se pedirá la autorización del juez. En cambio, en el marco normativo mexicano CNPP no se prevén excepciones para la intercepción de comunicaciones sólo para la localización geográfica por GPS y la conservación de datos. Los cuales son bastante similares en el marco estadounidense establecen cuatro requisitos: 1) Existencia de una situación de emergencia; 2) Un riesgo inminente de peligro de muerte o una herida grave; 3) actividades de conspiración que pongan en riesgo la seguridad nacional y, 4) actividades de conspiración que sean características de las organizadas por el crimen organizado.

En la legislación mexicana sólo está previsto en el caso de la localización geográfica y la conservación de datos en el cual señala diversas situaciones: 1) cuando esté en peligro la integridad física o la vida de una persona; 2) se encuentre en riesgo el objeto del delito; 3) en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada.

Otra disposición del marco normativo de EUA es establecer que las autorizaciones judiciales que sean denegadas o que hayan expirado tengan un registro donde se señale la siguiente información: i) los hechos que le dieron pie a la petición; ii) la fecha en que fue aprobada o desaprobada la orden judicial. iii) Si se concretó o no una intervención de comunicaciones.

Finalmente, el marco normativo estadounidense establece causales por las cuales una persona podría impugnar esta intervención de comunicaciones (si conociera del hecho). En el caso mexicano no hay en ninguna disposición que la persona pueda enterarse que sus comunicaciones fueron o están siendo intervenidas y que podría tratar de pelear la legalidad de estos actos. En la academia se ha discutido bastante el derecho de notificación el cual podría ser una gran ayuda para la transparencia y para defender los derechos de los ciudadanos mexicanos.

3.6.4 Cuarta Enmienda v Derecho a la privacidad

La Cuarta enmienda es una salvaguarda para prevenir arbitrariedades o por lo menos poner ciertos límites para las interferencias a la privacidad de los estadounidenses. Como lo he expuesto anteriormente, decidí usar a EUA como sujeto de estudio debido a su amplia jurisprudencia y su entendimiento en la materia de vigilancia. Si bien ambos sistemas jurídicos presentan diferencias importantes, no dejan de proteger y regular la misma materia que es la privacidad. Debido a la jurisprudencia previamente comentada como Katz, Jones y Carpenter la Cuarta enmienda ha logrado proteger y atacar los nuevos problemas de privacidad en la era digital.

Primero con Katz da un concepto clave para las siguientes decisiones en materia de privacidad que es la expectativa de privacidad el cual consiste en dos premisas: 1) El individuo exhibe una expectativa (subjetiva) de privacidad; 2) Esta expectativa es reconocida por la sociedad. Al leer estas dos reglas surge una cuestión fundamental y es que la regla se enfoca en las personas y se enfoca en cómo ellos o entienden la privacidad.

El cual es un punto para resaltar pues no despersonaliza el derecho por completo si no que lo trae a la vida diaria. El señor Katz tenía una expectativa de privacidad de que en la cabina de teléfono tenía privacidad y no podían ser escuchadas sus conversaciones. Son situaciones triviales, pero es importante tenerlas en cuenta para construir el derecho a la privacidad.

Es una regla que podría tener tintes subjetivos y tiene riesgo de cubrir situaciones que no necesariamente pueden o tener una expectativa de privacidad. No obstante, es una regla que tiene potencial de ayudar a adaptarla a futuras cuestiones como en el resto de la jurisprudencia estadounidense analizada.

En el caso *United States v Jones* el señor Jones le instalaron un dispositivo GPS para rastrear sus movimientos y en un principio la Corte de Distrito determinó que cuando el GPS señalaba que estaba en su hogar había una expectativa de privacidad, pero cuando estaba en la carretera o en las calles no había expectativa de privacidad.

Un razonamiento altamente cuestionable pues toda persona tiene una expectativa de privacidad de que sus movimientos no están siendo vigilados. Además, la Corte reconoce que

cuando nosotros intervenimos mediante la geolocalización a un coche en este caso, pero bien podría haber sido un celular lo que realmente estamos afectando es a la persona; quien sufre esa injerencia en su esfera de la privacidad es la persona no el automóvil o el celular.

Finalmente, con Carpenter la SCOTUS reconoce que la autoridad no puede tener un acceso ilimitado a las bases de datos de las empresas de telecomunicaciones. La autoridad forzosamente necesita una orden judicial. Hay que reconocer que la Corte entró a discutir conceptos sumamente técnicos que pueden dar cabida a discusiones sobre si son o no datos íntimos de la persona.

Ahora, el derecho mexicano ha entendido la privacidad no de manera expresa al igual que en el marco normativo estadounidense. El fundamento constitucional del derecho se encuentra en el art. 16 constitucional. Previamente había hecho un análisis del derecho a la privacidad en el marco legal mexicano por lo que no repetiré lo previamente explicado; sin embargo, si fuera prudente entender que en México no existen reglas como la expectativa de privacidad en EUA. Nuestro derecho es construido por medio de la legislación tanto mexicana como de la Corte Interamericana lo que enriquece la construcción de nuestro entendimiento del derecho.

Al igual que en el contexto estadounidense el derecho a la privacidad tiene múltiples dimensiones y ha existido jurisprudencia tanto mexicana como de la CIDH que ayudan a entender las distintas dimensiones. Desde el caso de Artavia Murillo donde la Corte sostuvo que "la vida privada engloba aspectos de la identidad física, emocional y social de la persona, incluyendo su autonomía personal y su derecho a establecer y desarrollar relaciones sociales con otra persona[139]

Donde se reconoce que el derecho a la privacidad está ligado con la libertad personal. En este caso nos enfocamos a la privacidad no desde la libertad personal sino desde la no injerencia a las comunicaciones del individuo. Tal como se ha analizado en la jurisprudencia de la CIDH en materia de privacidad. En los casos Tristán Donoso vs Panamá y Escher y otros vs Brasil la CIDH sostuvo que si bien el art. 11 de la Convención no prevé que las "comunicaciones" comprendan las comunicaciones telefónicas o las nuevas desarrolladas por

[139] OEA. *Estándares para una Internet Libre, Abierta e Incluyente Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.* OEA/Ser.L/V/II. (Marzo 15, 2017)

internet si están comprendidas jurisprudencialmente. Entonces, al leer el art. 11 de la Convención debemos entender que las comunicaciones son tanto físicas como digitales.

La jurisprudencia mexicana no ha sido la más extensa ni completa en el sentido de que ha negado que la localización por GPS necesita una autorización judicial, aunque afortunadamente en el CNPP si reconoce la necesidad de una autorización judicial. En México no hemos tenido grandes casos del Estado vs ciudadano como en EUA. Es un tema que se ha dejado a un lado por parte de la autoridad y que como lo he documentado requiere de gran atención debido a la creación de nuevas tecnologías como Pegasus.

3.6.5 Privacy Act v Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)

La legislación mexicana ofrece mayores salvaguardas al usuario y de adherirse al Convenio 108 Modernizada sería aún más profunda. La existencia de dos leyes federales para sujetos diferentes ofrece una distinción importante para una regulación sólida. Asimismo, la legislación local que expidan los Estados en materia de datos personales y para profundizar aún más la integración del Convenio 108 del Consejo de Europa a nuestro marco normativo.

La legislación en materia de datos personales es robusta y tiene un reconocimiento expreso constitucional en el art. 16 de la CPEUM. De este artículo se desprenden los derechos ARCO que permiten al ciudadano un mayor control sobre los datos personales que tiene la autoridad sobre sus datos.

La LGPDPPSO enmarca todos los principios por los cuales la autoridad tiene que sujetarse en el tratamiento de datos personales como los principios de: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad. Además, establece reglas básicas que son importantes pues son la base en la que las autoridades actuarán en la materia de protección de datos personales.

La ley contempla contenido relevante desde los principios que se deben aplicar en el manejo, la manera en que debe obtenerse en el consentimiento, la calidad en el manejo de datos personales, el aviso de privacidad y su contenido y diversas disposiciones que en mi opinión hacen que la regulación en materia de datos personales sea una materia digna de admirarse.

Aunado a lo anteriormente expuesto existe un órgano constitucional autónomo que es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) que es la autoridad encargada de atender todo lo relacionado en materia de protección de datos personales. Es una diferencia fundamental con el marco jurídico estadounidense que no cuenta con ningún organismo de esta naturaleza.

Si bien, el *Privacy Act* tiene algunas similitudes como que se le da el derecho de acceso y de rectificación a los ciudadanos estadounidenses, pero tiene ciertas limitantes como lo expuse anteriormente.

En el caso mexicano, en el art.55 se establecen las causales en las que puede ejercerse los derechos ARCO; sin embargo, no prevé ninguna fracción expresa que mencione que por razones de seguridad o de alguna investigación judicial pueda ser limitado. Sin embargo, la fracción V que señala "Cuando se obstaculicen actuaciones judiciales o administrativas" lo cual podría ser una fracción aplicable a estos casos de seguridad.

En el artículo 70 de la LGPDPPSO establece los casos en la que "El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos. para la materia del texto sería aplicable la fracción III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia."[140] Al igual que en el caso estadounidense existe una causal para compartir la información cuando se trate de investigación y persecución de delitos.

Sin embargo, no tiene la controvertida causal de "*routine use*" que es cuestionada y en general que puede dar lugar a muchas arbitrariedades. Aunque también dentro de la legislación en el art. 80 existen categorías que son ambiguas puesto que el art. 80 menciona:

"Art. 80: La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto."[141]

[140] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, LGPDPPSO, art. 70, Diario Oficial de la Federación [DOF] 26-01-2017, últimas reformas DOF 26-01-2017 (Mex.).
[141] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, LGPDPPSO, art. 80, Diario Oficial de la Federación [DOF] 26-01-2017, últimas reformas DOF 26-01-2017 (Mex.).

Tal y como expuse anteriormente existen diversas disposiciones dentro de la legislación de datos que es bastante cuestionable como que menciona que la obtención y tratamiento de datos personales por parte de los sujetos obligados competentes en materia de seguridad, procuración y administración de justicia está limitada a aquellos supuestos y categorías de datos que resulten "necesarios y proporcionales" ¿Qué significa eso? La legislación mexicana aún es ambigua y si bien no tenemos ningún concepto de "*routine use*" si tenemos nuestra legislación que aún tiene mucho por mejorar es un texto mejor construido y robusto que la legislación estadounidense.

4 CAPÍTULO IV: VIGILEMOS AL VIGILANTE

4.1.1 Justificación de la propuesta

El problema que enfrenta México tal y como ha sido analizado es que al no existir una regulación específica y actualizada a estas herramientas de vigilancia respecto de un uso proporcional, necesario e idóneo además de un correcto tratamiento de datos y transparencia en el uso de estos viola el derecho a la privacidad y la protección de datos de los mexicanos. Lo demostrado en este texto es que la legislación con la que contamos es insuficiente y no alcanza a proteger al ciudadano de una intervención con este tipo de *spywares*.

La legislación mexicana tiene serias limitaciones y no ha sido actualizada bajo los estándares de derechos humanos en torno a medidas de vigilancia. La propuesta que aporta el texto es que los programas de vigilancia como Pegasus deben ser el último recurso que pueda emplear la autoridad y nunca deben constituirse como la herramienta básica para realizar este tipo de intervenciones. Debido a su naturaleza tan intrusiva deben estar regulados y que solo sean operables bajo supuestos específicos y con supervisión judicial

Una posible solución podría ser prohibir el uso de este tipo de *spywares*, es una medida que desaprovecharía todas las ventajas de las nuevas herramientas de vigilancia. Las ventajas que tienen este tipo de programas de vigilancia son innegables y su capacidad para obtener datos sin ningún tipo de violencia o uso de la fuerza físico es atractiva.

Son herramientas que deben estar resguardadas y reguladas a profundidad como todas las demás herramientas de vigilancia; sin embargo, deben de requerir un especial cuidado y tratamiento. En un país rebasado por la violencia y el narcotráfico, podría apostarse a nuevas tecnologías que permitan resolver el problema sin poner en peligro más vidas humanas.

El Consejo de Derechos Humanos de la ONU reconoce la premisa sobre el avance de la tecnología a pasos exponenciales y que las medidas de vigilancia avanzan junto con ella por eso es necesario contar con legislación específica y actualizada para atacar este problema. Tal como expone en el *Report of the Special Rapporteur on the promotion on the promotion and protection of the right to freedom of opinion and expression:*

"Innovations in technology have facilitated increased possibilities for communication and freedom of expression, enabling anonymity, rapid information sharing, and cross-cultural dialogues. At the same time, changes in technologies have also provided new opportunities for State surveillance and intervention into individuals' private lives. As information and communication technologies evolved, so did the means by which States sought to monitor private communications. "[142]

La línea del reporte del Relator Especial en libertad de expresión sostiene esta premisa la tecnología avanza exponencialmente junto con el avance de las herramientas de vigilancia. Por lo tanto, debe existir legislación clara que establezca un uso proporcional, necesario e idóneo de estas nuevas herramientas.

El Reporte del Relator Especial considera que la gran mayoría de los países no han actualizado su legislación conforme al avance de la tecnología. Sin leyes explícitas que autoricen este tipo de tecnologías y herramientas y que definan el alcance de su uso los ciudadanos no pueden saber cuándo pudieran estar siendo intervenidos.[143]

Los datos personales ahora son altamente valiosos tanto para privados como autoridades. Los datos pueden comercializarse y crear un ingreso enorme; sin embargo, también pueden demostrar aspectos sumamente íntimos de la persona. Todos estos datos pueden ser almacenados por las empresas de telecomunicaciones como los metadatos lo cual pone en riesgo el derecho a la protección de datos. Como fue analizado en la sección sobre datos personales y la colaboración entre instancias de seguridad y empresas de telecomunicaciones existen deficiencias dentro de esta relación que ponen en riesgo la protección de datos.

El Estado mexicano tiene acceso a múltiples herramientas de vigilancia dirigida; en otras palabras, la vigilancia está orientada a un sujeto o a un grupo reducido de sujetos. Al contrario de la vigilancia masiva en la cual el Estado puede observar y analizar la información de no solamente nacionales sino extranjeros como fue el caso previamente discutido de Edward Snowden frente a la NSA con sus diversos programas.

Desafortunadamente, debido a las nuevas revelaciones del diario El País, México cuenta con herramientas de vigilancia masiva la cual es una tecnología claramente violatoria de derechos humanos puesto que no está sujeta a controles ni de necesidad, proporcionalidad e idoneidad.

---

[142] U.N. Human Rights Council [HRC]. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27. (May 16, 2011)
[143] U.N. Human Rights Council [HRC]. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27. (May 16, 2011)

En México contamos con la intervención de comunicaciones prevista en el artículo 91 y si bien pretende ser sumamente amplia para poder dar una justificación a que el Estado pueda entrar intervenir no sólo las comunicaciones de llamadas y SMS si no las llamadas y mensajes que se realizan por aplicaciones de mensajería o incluso redes sociales. No hay una mención explícita de las herramientas de vigilancia que el Estado puede usar ni los límites a estas herramientas.

Lo cual es un hecho grave puesto que da pie a que la autoridad pueda utilizar cualquier herramienta disponible sin importar sus capacidades o su origen. Debido a esto podría causar discrecionalidades en el uso y compra de estas herramientas. En el primer capítulo fue analizado cómo gobiernos y entidades que no tienen facultades para solicitar intervención de comunicaciones cuentan con *spyware* como Pegasus o Galileo.

4.1.2 Registro de las herramientas de vigilancia

Una de las soluciones debe ser la creación de un registro claro de la tecnología que se compra para la intervención de comunicaciones. El registro podría indicar ¿Qué autoridades adquirieron herramientas de vigilancia? Previamente deben existir disposiciones claras sobre las autoridades que pueden adquirir y usar estas herramientas.

Tal como fue expuesto en el primer capítulo no existe una interpretación clara de quiénes son las autoridades en este momento que pueden solicitar la intervención de comunicaciones y que pueden adquirir herramientas de vigilancia. ¿A quién le compraron el *software*? En este punto sería importante acreditar que el vendedor está constituido legalmente y que puede ser sujeto a responsabilidades legales en caso de haberlas. ¿Por cuánto tiempo adquirieron las herramientas?

La creación del registro está respaldada por las directrices establecidas en el Informe Anual de la Comisión Interamericana de Derechos Humanos 2013, Volumen II, informe de la Relatoría Especial para la Libertad de Expresión en la que establece que se debe asegurar que el público pueda acceder a información sobre los programas de vigilancia de comunicaciones privadas, su alcance y los controles existentes para garantizar que no puedan ser usados de manera arbitraria.[144] Actualmente, los ciudadanos saben que existe la intervención de

[144] CIDH. *Informe Anual de la Comisión Interamericana de Derechos Humanos 2013 Informe de la Relatoría Especial para la Libertad de Expresión*. OEA /Ser.L/V/II.149. (Diciembre 31, 2013)

comunicaciones pero desconocen completamente las herramientas y los programas que tiene el gobierno, debe existir una mayor rendición de cuentas y transparencia.

Acompañado de este registro puede plantearse la posibilidad de establecer una prohibición expresa de que los particulares puedan adquirir este tipo de herramientas tal y como lo hace EUA en su ECPA. El cual establece prohibiciones a los ciudadanos de comprar o hacer uso de este tipo de herramientas y, además, establece el uso de vendedores autorizados por lo que solo puede adquirirse este tipo de herramientas a través de vendedores autorizados. No hay nada que prohíba a empresas a no adquirir herramientas de esta naturaleza por lo cual el ciudadano no solo puede tener una injerencia a su derecho de privacidad por parte de la autoridad, si no, que particulares también pudieran hacer uso de este tipo de herramientas. Por lo que podría apostarse por una actualización a la legislación para contemplar sanciones a quienes adquieran este tipo de herramientas sin la debida autorización o a vendedores no autorizados y la creación de un registro público y transparente donde cualquier persona tenga conocimiento del tipo de instrumentos con los cuales el Estado puede intervenir las comunicaciones.

4.1.3 Respecto a los principios de proporcionalidad, necesidad e idoneidad

4.1.3.1 Principio de legalidad

Para que México pueda tener una regulación apropiada y actualizada a las nuevas medidas de vigilancia deben quedar claros los conceptos de limitación de derechos fundamentales. El Relator Especial establece que cuando se limite un derecho y especialmente el derecho de privacidad deben cumplirse con seis puntos esenciales: “a) Cualquier restricción tiene que estar prevista en ley; b) La esencia del derecho humano no está sujeto a restricción; c) Las restricciones deben ser necesarias en una sociedad democrática; d) La aplicación de restricciones no debe conferir una discrecionalidad sin complicaciones; e) No basta con que las restricciones se utilicen para conseguir uno de los fines permisibles enumerados; deben ser necesarias también para conseguir el objetivo legítimo y, f) Las medidas restrictivas deben ajustarse al principio de proporcionalidad; deben ser adecuadas para desempeñar su función

protectora; debe ser el instrumento menos perturbador de los que permitan conseguir el resultado deseado, y deben guardar proporción con el interés que debe protegerse."[145]

México no tiene una legislación actualizada y clara respecto a este tipo de instrumentos de vigilancia. El *spyware* de Pegasus es sumamente intrusivo y con una capacidad enorme para revelar datos personales de los ciudadanos. Por lo que la medida de uso de herramientas de vigilancia dirigida tiene que estar prevista en una ley.

Podría considerarse incluir en la ley que el Estado pueda utilizar este tipo de vigilancia en supuestos específicos y sin ser ambiguos. Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones[146] establecen en su primer principio de "Legalidad" que "Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación" Es por esto por lo que la limitación a los derechos de privacidad y protección de datos por medio de estas herramientas deben estar establecidos en ley.

La intervención de comunicaciones prevista en el artículo 291 del CNPP como ha sido analizado no alcanza a regular la intervención de comunicaciones usando Pegasus. Además, no hay un estándar claro y preciso sobre el uso de estas tecnologías por lo que el usuario no puede prever su aplicación y alcance. Herramientas como Pegasus operan en un margen sumamente ambiguo y cómo ha sido discutido anteriormente sus capacidades son altamente invasivas por lo que una medida tan drástica debería de quedar en la ley podría ser en este caso el CNPP de manera explícita sobre en qué supuestos y que restricciones tiene el uso de estas herramientas.

4.1.3.2 Principio de necesidad

Ahora, el uso de estas herramientas debe ser solo cuando sea estrictamente necesario. No puede usarse indiscriminadamente ni sin un control adecuado. Existen múltiples métodos

[145] U.N. Human Rights Council [HRC]. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27. (May 16, 2011)
[146] "Los Principios," Necesarios & Proporcionados Sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, última modificación 10 de mayo de 2014, https://necessaryandproportionate.org/es/principios/.

de investigación y herramientas que pueden ayudar a la prevención del delito que son mucho menos invasivos que el uso de estas herramientas. El tercer principio sobre derechos humanos en la vigilancia de comunicaciones establece lo siguiente

"Necesidad: Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La Vigilancia de las Comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado."[147]

La última oración es clave puesto que cualquier autoridad que pretenda justificar la necesidad de usar el instrumento debe justificarlo, no basta con decirle al juez a quién y cual celular, por cuánto tiempo. Es decir, todos los requisitos del 292 del CNPP debe realmente haber una justificación del porqué esa medida y no otra. En EUA su legislación contempla controles donde se establecen registros sobre cuántas veces ha pedido la autoridad una intervención de comunicaciones, la decisión del órgano jurisdiccional y el resultado de estas intervenciones.

El texto normativo mexicano podría incluir disposiciones que obliguen a justificar cuál es la necesidad de la medida a detalle, establecer por qué es necesaria e idónea esa medida y por qué las demás herramientas de vigilancia no ayudarían.

4.1.3.3 Principio de idoneidad

Juntamente con el principio de necesidad debe incluirse el principio de idoneidad el cual señala que "Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado." Siempre tiene que valorarse si la medida es idónea para el objetivo legítimo. Todo esto debe estar en ley y debe contemplarse de manera expresa puesto que actualmente lo único que menciona la ley son lo que tiene que contener la autorización y que esté fundado y motivado.

[147] Juan Carlos Lara, Valentina Hernández y Katitza Rodríguez, *Principios Internacionales Sobre la Aplicación de los Derechos Humanos a la Vigilancia de Comunicaciones y el Sistema Interamericano de Protección de Derechos Humanos,* Electronic Frointier Foundation, 2016. https://necessaryandproportionate.org/es/an%C3%A1lisis-jur%C3%ADdico-inter-americano/iachr-sp-agosto2016.pdf.

La fundamentación concluiría con señalar los artículos que facultan a esa autoridad para pedir la intervención, pero ¿La motivación? Podría prestarse a criterios poco sólidos tales como "Se solicita el uso de Pegasus para el esclarecimiento de los hechos imputados a X" Esto permite que no se tengan que hacer motivaciones profundas pues no hay requisitos apropiados a derechos humanos para la autoridad.

Los datos más recientes que existen acerca de la aprobación o denegación de autoridades judiciales sobre intervenciones de comunicaciones entre 2013 y 2015 por una investigación de R3D. De las cuáles de 3181 solicitudes documentadas que se hicieron en ese lapso solo 168 fueron negadas.[148] Esto quiere decir que solo el 5% de las solicitudes fueron negadas. Es una tasa demasiado baja y cuestionable para una medida tan restrictiva. De hecho, esta preocupación no es exclusiva en México si no que el Relator Especial ha mencionado que a pesar de que exista un requisito legal sobre una autorización de autoridad judicial (Como en el caso mexicano) la aprobación es básicamente de facto.

Por ejemplo, en Uganda en 2010 la ley sólo requiere que las autoridades comprueben que existe un "sustento razonable" para permitir la intervención de comunicaciones. Además, existe una grave disparidad en los datos que las autoridades presentan y aquellos registrados por el Consejo de la Judicatura (CJF). Por ejemplo, de 2013 a 2015 según datos de la PGR pidió 866 solicitudes de intervención de datos; sin embargo, el CJF reporta que entre esos años pidió 2392 solicitudes. ¿Cómo puede permitirse una disparidad en los datos tan grande?

4.1.3.4 Principio de proporcionalidad

Por otro lado, el principio de proporcionalidad tiene que ser otro eje en la fundamentación y motivación tanto de las autoridades. El que sea proporcional es una constante dentro de la literatura sobre regulación de herramientas de vigilancia. En el uso de estos instrumentos siempre deben de usarse las técnicas menos invasivas y que se hayan agotado todos los medios posibles antes de pedir el uso de una medida mucho más restrictiva.[149]

[148] R3D, *Gobierno Espía,* 42.
[149] U.N. Human Rights Council [HRC]. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40. (May 16, 2011)

Ahora este punto es crucial para el uso de herramientas como Pegasus puesto que hay un abanico de opciones de vigilancia. Tienen que estar muy bien delimitadas las funciones que usará la autoridad con sus respectivas responsabilidades y particularidades. Puesto que podemos permitir la grabación de sonido, pero toda aquella conversación que no genere valor probatorio tiene que ser inmediatamente desechada. Todo esto tiene que ir con las respectivas responsabilidades tanto administrativas como penales para quien está haciendo uso de la herramienta. Debe estar sujeto a un control estricto y bajo una constante vigilancia.

Es por esta razón que podría considerarse la creación un registro de las herramientas de vigilancia disponibles en México con una descripción detallada de las capacidades técnicas de cada herramienta. Cuidando que efectivamente se registren todas las capacidades, pues sería riesgoso registrar un *spyware* como Pegasus y mencionar que lo único que hace es registrar llamadas y mensajes de texto. Cada que se use una herramienta no solo debe ser proporcional en la herramienta per se sino en las funciones que podrá usar las herramientas en cada caso.

Por eso en la prueba de proporcionalidad previamente realizado se hizo énfasis en que funciones de Pegasus podían usarse y estaban habilitadas, pues un uso irrestricto del *spyware* podría provocar una violación seria y sumamente dañina que estaría lejos de cualquier justificación. Las autoridades deben respetar estos principios de proporcionalidad, necesidad e idoneidad.

4.1.4 Autorización judicial

Ahora respecto a la autorización judicial debe otorgarse verificando que se cumplan ciertas premisas. Primero, debe asegurarse que efectivamente hay una justificación detrás de la medida que cumpla con los principios de proporcionalidad, necesidad e idoneidad. De no haberla, la autoridad judicial deberá rechazar la solicitud o bien prevenirla para que sea corregida acorde a los estándares en derechos humanos. Otro punto importante es que debe entenderse que la intervención de comunicaciones y el uso de herramientas de vigilancia no se hacen sobre el dispositivo. Entonces el dispositivo no sufre la intervención sino la persona es la que va en el centro de la afectación.

La verdadera afectada es la persona, la medida no va contra el dispositivo, va contra el ser humano por eso se limitan los derechos de privacidad y protección de datos. De otra manera no podría garantizarse y entenderse que estas medidas pueden ser violatorias de derechos humanos.

Esto va de la mano con el principio sexto que establecen los Principios sobre la Vigilancia de Comunicaciones "Autoridad Judicial Competente" en el cual establece que todas las decisiones relacionadas con vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente imparcial e independiente. Deben "1) Estar separada e independiente de las autoridades encargadas de la Vigilancia de las Comunicaciones. 2)Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos, y 3) Tener los recursos adecuados en el ejercicio de las funciones que se le asignen."[150]

Ahora, sobre el primer punto es necesario revisar si de verdad no hay ningún tipo de coerción por la autoridad puesto que la tasa de aprobación de solicitudes es elevada parece como si la solicitud de facto fuera aprobada tal como fue analizado anteriormente. Respecto al segundo punto es necesario saber si nuestros jueces están debidamente capacitados en estas materias, debido al avance de la tecnología es complicado mantenerse al día; sin embargo, no es una justificación para no estar al tanto en cómo estas herramientas pueden vulnerar derechos humanos.

Asimismo, podría ser que sin un registro claro de las herramientas utilizadas, la autoridad no tiene los insumos necesarios para resolver de una manera informada y no puede ponderar apropiadamente los principios de necesidad, proporcionalidad e idoneidad; esto va de la mano con el tercer punto de la autoridad.

Un punto que se puede retomar de la legislación estadounidense es que existan registros de las autoridades que han solicitado la intervención de comunicaciones, los resultados que ha tenido y las motivaciones detrás de estas.

---

[150] Juan Carlos Lara, Valentina Hernández y Katitza Rodríguez, *Principios Internacionales Sobre la Aplicación de los Derechos Humanos a la Vigilancia de Comunicaciones y el Sistema Interamericano de Protección de Derechos Humanos,* Electronic Frointier Foundation, 2016. https://necessaryandproportionate.org/es/an%C3%A1lisis-jur%C3%ADdico-inter-americano/iachr-sp-agosto2016.pdf.

Esto crea incentivos para que las autoridades cada vez que soliciten una intervención de comunicaciones la justifiquen de buena manera puesto que siempre se haría un registro de esta solicitud. La intervención de comunicaciones es una herramienta intrusiva de derechos humanos y debe dársele la seriedad que merece. Actualmente, en la legislación mexicana no hay ninguna disposición que contemple este hecho. Además, abona a los insumos que tiene el juez para la toma de decisiones pues no solo tendría que realizar de acuerdo los estándares en derechos humanos, sino que podría contemplar si la autoridad solicitante no ha hecho un uso indebido de esta medida en el pasado.

Otro punto central es tener un límite claro sobre la duración de la medida. El Consejo de Derechos Humanos ya ha advertido que existen legislaciones donde la intervención puede extenderse en repetidas ocasiones e incluso indefinidamente. En el caso de la normativa angloamericana no es lo suficientemente claro el plazo que tiene la autoridad para seguir con la intervención. En México la ley señala que el máximo serán seis meses y que puede prorrogarse si hay nuevos elementos de prueba aportados por el MP.

Dentro de este proceso judicial podría garantizarse un recurso efectivo a las personas cuyos derechos fueron vulnerados ya sea el derecho a la privacidad, protección de datos o libertad de expresión. Dentro de las apuestas en la jurisprudencia internacional está brindarle al ciudadano los medios para defenderse de una intervención de comunicaciones y el derecho a ser notificado de la intervención. El Principio ocho "Notificación al Usuario" menciona que aquellas comunicaciones que están siendo sujetas a vigilancia deben ser notificadas con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los documentos que las autoridades presentaron para solicitar esta intervención.

La persona no tiene en ningún momento la posibilidad de poder combatir la legalidad de estos actos inclusive, puede que nunca tenga conocimiento de ellos. Son permisiones que se le dan a la autoridad que pueden desembocar en violaciones a los derechos humanos. Sin previa notificación resulta difícil para el ciudadano impugnar estos actos de la autoridad.

No solamente los principios mencionan estas medidas, si no, en los informes el Consejo de Derechos Humanos establece que dentro del marco legal para la vigilancia de comunicaciones debe "*a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their*

application;" Asimismo, en la resolución A/HRC/23/40 menciona "*Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State*." Por lo que resulta necesario una notificación al usuario para que tenga medios de defensa contra este tipo de actos.

Un argumento en contra del derecho de notificación sería que podría poner en riesgo el desarrollo de la investigación lo cual es un punto importante para considerar; sin embargo, el derecho a la notificación puede darse finalizando la intervención.

Inclusive el principio octavo de notificación al usuario prevé ciertos supuestos podría retrasar la notificación: "1) La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y 2) La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y 3) El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente."[151] Todo acto de autoridad que se ejerza contra un ciudadano debe tener acceso a un recurso efectivo para su defensa y a su notificación.

4.1.5 Protección de datos y transparencia

Ahora bien, respecto a la protección de datos también es necesarios asegurar unas condiciones de mayor seguridad. La resolución A/HRC/23/40 advierte que la capacidad que el Estado pueda ordenar a empresas de telecomunicaciones que almacenan por largos periodos de tiempo puede ser violatorio para derechos humanos debido a que incrementan la capacidad de vigilancia del Estado y los datos pueden ser vulnerables a fraude, robo o filtrado. En la Ley Federal de Telecomunicaciones y Radiodifusión en su artículo 190 establece que el concesionario tiene que recolectar y resguardar por prácticamente dos años los siguientes datos.[152] Igualmente, para salvaguardar este derecho tendría que valorarse en todo momento los

[151] Juan Carlos Lara, Valentina Hernández y Katitza Rodríguez, *Principios Internacionales Sobre la Aplicación de los Derechos Humanos a la Vigilancia de Comunicaciones y el Sistema Interamericano de Protección de Derechos Humanos*, Electronic Frointier Foundation, 2016. https://necessaryandproportionate.org/es/an%C3%A1lisis-jur%C3%ADdico-inter-americano/iachr-sp-agosto2016.pdf.

[152] Art. 190: Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

principios de proporcionalidad, necesidad e idoneidad para la intervención de comunicaciones lo mismo debería pedirse para la utilización de los datos recopilados por las empresas de telecomunicaciones.

Inclusive, el principio onceavo de los Principios de Vigilancia contempla que los Estados deberían de abstenerse por completo de exigir a los particulares la recolección de datos que permitan identificarlos. "La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios."

Un punto por considerar es las regulaciones que existen con los vendedores de productos de vigilancia como *NSO Group* o *Hacking Team*. Los productos que venden solamente los comercian con gobiernos supuestamente; sin embargo, las herramientas comercializadas tienen un amplio poder para que sean violatorias de derechos humanos. Son armas digitales que deben usarse y venderse solo en ciertos casos delimitados por la ley y sólo a ciertas personas autorizadas. Incluso el Relator Especial hace un comentario al respecto:

"In the most serious circumstances, the private sector has been complicit in developing technologies that enable mass or invasive surveillance in contravention of existing legal standards. (...) Such technologies are often sold to countries in which there is a serious risk that they will be used to violate human rights, particularly those of human rights defenders, journalists or other vulnerable groups. This industry is virtually unregulated as States have failed to keep pace with technological and political developments."

II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:
a) Nombre, denominación o razón social y domicilio del suscriptor;
b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);
c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;
d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;
e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;
f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;
g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y
h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

La industria privada tiene una responsabilidad en las posibles violaciones que surjan por la venta y uso de estas herramientas. México podría considerar establecer una legislación estricta para su venta en el país donde requieran permisos para vender este tipo de herramientas donde quede claro ¿Quién es el vendedor y comprador? ¿Qué productos se están adquiriendo y por cuánto tiempo? Deben de registrarse estos contratos y productos en bases de datos públicas para garantizar la transparencia.

Hasta la fecha los únicos contratos que existen sobre *Hacking Team* y *NSO Group* están en la red porque fueron filtrados y no por una obligación de transparencia por parte de la autoridad. El INAI ha ordenado al CNI para que dé a conocer los contratos hechos con *Hacking Team*; si bien, es un acierto del INAI, este hecho pone en duda la transparencia con la que se celebran estos contratos. El INAI ya se ha pronunciado al respecto señalando la obligación de estas autoridades para hacer públicos estos contratos.[153] Una posibilidad sería regular no solo las herramientas sino también los procesos de compra, venta, desarrollo y exportación de este tipo de herramientas pues de nada sirve no atender el problema integralmente.

Un tema pendiente del caso mexicano definitivamente son las graves deficiencias en transparencia que existen en la cantidad de veces que ha sido usada esta medida contra los ciudadanos. Tanto la resolución de "La privacidad en la era digital" como la resolución A/HRC/23/40 señalan la necesidad de ofrecer mecanismos en los cuales tanto las autoridades como los concesionarios revelen cuantas veces han solicitado o les han solicitado la intervención de comunicaciones.[154]

Asimismo, el principio noveno "Transparencia" establece que los Estados "Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos." En la Ley General de Transparencia y Acceso a la Información Pública (LGTA), art. 70, fracc. XLVII establece dicha exigencia.[155] La falta

[153] INAI, "Centro Nacional de Inteligencia debería dar a conocer contratos suscritos con agencia Hacking Team: INAI," Comunicado INAI/004/20, 22 de enero de 2020, https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-004-20.pdf.
[154] A.G. Res. 73/179. A/RES/73/179. (Octubre 31, 2016).
[155] LGTA - Artículo 70. En la Ley Federal y de las Entidades Federativas se contemplará que los sujetos obligados pongan a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan: XLVII. Para efectos estadísticos, el listado de

de transparencia en estos portales ha sido documentada por R3D cuando la SCJN resolvió el segundo recurso en materia de seguridad nacional en la historia donde R3D exige solamente el número de personas con dispositivos intervenidos y los dispositivos intervenidos. El Centro de Investigación y Seguridad Nacional (CISEN) argumentaba que esto podía poner en riesgo la seguridad nacional cuando realmente eran sólo números, nunca se pidió la identidad ni la razón de la intervención. Al final la SCJN resolvió a favor de R3D y ordenó al CISEN la publicación de la información.[156]

4.1.6 Consejo Independiente

Asimismo, valdría la pena considerar la idea de un Consejo Independiente podría ser integrado por funcionarios públicos del INAI o del órgano de transparencia local dependiendo de si es federal o local. El Consejo Independiente tendría la tarea de asegurarse que se cumplan con todas las medidas anteriormente expuestas pero una función clave sería supervisar en caso de que se use alguna herramienta de vigilancia sumamente intrusiva como Pegasus.

Tal como fue discutido en el primer capítulo usar herramientas como Pegasus omiten un paso crucial de control que es pedirle al concesionario los datos. Las herramientas como Pegasus o Galileo no necesitan que el concesionario de telecomunicaciones brinde los datos o la geolocalización. Por eso es podría considerase que exista un consejo independiente de funcionarios que además del juez estén supervisando que las autoridades hagan un uso correcto de las herramientas. De esta manera podría brindar más seguridad a los ciudadanos que la intervención se hará conforme a derecho.

Ahora, si bien por la naturaleza de la intervención de comunicaciones al ser una herramienta que muchas veces se ocupa de emergencia y es necesaria su rapidez para la resolución de casos podría utilizarse lo que se prevé en los Principios sobre la Vigilancia de

solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, que contenga exclusivamente el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente.

[156] Recurso de Revisión en Materia de Seguridad Nacional previsto en la Ley General de Transparencia y Acceso a la Información Pública 1/2016, Pleno de la Suprema Corte de Justicia [SCJN].

Comunicaciones es que exista una solicitud simultánea en lo que revisa la autoridad la solicitud, la autoridad hace uso. Posteriormente, la autoridad revisa y en su caso pide la opinión al Consejo.

Otro esquema de supervisión podría ser el usado en Reino Unido con la "Investigatory Powers Commissioners Office" el cual se encarga de supervisar las medidas de vigilancia usada por las autoridades públicas tanto los centros de inteligencia, fiscalías, policías y prisiones.[157] Son dos modelos que pueden ofrecer alternativas para brindar un mayor control frente al crecimiento de herramientas de vigilancia que ya no necesariamente ocupen los datos de los concesionarios por el avance de la tecnología. Estos mecanismos de supervisión independientes han sido recomendados por los Principios de Vigilancia de Comunicaciones en el principio décimo "Supervisión Pública"

"Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, según proceda, al acceso a información secreta o clasificada para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha publicado de forma transparente y precisa información sobre el uso y alcance de las técnicas y poderes de la Vigilancia de las Comunicaciones;"

Al igual que en las recomendaciones del Relator Especial donde establece que "*States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance of communications*." Asimismo, en la resolución "El derecho a la privacidad en la era digital" también se insta a la creación de mecanismos de supervisión

"Establezcan o mantengan mecanismos nacionales de supervisión, de índole judicial, administrativa o parlamentaria, que cuenten con los recursos necesarios y sean independientes, efectivos e imparciales, así como capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado."[158]

México podría considerar establecer este tipo de organismos para la utilización de herramientas de vigilancia como Pegasus de otra manera habría una seria falta de supervisión al no tener un paso extra de control con los concesionarios.

Dentro de las recomendaciones establecidas por la Relatoría Especial menciona que "*Surveillance techniques and practices that are employed outside of the rule of law must be*

[157] "What we do," IPCO, visitado el 4 de abril de 2021, ipco.org.uk/what-we-do/
[158] U.N. Human Rights Council [HRC]. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27. (May 16, 2011).

brought under legislative control. Their extra-legal usage undermines basic principles of democracy and is likely to have harmful political and social effects." Todas las técnicas de vigilancia que operan fuera de la ley tienen que ser reguladas y analizadas para establecer criterios claros de utilización y sus restricciones. Queramos o no queramos su uso es otro tema lo importante es legislar antes de que sea demasiado tarde.

5 CONCLUSIÓN

En conclusión, en el presente texto se ha analizado la falta de regulación clara y actualizada que proteja integralmente los derechos de privacidad y de protección de datos. Ambos países analizados presentan avances en la protección de estos derechos, pero aún quedan temas pendientes por resolver. En especial, una legislación que pueda regular las nuevas herramientas de vigilancia como Pegasus o Galileo, así como el resto de las herramientas de vigilancia. Es necesaria más regulación en el sentido de regular el uso de las nuevas herramientas de vigilancia y por supuesto un estricto cumplimiento de la normativa de datos para su correcto manejo.

En la primera parte del texto fue analizado el Caso Pegasus en México, el cual fue analizado y se llegó a la conclusión que el Estado mexicano hizo un uso indebido de esta herramientas que no tenía ningún tipo de investigación penal en contra suya. De igual manera, la normativa más completa y que brinda una mayor protección al ciudadano es la CNPP; sin embargo, es necesaria normativa que regule las herramientas además del proceso para intervenir comunicaciones.

Los datos recabados por las herramientas de vigilancia son sensibles y si se da un mal manejo por parte de la autoridad puede provocar una violación al derecho a la protección de datos como fue el caso de la PGR y su manejo de datos en el caso Pegasus. De igual manera, fue observado que en el caso de la intervención de comunicaciones, las concesionarias ofrecen otro control para que la autoridad pueda intervenir comunicaciones. No obstante, en el caso de las herramientas de vigilancia no hay intervención de las concesionarias pues el *spyware* es capaz de intervenir las comunicaciones sin la ayuda de las concesionarias.

Por lo tanto, se llegó a la conclusión que es necesaria regulación para salvaguardar los derechos a la privacidad y a la protección de datos de los ciudadanos cuando la autoridad utilicé este tipo de intervención de comunicaciones.

El uso de este tipo de herramientas en México es un fenómeno reciente a partir del año 2000 fue documentado el uso de estos *softwares* en el sexenio de Vicente Fox y Felipe Calderón. Se observó que fueron realizados contratos para la compra de herramientas de vigilancia invasivas y con fondos de la iniciativa merida. Igualmente, resalta que este tipo de *softwares* fueran vendidos a organismos como el SAT o Pemex. El panorama actual es similar al que había en esos años múltiples Estados de la república han adquirido estas herramientas y

nuevamente organismos como Pemex figura como un cliente. Por lo que resalta la necesidad de ejercer un control sobre los contratos celebrados. Debe cuidarse ¿Quién los contrata? ¿Por cuánto tiempo? ¿Con qué empresa y si la empresa está correctamente constituida? ¿Qué tipo de *software* fue adquirido?

En el segundo capítulo, quedó demostrado las múltiples dimensiones que existen sobre el derecho a la privacidad. Tanto teóricos como la Corte interamericana de derechos humanos coinciden que hay múltiples dimensiones del derecho por lo que al hablar del derecho tenemos que enfatizar en cuál nos vamos a enfocar. La SCJN reconoce esta división de dimensiones y coincide que el derecho a la privacidad en México está previsto en el 16 constitucional.

El derecho a la privacidad en el plano de la intervención de comunicaciones se nutre con la jurisprudencia de la Corte Interamericana de Derechos Humanos. La cual ha reconocido la importancia de salvaguardar este derecho frente a las nuevas tecnologías.

Las sentencias de la Corte si bien reconocen que los metadatos son parte de este derecho sigue sin reconocer que la geolocalización es interfiere igualmente en el derecho a la privacidad. Posteriormente, fue analizado el derecho a la privacidad bajo el marco normativo angloamericano. La forma en la que este derecho entiende el derecho a la privacidad es similar a la nuestra, refiriéndonos a la dimensión de la no inviolabilidad de la esfera privada. La cuarta enmienda tiene un fraseo similar a lo estipulado en el 16 constitucional.

Asimismo, tienen diferentes dimensiones respecto al derecho a la privacidad: por ejemplo, no es lo mismo el *right to privacy* que el *right to intimacy*. El primero tiene su eje en torno a la privacidad que tiene el usuario de no ser sujeto a injerencias que invadan su esfera a la privacidad sin una autorización previa del Estado que está fuertemente relacionado con la Cuarta Enmienda. El *right to intimacy* sería el derecho que tienen a que el Estado no interfiera dentro de sus creencias, vida personal y vida íntima.

De igual, fueron analizados tres casos emblemáticos sobre la privacidad y la protección de datos en Estados Unidos lo que da una idea del debate que EUA ha tenido y que en México aún no ha puesto en la mesa de discusión dichos temas. Katz con su emblemática regla "*Expectation of privacy*" que es una regla que pone a la persona y su concepción de privacidad al centro.

En el caso Jones aporta una visión importante que la Corte mexicana no simpatiza mucho y es que la geolocalización es una medida contra el individuo por medio de un

dispositivo. El alcance de la medida es bastante grande por lo que es necesaria una orden judicial puesto que interfiere en su esfera de privacidad. Este es un hecho a tomar en cuenta y que el juez mexicano debería de poner al centro a la persona y no al dispositivo.

Aunado a lo anterior, el caso de *Kyllon v United States* ofrece una visión importante para entender que no siempre vamos a tener la legislación actualizada, pero si tenemos que valorar lo que pueden revelar las nuevas tecnologías. Toda medida debe ponderarse en los criterios constitucionales aún cuando no se prevea explícitamente en la legislación. Esta regla ayuda a guiar la protección de los ciudadanos en lo que el legislador realiza reglas que regulen estas herramientas de vigilancia.

Finalmente, el caso de *Carpenter v United States* trae a la luz un tema importante en materia de metadatos y su importancia para salvaguardar el derecho a la privacidad. Puesto que resalta que debe pedirse una autorización judicial para acceder a los metadatos de las telecomunicaciones de los ciudadanos. México ha hecho grandes avances en esta materia puesto que hay una legislación robusto en materia de protección de datos y en el amparo 937/2015 establece que es necesaria la autorización judicial para acceder a los metadatos lo cual es un acierto y protege a los ciudadanos frente arbitrariedades.

En otro orden de ideas, fue analizado el derecho a la protección de datos el cual ha sido un derecho en constante construcción y actualización desde 2002. La materia de protección de datos y transparencia ha dado buenos pasos hacia adelante. Desde reconocer el derecho expreso a la protección de datos personales; además, regular la protección en dos ejes: uno para proteger los datos en posesión de particulares y otro para protegerlos en materia de sujetos obligados.

Asimismo, el que México cuente con organismo constitucional autónomo encargado de proteger este derecho y el acceso a la información brinda una mayor seguridad a los ciudadanos. Este órgano puede intervenir para la protección de los ciudadanos frente a las herramientas de vigilancia. Un paso podría ser el señalado anteriormente respecto de revisar a profundidad la manera en que los Ministerios públicos manejan los datos recopilados en la intervención de comunicaciones.

Al hacer un test de proporcionalidad utilizando estos derechos fue claro que existe una falta de normativa clara y actualizada para que el juez tenga certeza de que los derechos no será vulnerados al utilizar estas herramientas de vigilancia. Esto demostró cómo estos derechos juegan un papel decisivo para la toma de decisiones de un juez frente a un caso en los que tenga

que decidir si autoriza o no la intervención de comunicaciones usando una herramienta como Pegasus. Esta ponderación permite observar el rol de estos dos derechos frente a una medida que pudiera entrometerse en el derecho a la privacidad y la protección de datos.

Al analizar el marco normativo angloamericano frente al marco normativo mexicano surgen contrastes fuertes como que el marco americano privilegia mucho causales como terrorismo o ataques a la seguridad nacional para justificar acciones en contra de la ciudadanía. En el marco mexicano, si bien si hay este tipo de situaciones, son en menor medida que en al americano. Igualmente, el marco normativo mexicano en materia de protección de datos ofrece mayores garantías a los ciudadanos para salvaguardar el derecho a la protección de datos. Aunado con que México forma parte de la Convención 108 y de concretarse su respaldo a la Convención 108 modernizada daría aún más protecciones a los ciudadanos.

Asimismo, resalta que en el marco normativo angloamericano está regulado la compra y venta de estas herramientas de vigilancia. Debe existir un registro y solo puede comprarse a empresas que estén autorizadas en el registro. Este es un punto que valdría considerar en el marco normativo mexicano puesto que no hay una normativa que prevea conocer el registro de herramientas con las que cuenta México y valdría la pena apostar por regular este aspecto pues mucha de la venta ha sido por empresas de dudosa procedencia. Un registro sobre quién compra, por cuántos años, qué tipo de herramientas, quién vende sería vital para frenar el uso ilegal de este tipo de herramientas.

Respecto a las soluciones propuestas, debe resaltarse la necesidad de regular no solo la intervención de comunicaciones si no las herramientas de vigilancia empleadas. Debe prestarse atención a las herramientas y no solamente al proceso. Al no haber un registro claro de ellas no podemos saber cómo funcionan, cómo podemos limitar su uso y en qué casos pueden usarse. Si no hay regulación no solamente el Estado podría comprarlas si no los ciudadanos podrían acceder a estas herramientas y usarlas de manera ilegal y sin controles.

Entonces, debe apostarse por normativa clara y actualizada que regule su uso y establezca en la ley límites claro respecto a qué casos debería usarse una herramienta tan poderosa como Pegasus. Igualmente, para la solicitud que hace el Ministerio Público debería de existir un mayor grado de rigurosidad para pedirle al juez que utilizar herramientas como Pegasus en lugar de otras. Asimismo, debe de haber un conocimiento por parte del juez debido a que podría el juez desconocer que la herramienta no solo permite la grabación de audio si no

también la toma de fotos y extracción de contraseñas. Debe actualizarse a los jueces con las herramientas actuales que posee México.

En materia de transparencia es importante que la autoridad ofrezca datos exactos sobre las veces que ha utilizado ese tipo de herramientas y que no existan disparidades en los datos. Los contratos que ha hecho México con estas empresas deben ser información pública puesto que son relevantes para una mayor rendición de cuentas por parte de la autoridad. Debe existir un mayor presión para que las autoridades hayan celebrado estos contratos reconozcan el hecho y publiquen la información de dicho contrato.

La falta de regulación específica ha perjudicado el derecho a la privacidad y a la protección de datos de los mexicanos No existe una regulación que permita usar tanto la intervención de comunicaciones con los medios ordinarios y con las nuevas tecnologías que realmente garantice la protección a los derechos humanos. La tecnología avanza exponencialmente y este es un tema que no se va a resolver sin que Estados, industria privada y sociedad civil se sienten a legislar en la materia. El Estado mexicano ha utilizado estas herramientas como armas contra periodistas, sociedad civil y opositores al gobierno. Sin un verdadero control y regulación no existe una verdadera manera de solucionar el problema o por lo menos dar pasos en la dirección correcta. Mientras tanto los nuevos enemigos del Estado somos nosotros.

6 BIBLIOGRAFÍA:

"Electronic Surveillance," Electronic Surveillance. Visitado el 9 de febrero de 2020. https://www.law.cornell.edu/wex/electronic_surveillance.

A.G. Res. 73/179. A/RES/73/179. (Octubre 31, 2016).

ACLU. "SURVEILLANCE UNDER THE USA/PATRIOT ACT." ACLU. Visitado el 24 de marzo de 2021. https://www.aclu.org/other/surveillance-under-usapatriot-act.

ACUERDO del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas." Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Diario Oficial de la Federación [DOF]15-04-2016 (Mex.), formato HTML, http://www.dof.gob.mx/nota_detalle.php?codigo=5433280&fecha=15/04/2016.

Amparo en Revisión 134/2008, Segunda Sala de la Suprema Corte de Justicia [SCJN].

Amparo en Revisión 964/2015, Segunda Sala de la Suprema Corte de Justicia [SCJN].

Ángel, Arturo. "El Sabueso: ¿Jalisco compró el sistema de Hacking Team sólo para investigar secuestros?" *Animal Político*, 24 de julio de 2015. https://www.animalpolitico.com/elsabueso/el-sabueso-jalisco-compro-galileo-solo-para-investigar-secuestros-y-sin-conocer-a-hacking-team/.

Authorization for interception of wire, oral, or electronic communications, U.S.C § 2516.

B. Lee, Timothy. "Here's everything we know about prism to date." *Washington Post*, 12 de junio de 2013. https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

Ball, James. "NSA collects millions of text messages daily in 'untargeted' global sweep." *The Guardian*, 16 de enero de 2014. https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

Caballero, José Antonio, Miguel Carbonell, Héctor Felix – Fierro, Sergio Ayllón, José Roldán y Pedro Salazar *Ugarte. El Futuro del Instituto Federal De Acceso A La Información Pública y Protección De Datos Personales: Consideraciones Sobre Su Autonomía*

Constitucional. Distrito Federal: Instituto de Investigaciones Jurídicas, 2012. https://archivos.juridicas.unam.mx/www/bjv/libros/7/3196/2.pdf.

Carpenter v. United States. 819 F. 3d 880 (2018).

Caso Tristán Donoso vs. Panamá. Caso 12.360. Inter-Am. C.H.R. (2009). Caso Escher vs. Brasil. Caso 12.353. Inter-Am. C.H.R. (2009)

Charles Katz v. United States, 389 U.S. 347 (1967).

CIDH. *Informe Anual 2013*. *Informe de la Relatoría Especial para la Libertad de Expresión.* OEA/Ser.L/V/II.149. (Diciembre 31, 1999)

Clérico, Laura. *Derechos y Proporcionalidad: Violaciones por acción, insuficiencia y por regresión. Miradas locales, interamericanas y comparadas.* Querétaro: Instituto de Estudios Constitucionales del Estado de Querétaro, 2018.

Communications Assistance for Law Enforcement Act, 47 USC 1001 (1994).

COMUNICACIONES PRIVADAS. LA SOLICITUD DE ACCESO A LOS DATOS DE TRÁFICO RETENIDOS POR LOS CONCESIONARIOS, QUE REFIERE EL ARTÍCULO 190, FRACCIÓN II, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN, DEBE REALIZARSE EN TÉRMINOS DEL ARTÍCULO 16 CONSTITUCIONAL Y SÓLO LA AUTORIDAD JUDICIAL PODRÁ AUTORIZAR LA ENTREGA DE LA INFORMACIÓN RESGUARDADA, Segunda Sala de la Suprema Corte de Justicia [SCJN], Gaceta del Semanario Judicial de la Federación, Décima Época, tomo I, Julio de 2016, Tesis 2a. XXXV/2016, Página 776. (Mex).

Constitución 1917 - 2017. "ÍNDICE DEL PROCESO LEGISLATIVO CORRESPONDIENTE A LA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 01 DE JUNIO DE 2009" Visitado el 20 de febrero de 2021. https://www.constitucion1917-2017.pjf.gob.mx/sites/default/files/CPEUM_1917_CC/procLeg/187%20-%2001%20JUN%202009.pdf.

Constitución Política de los Estados Unidos Mexicanos, CP, Diario Oficial de la Federación [DOF] 05-02-1917, últimas reformas DOF 28-05-2021 (Mex), formato PDF, http://www.diputados.gob.mx/LeyesBiblio/pdf/1_280521.pdf.

Convención Americana sobre Derechos Humanos (Pacto de San José). 22 de noviembre de 1969.

Declaración Americana de los Derechos y Deberes del Hombre. 1948.

Decreto del Instituto Federal de Acceso a la Información Pública, Diario Oficial de la Federación [DOF] 24-12-2002 (Mex.), formato HTML, https://www.dof.gob.mx/nota_detalle.php?codigo=716452&fecha=24/12/2002.

Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación [DOF] 30-04-2009 (Mex.), formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5089047&fecha=30/04/2009.

Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación [DOF] 01-06-2009 (Mex.), formato HTML, https://www.dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009.

DECRETO por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente, Diario Oficial de la Federación [DOF] 12-06-2018 (Mex.), formato HTML, https://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018.

DECRETO por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. Diario Oficial de la Federación [DOF] 04-05-2015 (Mex.)., formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015.

DECRETO por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia. Diario Oficial de la Federación [DOF] 07-02-2014 (Mex.), formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014.

DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, Segunda Sala de la Suprema Corte de Justicia [SCJN],

Semanario Judicial de la Federación y su Gaceta, Novena Época, tomo XXVII, mayo de 2008, Tesis 2a. LXIII/2008, página 229 (Mex).

Estrada Tanck, Mónica. "De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia." En *Ley General de Datos para la Protección de Datos en Posesión de Sujetos Obligados Comentada*, editado por el INAI, 244 - 245. Ciudad de México: INAI, 2018.

Exploring Constitutional Conflicts. "The Right to Privacy." Visitado el 26 de enero de 2020. http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

Forcese, Craig. "Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives." In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Geist Michael, 127-160. University of Ottawa Press, 2015.

Gallegos, Zorayda. "La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles." *El País*, 14 de abril de 2021, https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html.

Geliman, Barton. "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls." *Washington Post*, 18 de marzo de 2014. https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

Glüsing, Von Jens, Laura Poitras, Marcel Rosenbach, y Holger Stark. "NSA Accessed Mexican President 's Email." *Spiegel International*, 20 de octubre 20 de 2013. https://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

Guadarrama, Jesús. "¿Cuántos mexicanos tienen teléfono celular? Actualizado." *Milenio*, 17 de febrero de 2020. https://www.excelsior.com.mx/hacker/cuantos-mexicanos-tienen-telefono-celular-actualizado/1364594.

Hasty, Robert, Dr. Trevor Nagel, and Mariam Subjally White and Case. *Data Protection Law in the USA*. Advocates for International Development Lawyers Eradicating Poverty, agosto 2013. https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf.

https://aristeguinoticias.com/0801/mexico/mexico-compro-equipos-de-espionaje-a-empresas-vinculadas-con-la-nsa-de-eu/.

INAI. "Centro Nacional de Inteligencia debería dar a conocer contratos suscritos con agencia Hacking Team: INAI." Comunicado INAI/004/20, 22 de enero de 2020. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-004-20.pdf.

INAI. "DETERMINA INAI QUE FGR, RESPECTO AL SOFTWARE PEGASUS, INCUMPLIÓ LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS." Comunicado INAI/054/19, 20 de febrero de 2019. http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf.

INAI. *Guía para el Borrado Seguro de Datos Personales*. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, junio de 2016. http://inicio.inai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf.

INTERVENCIÓN DE COMUNICACIONES PRIVADAS SIN AUTORIZACIÓN JUDICIAL. LAS GRABACIONES DERIVADAS DE UN ACTO DE ESA NATURALEZA CONSTITUYEN PRUEBAS ILÍCITAS QUE POR MANDATO EXPRESO DEL ARTÍCULO 16 CONSTITUCIONAL CARECEN DE TODO VALOR PROBATORIO, Pleno de la Suprema Corte de Justicia [SCJN], Semanario Judicial de la Federación y su Gaceta, Novena Época, tomo XXVII, abril de 2008, Tesis P. XXXIII/2008, página 6.

IPCO. "What we do." Accesado el 4 de abril de 2021. ipco.org.uk/what-we-do/.

Kyllo v. United States, 533 U.S. 27 (2001).

Lara, Juan Carlos, Valentina Hernández y Katitza Rodríguez. *Principios Internacionales Sobre la Aplicación de los Derechos Humanos a la Vigilancia de Comunicaciones y el Sistema Interamericano de Protección de Derechos Humanos*. Electronic Frointier Foundation, 2016. https://necessaryandproportionate.org/es/an%C3%A1lisis-jur%C3%ADdico-inter-americano/iachr-sp-agosto2016.pdf.

Ley de la Guardia Nacional [LGN], Diario Oficial de la Federación [DOF] 27-05-2019, últimas reformas DOF 27-05-2019 (Mex), formato HTML, http://dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019.

Lind, Dara. “Everyone's heard of the Patriot Act. Here's what it actually does.” *Vox*, 2 de junio 2015. https://www.vox.com/2015/6/2/8701499/patriot-act-explain.

Lineamientos de Colaboración en Materia de Seguridad y Justicia [LCMSJ], Diario Oficial de la Federación [DOF] 21 de junio de 1996, últimas reformas DOF 2-12-2015 (Mex.), formato PDF, http://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/dofpiftext111115159.pdf.

Lynskey, Orla. “DECONSTRUCTING DATA PROTECTION: THE 'ADDED-VALUE' OF A RIGHT TO DATA PROTECTION IN THE EU LEGAL ORDER.” *The International and Comparative Law Quarterly* 63, No. 3 (Julio 2014): 569-597.

Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited, 18 U.S.C § 2512.

Marczak, B. y John Scott - Railton. *“The Million Dollar Dissident: NSO Group’s iPhone Zero-Days used against a UAE Human Rights Defender.”* Citizen Lab Research Report No. 78, University of Toronto, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Mayer, J y Patrick Mutchler. “MetaPhone: The Sensitivity of Telephone Metadata.” *Web Policy*, 12 de marzo de 2014. http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

OCDE. *The OCDE Privacy Network*. OECD Publishing, 2013. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OEA. *Estándares para una Internet Libre, Abierta e Incluyente Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.* OEA/Ser.L/V/II. (Marzo 15, 2017).

OEA. *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*. OEA/Ser.Q. (Marzo 26, 2015).

Olmos, Raúl. “SUBORDINADO DE MURILLO KARAM, LIGADO A GRUPO EMPRESARIAL QUE VENDIÓ PEGASUS A LA PGR.” *Mexicanos Contra la Corrupción e Impunidad,* 20 de febrero de 2017. https://contralacorrupcion.mx/pegasus-pgr/.

Pozen, D. "Privacy - Privacy Tradeoffs." *The University of Chicago Law Review* 83, No. 1 (Invierno 2016): 221-247.

Privacy Act of 1974, 5 U.S.C. § 552a (1974).

Procedure for interception of wire, oral, or electronic communications, 18 U.S.C § 2518.

Prohibition of use as evidence of intercepted wire or oral communications, 18 U.S.C § 2515.

PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS, Tribunales Colegiados de Circuito [TCC], Gaceta del Semanario Judicial de la Federación, Décima Época, tomo III, Septiembre de 2009, Tesis I.10o.A.6 CS, página 2200 (Mex.).

Quintana, Yolanda. "Todos los programas de espionaje de la NSA desvelados por Snowden." *elDiario.es*, 19 de marzo de 2014. https://www.eldiario.es/turing/vigilancia_y_privacidad/nsa-programas-vigilancia-desvelados-snowden_1_4974573.html.

R3D: Red en Defensa de los Derechos Digitales, *Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México*. R3D.

R3D. "Recolección de datos de geolocalización de datos en banca en línea es desproporcionada riesgosa e innecesaria." *R3D*, 23 de marzo de 2021. https://r3d.mx/2021/03/23/recoleccion-de-datos-de-geolocalizacion-en-banca-en-linea-es-desproporcionada-riesgosa-e-innecesaria/.

Railton, J, B. Marczack, C Guarneri, y Masashi Nishihata. "BITTERSWEET: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links". Citizen Lab Research Report No. 89, University of Toronto, 2017. https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

Records maintained on individuals – (b) Conditions of disclosure, 5 U.S.C. § 552a.

Recurso de Revisión en Materia de Seguridad Nacional previsto en la Ley General de Transparencia y Acceso a la Información Pública 1/2016, Pleno de la Suprema Corte de Justicia [SCJN].

Redacción. “México compró equipos de espionaje a empresas vinculadas con la NSA de EU.” *Aristegui Noticias*, 8 de enero de 2014.

Redacción. “Adquiere la PGR equipo para espiar.” *Reforma*, 12 de septiembre de 2016. https://www.reforma.com/aplicacioneslibre/articulo/default.aspx?id=937450&md5=6796275797392efc0223b450c4b2d0e2&ta=0dfdbac11765226904c16cb9ad1b2efe&lcmd5=daff83a6dbd92c568ac692898d5f4c2b.

Reuters. “NSA surveillance exposed by Snowden was illegal, court rules seven years on.” *The Guardian*, 3 de septiembre de 2020. https://www.theguardian.com/us-news/2020/sep/03/edward-snowden-nsa-surveillance-guardian-court-rules.

Rodríguez Real, Leticia. “Desmantelar el INAI.” *Nexos*, 14 de enero de 2021. https://anticorrupcion.nexos.com.mx/desmantelar-el-inai/.

Solange, María y Alessandra Barzizza Vignau. *Democracia, privacidad y protección de datos personales*. Ciudad de México: Instituto Nacional Electoral, 2019.

SOLICITUD MINISTERIAL DE ENTREGA DE DATOS CONSERVADOS POR LOS CONCESIONARIOS DE TELECOMUNICACIONES. SU AUTORIZACIÓN ES COMPETENCIA EXCLUSIVA DEL PODER JUDICIAL DE LA FEDERACIÓN (INTERPRETACIÓN CONFORME DEL ARTÍCULO 303 DEL CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES), Tribunales Colegiados de Circuito [TCC], Gaceta del Semanario Judicial de la Federación, Décima Época, Tomo IV, Diciembre de 2017, Tesis I.8o.P.18 P, Página 2267 (Mex).

The Guardian. “NSA Prism program slides.” *The Guardian*, 1 de noviembre de 2013. https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document.

Toomey, Patrick. “The NSA Continues to Violate Americans' Internet Privacy Rights.” *ACLU*, 22 de agosto de 2018. https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

U.N. Human Rights Council [HRC]. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/17/27. (May 16, 2011).

U.N. Human Rights Council [HRC]. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/23/40. (May 16, 2011).

United States v. Jones, 615 F. 3d 544 (2012).

Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act, 50 USC 1801(2015).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 18 USC 1 (2001).

Warren, S y Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, No. 5 (Dec. 15, 1890): 193-220. http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C.

Wikileaks. "Hacking Team." Hacking Team Archive. Visitado el 12 de noviembre de 2020.https://wikileaks.org/hackingteam/emails/emailid/5391.

Wolfson, Josiah. "The Expanding Scope of Human Rights in a Technological World—Using the Inter-American Court of Human Rights to Establish a Minimum Data Protection Standard across Latin America." *The University of Miami Inter-American Law Review* 48, No. 3 (Primavera 2017).

Zerega, Georgina y Pablo Ferri. "El Estado Mexicano se atraganta con el caso Pegasus." *El País*, 6 de agosto de 2020. https://elpais.com/mexico/2020-08-06/el-estado-mexicano-se-atraganta-con-el-caso-pegasus.html.