H. CONGRESO DEL ESTADO
DE CHIHUAHUA

COMISIÓN DE SEGURIDAD PÚBLICA Y PROTECCIÓN CIVIL
LXVI LEGISLATURA
DCSPPC/026/2020

ACUERDO No.
LXVI/AARCH/0564/2020 I P.O.
UNÁNIME

H. CONGRESO DEL ESTADO
P R E S E N T E.-

La Comisión de Seguridad Pública y Protección Civil, con fundamento en lo dispuesto por los artículos 57 y 64, fracción I, de la Constitución Política del Estado de Chihuahua; los artículos 87, 88 y 111 de la Ley Orgánica, así como los artículos 80 y 81 del Reglamento Interior y de Prácticas Parlamentarias, ambos del Poder Legislativo del Estado de Chihuahua, somete a la consideración del Pleno el presente Dictamen elaborado con base en los siguientes:

ANTECEDENTES:

I.- Con fecha 28 de mayo de 2020, el Diputado Omar Bazán Flores, integrante del Grupo Parlamentario del Partido Revolucionario Institucional, presentó Iniciativa con carácter de Punto de Acuerdo, a efecto de exhortar al Poder Ejecutivo Estatal, a través de la Secretaría de Seguridad Pública, a fin de que se abstenga de adquirir equipos de espionaje, hasta en tanto existan lineamientos específicos para su utilización.

II.- La Presidencia del Honorable Congreso del Estado, en uso de las facultades que le confiere el artículo 75, fracción XIII, de la Ley Orgánica del Poder Legislativo, el día 28 de mayo de 2020, tuvo a bien turnar a quienes integramos la Comisión de Seguridad Pública y Protección Civil la iniciativa antes referida, a

efecto de proceder a su estudio, análisis y elaboración del dictamen correspondiente.

III.- La iniciativa citada se sustenta esencialmente en los siguientes argumentos, los cuales son copia textual de su parte expositiva:

> *"La Declaración Universal de los Derechos Humanos es un documento que marca un hito en la historia de los derechos humanos. Elaborada por representantes de todas las regiones del mundo con diferentes antecedentes jurídicos y culturales, la Declaración fue proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su Resolución 217 A, como un ideal común para todos los pueblos y naciones. La Declaración establece, por primera vez, los derechos humanos fundamentales que deben protegerse en el mundo entero y Considerando que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana; Así mismo, Considerando que el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad, y que se ha proclamado, como la aspiración más elevada del hombre, el advenimiento de un mundo en que los seres humanos, liberados del temor y de la miseria, disfruten de la libertad de palabra y de la libertad de creencias. Por último, LA ASAMBLEA GENERAL proclama la actual DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos, tanto entre los pueblos de los Estados Miembros como*

entre los de los territorios colocados bajo su jurisdicción. (Preámbulo de DUDH)

En su artículo 12 afirma que: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Así mismo el artículo 29 afirma que:
1. Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad.
2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.
3. Estos derechos y libertades no podrán, en ningún caso, ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas.

Por su paste la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares. Adoptada por la Asamblea General en su resolución 45/158, de 18 de diciembre de 1990, establece:

Los Estados Partes en la presente Convención, Teniendo en cuenta los principios consagrados en los instrumentos fundamentales de las Naciones Unidas en materia de derechos humanos, en particular la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial, la Convención sobre la eliminación de todas las formas de discriminación contra la mujer y la Convención sobre

los Derechos del Niño... Articulo 14 "Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques".

En tanto que el Pacto Internacional de Derechos Civiles y Políticos, Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966 Entrada en vigor: 23 de marzo de 1976, de conformidad con el artículo 49 Lista de los Estados que han ratificado el pacto, establece:

Los Estados Partes en el presente Pacto, Considerando que, conforme a los principios enunciados en la Carta de las Naciones Unidas, la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables...artículo 17: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Por otro lado la Convención Americana sobre Derechos Humanos (pacto de San José), establece que:

Los Estados Americanos signatarios de la presente Convención, Reconociendo que los derechos esenciales del hombre no nacen del hecho de ser nacional de determinado Estado, sino que tienen como fundamento los atributos de la persona humana, razón por la cual justifican una protección internacional, de naturaleza convencional coadyuvante o complementaria de la que ofrece el derecho interno de los Estados americanos... artículo 11. Protección de la Honra y de la Dignidad estipula 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.

En tanto que la Declaración Americana de los Derechos y Deberes del Hombre, Aprobada en la Novena Conferencia Internacional Americana Bogotá, Colombia, 1948 La IX Conferencia Internacional Americana, establece en su artículo 5. El Derecho a la protección a la honra, la reputación personal y la vida privada y familiar.
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.

Por su parte el Convenio Europeo de Derechos Humanos, Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales Roma, 4.XI.1950, establece en su artículo 8 del Derecho al respeto a la vida privada y familiar
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Por su parte el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión presentó este informe

al Consejo de Derechos Humanos de conformidad con la resolución 7/36 del Consejo:

"Protección inadecuada del derecho a la intimidad y a la protección de datos...
53. El derecho a la intimidad es fundamental para la libre expresión personal. De hecho, a lo largo de la historia la voluntad de las personas de participar en debates públicos sobre temas controvertidos ha estado siempre vinculada con la posibilidad de poder hacerlo de forma anónima. Internet permite acceder a información y tomar parte en debates públicos sin tener que revelar la identidad personal, por ejemplo, usando seudónimos en tableros electrónicos de mensajes y foros en línea. A la vez, Internet ofrece nuevos instrumentos y mecanismos por medio de los cuales los actores, tanto estatales como privados, pueden supervisar y reunir información sobre las comunicaciones y actividades de los usuarios de Internet.

Estas prácticas pueden constituir una violación del derecho de estos usuarios a la
intimidad y, al socavar la confianza del público y la seguridad de Internet, obstruir el libre flujo de información e ideas en línea.

54. El Relator Especial está muy preocupado por las medidas adoptadas por ciertos
Estados contra personas que se comunican por Internet, con frecuencia justificándolas en términos generales por su necesidad para proteger la seguridad nacional o luchar contra el terrorismo. Aunque esos fines pueden ser legítimos de conformidad con el derecho internacional de los derechos humanos, la vigilancia suele tener motivos políticos y no de seguridad y llevarse a cabo de forma arbitraria y encubierta. Por ejemplo, algunos Estados han hecho uso de sitios populares de redes sociales, como Facebook, para detectar y vigilar actividades de defensores de los derechos humanos y miembros de la oposición, y en algunos casos han obtenido nombres

de usuarios y contraseñas para acceder a las comunicaciones privadas de usuarios de Facebook.

55. Varios Estados están promulgando leyes nuevas o modificando leyes existentes para tener más margen de vigilancia de las actividades de los usuarios de Internet, así como del contenido de sus comunicaciones, sin ofrecer suficientes garantías frente a los abusos.

Además, hay Estados que han establecido un sistema de identificación del usuario por su nombre verdadero para enviar comentarios o subir contenido en línea, lo cual puede poner en peligro su capacidad de expresarse de forma anónima, especialmente en países en los que los derechos humanos se violan con frecuencia. Además, en muchos países se están adoptando medidas para reducir la capacidad de los usuarios de Internet de protegerse de la vigilancia arbitraria, por ejemplo, limitando el uso de tecnologías de cifrado.

56. El Relator Especial observa asimismo que en muchos Estados son insuficientes o inadecuadas las leyes de protección de datos que establecen quién tiene permitido el acceso a los datos personales, para qué pueden usarse, cómo han de almacenarse y durante cuánto tiempo. La necesidad de adoptar leyes claras para proteger los datos personales es todavía más imperiosa en la actual era de la información, en la que los intermediarios reúnen y almacenan un gran volumen de datos personales, y es preocupante la inclinación de los Estados a obligar a estos agentes privados a facilitar información sobre sus usuarios o ejercer presión sobre ellos para que lo hagan. Además, con el auge de los servicios de computación en nube, que almacenan la información en servidores distribuidos en distintas ubicaciones geográficas, es imprescindible velar por que los terceros respeten también garantías estrictas en materia de protección de datos.

57. El derecho a la intimidad está garantizado en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. En este último se establece que: "1) nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; 2) toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". Aunque "correspondencia" se ha interpretado fundamentalmente como cartas escritas, el vocablo abarca todas las formas de comunicación, incluso por Internet. Así pues, el derecho a la correspondencia privada genera una amplia obligación del Estado de velar por que el correo electrónico y otras formas de comunicación en línea lleguen a su destinatario previsto sin injerencia o inspección por parte de órganos estatales o de terceros.

58. Además, la protección de los datos personales representa una forma especial de respeto del derecho a la intimidad. De conformidad con el artículo 17, párrafo 2, los Estados deben regular, mediante leyes articuladas con claridad, el registro, procesamiento, uso y transmisión de datos personales automatizados y proteger a los afectados contra el uso indebido por parte de órganos estatales y partes privadas. Además de prohibir el procesamiento de datos para fines incompatibles con el Pacto, las leyes de protección de datos deben establecer derechos a la información, la corrección y, de ser necesario, la supresión de datos y arbitrar medidas eficaces de supervisión. Asimismo, como se afirma en la observación general del Comité de Derechos Humanos sobre el derecho a la intimidad, "para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos".

59. El Relator Especial observa que el derecho a la intimidad puede ser objeto de restricciones o limitaciones en determinadas circunstancias excepcionales, que pueden incluir medidas de vigilancia estatal con fines de administración de la justicia penal, prevención del delito o lucha contra el terrorismo. No obstante, esa injerencia solo es permisible si se cumplen los criterios correspondientes a las limitaciones admisibles de conformidad con el derecho internacional de los derechos humanos. Por eso es necesario que exista una ley en la que se expongan con claridad las condiciones en que puede restringirse el derecho de una persona a la intimidad en circunstancias excepcionales y que las medidas que vulneren este derecho se adopten sobre la base de una decisión concreta de una autoridad estatal facultada expresamente a ello por la ley, normalmente el poder judicial, a efectos de proteger los derechos de otras personas, por ejemplo para obtener pruebas a fin de impedir que se cometa un delito, respetando el principio de proporcionalidad".

Dentro de las Conclusiones y recomendaciones que se presentan en el análisis y con las cuales coincidimos en plenitud, me permito continuar destacar las siguientes:

82. ..., aunque los usuarios pueden disfrutar en Internet de un anonimato relativo, los Estados y agentes privados tengan acceso a tecnologías de seguimiento y reunión de información sobre las comunicaciones y actividades de estos usuarios. Esas prácticas pueden constituir una violación del derecho de los usuarios a la intimidad y, al socavar la confianza del público y la seguridad de Internet, obstruir el libre flujo de información e ideas en línea.

83. ...la obligación de los Estados de adoptar leyes eficaces de protección de la intimidad y los datos de conformidad con el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y la Observación general N° 16 del Comité de Derechos Humanos, con inclusión de leyes que garanticen claramente el derecho de toda persona a verificar de forma inteligible si hay datos personales suyos

almacenados en archivos automáticos de datos y, en caso afirmativo, a obtener información sobre cuáles son esos datos y con qué fin se han almacenado, así como qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos.

84. Asimismo, el Relator Especial exhorta a los Estados a que velen por que las personas puedan expresarse anónimamente en línea y a que se abstengan de adoptar sistemas de registro de los nombres verdaderos. En determinadas situaciones excepcionales en las que los Estados pueden limitar el derecho a la intimidad con fines de administración de la justicia penal o de prevención del delito, el Relator Especial subraya que esas medidas deben respetar el marco internacional de derechos humanos y contar con salvaguardias adecuadas contra el abuso, incluida la obligación de que toda medida encaminada a limitar el derecho a la intimidad se adopte sobre la base de una decisión concreta de una autoridad estatal facultada expresamente a ello por la ley, y respete los principios de necesidad y proporcionalidad".

Por su parte la Coalición necesaria y proporcional, (mayo de 2014), establece los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, que se lanzó oficialmente en el Consejo de Derechos Humanos de la ONU en Ginebra en septiembre de 2013. Versión Final Mayo 2014

En su Preámbulo afirma: "La privacidad es un derecho humano fundamental y es fundamental para el mantenimiento de las sociedades democráticas. Es esencial para la dignidad humana y refuerza otros derechos, como la libertad de expresión e información, y la libertad de asociación, y está reconocido por el derecho internacional de los derechos humanos. La vigilancia de las comunicaciones interfiere con el derecho a la privacidad entre otros derechos humanos. Como resultado, solo puede justificarse cuando lo prescribe la ley, es necesario para lograr un objetivo legítimo y proporcional al objetivo perseguido.

Así mismo, La frecuencia con la que los Estados buscan acceso tanto al contenido de comunicaciones como a los metadatos está aumentando dramáticamente, sin un escrutinio adecuado. Los metadatos de las comunicaciones pueden crear un perfil de la vida de un individuo, que incluye afecciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tantos detalles o incluso más detalles de los que se podrían discernir del contenido de las comunicaciones. A pesar del vasto potencial de intrusión en la vida de un individuo y el efecto escalofriante en las asociaciones políticas y de otro tipo, las leyes, las actividades de regulación, los poderes o las autoridades a menudo otorgan a los metadatos de las comunicaciones un menor nivel de protección y no imponen restricciones suficientes sobre cómo pueden ser posteriormente utilizado por los Estados.

Al adoptar una nueva técnica de Vigilancia de las Comunicaciones o expandir el alcance de una técnica existente, el Estado debe determinar si la información que se puede obtener cae dentro del ámbito de la Información Protegida antes de buscarla, y debe someterse al escrutinio del poder judicial u otra autoridad democrática. Mecanismo de supervisión. Al considerar si la información obtenida a través de la Vigilancia de las comunicaciones se eleva al nivel de Información protegida, la forma, así como el alcance y la duración de la vigilancia son factores relevantes. Debido a que el monitoreo generalizado o sistemático o las técnicas invasivas utilizadas para lograr la Vigilancia de las Comunicaciones tienen la capacidad de revelar información privada muy superior a sus partes constituyentes.
La determinación de si el Estado puede llevar a cabo la Vigilancia de las comunicaciones con respecto a la Información protegida debe ser coherente con los siguientes principios:
"Principio 1: legalidad
Cualquier limitación a los derechos humanos debe ser prescrita por la ley. El Estado no debe adoptar o implementar una medida que interfiera con estos derechos en ausencia de un acto legislativo

disponible públicamente, que cumpla con un estándar de claridad y precisión que sea suficiente para garantizar que las personas tengan un aviso previo y puedan prever su aplicación. Dada la tasa de cambios tecnológicos, las leyes que limitan los derechos humanos deberían estar sujetas a revisiones periódicas mediante un proceso legislativo o reglamentario participativo.

Principio 2: objetivo legítimo
Las leyes solo deberían permitir la vigilancia de las comunicaciones por parte de las autoridades estatales específicas para lograr un objetivo legítimo que corresponda a un interés legal predominantemente importante que es necesario en una sociedad democrática. No se debe aplicar ninguna medida que discrimine por motivos de raza, color, sexo, idioma, religión, opinión política u otra, origen nacional o social, propiedad, nacimiento u otro estado.

Principio 3: Necesidad
Las leyes, reglamentos, actividades, poderes o autoridades de vigilancia deben limitarse a aquellos que sean estricta y demostrablemente necesarios para lograr un objetivo legítimo. La vigilancia de las comunicaciones solo debe llevarse a cabo cuando es el único medio para lograr un objetivo legítimo o, cuando existen múltiples medios, es el medio con menos probabilidades de infringir los derechos humanos. La responsabilidad de establecer esta justificación siempre recae en el Estado.

Principio 4: Adecuación
Cualquier instancia de vigilancia de comunicaciones autorizada por ley debe ser apropiada para cumplir con el objetivo legítimo específico identificado.

Principio 5: Proporcionalidad
La vigilancia de las comunicaciones debe considerarse como un acto altamente intrusivo que interfiere con los derechos humanos que amenazan los cimientos de una sociedad democrática. Las decisiones sobre la vigilancia de las comunicaciones deben tener en

cuenta la sensibilidad de la información a la que se accede y la gravedad de la infracción de los derechos humanos y otros intereses en competencia.

Esto requiere que un Estado, como mínimo, establezca lo siguiente ante una Autoridad Judicial Competente, antes de llevar a cabo la Vigilancia de las Comunicaciones con el propósito de hacer cumplir la ley, proteger la seguridad nacional o recopilar información:

1. existe un alto grado de probabilidad de que se haya llevado a cabo o se lleve a cabo un delito grave o una amenaza específica a un objetivo legítimo; y

2. existe un alto grado de probabilidad de que se obtenga evidencia relevante y material de un delito tan grave o una amenaza específica a un Objetivo legítimo al acceder a la Información protegida buscada; y

3. otras técnicas menos invasivas se han agotado o serían inútiles, de modo que las técnicas utilizadas son la opción menos invasiva; y

4. la información accedida se limitará a lo que sea relevante y material para el delito grave o la amenaza específica a un objetivo legítimo alegado; y

5. cualquier exceso de información recopilada no se retendrá, sino que se destruirá o devolverá de inmediato; y

6. solo la autoridad especificada accederá a la información y la utilizará solo para el propósito y la duración para la que se otorgó la autorización; y

7. que las actividades de vigilancia solicitadas y las técnicas propuestas no socavan la esencia del derecho a la privacidad o de las libertades fundamentales.

Principio 6: autoridad judicial competente

Las determinaciones relacionadas con la vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe ser:

1. separado e independiente de las autoridades que realizan vigilancia de comunicaciones;

2. versado en temas relacionados y competentes para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos; y
3. tener recursos adecuados para ejercer las funciones que se les asignan.

Principio 7: debido proceso
El debido proceso requiere que los Estados respeten y garanticen los derechos humanos de las personas garantizando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos se enumeren adecuadamente en la ley, se practiquen de manera coherente y estén disponibles para el público en general. Específicamente, en la determinación de sus derechos humanos, todos tienen derecho a una audiencia justa y pública en un plazo razonable por un tribunal independiente, competente e imparcial establecido por la ley, excepto en casos de emergencia cuando exista un riesgo inminente de peligro. a la vida humana. En tales casos, la autorización retroactiva debe buscarse dentro de un período de tiempo razonablemente practicable. El mero riesgo de fuga o destrucción de pruebas nunca se considerará suficiente para justificar la autorización retroactiva.

Principio 8: Notificación del usuario
Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificadas de una decisión que autorice la Vigilancia de Comunicaciones con suficiente tiempo e información para permitirles cuestionar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. La demora en la notificación solo se justifica en las siguientes circunstancias:
1. La notificación pondría en grave peligro el propósito para el cual está autorizada la Vigilancia de comunicaciones, o existe un riesgo inminente de peligro para la vida humana; y
2. La autorización para retrasar la notificación es otorgada por una autoridad judicial competente; y

3. El usuario afectado es notificado tan pronto como se levanta el riesgo según lo determine una autoridad judicial competente.
La obligación de dar aviso recae en el Estado, pero los proveedores de servicios de comunicaciones deben tener la libertad de notificar a las personas sobre la Vigilancia de Comunicaciones, de manera voluntaria o previa solicitud.

Principio 9: Transparencia
Los estados deben ser transparentes sobre el uso y el alcance de las leyes, reglamentos, actividades, poderes o autoridades de vigilancia de las comunicaciones. Deben publicar, como mínimo, información agregada sobre el número específico de solicitudes aprobadas y rechazadas, una desagregación de las solicitudes por proveedor de servicios y por autoridad de investigación, tipo y propósito, y el número específico de individuos afectados por cada uno. Los estados deben proporcionar a las personas información suficiente para que puedan comprender completamente el alcance, la naturaleza y la aplicación de las leyes que permiten la Vigilancia de las Comunicaciones. Los Estados no deben interferir con los proveedores de servicios en sus esfuerzos por publicar los procedimientos que aplican al evaluar y cumplir con las solicitudes estatales de Vigilancia de las Comunicaciones, adherirse a esos procedimientos,

Principio 10: supervisión pública
Los Estados deberían establecer mecanismos de supervisión independientes para garantizar la transparencia y la responsabilidad de la vigilancia de las comunicaciones. Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante sobre las acciones del Estado, incluido, cuando corresponda, el acceso a información secreta o clasificada; evaluar si el Estado está haciendo un uso legítimo de sus capacidades legales; evaluar si el Estado ha estado publicando de manera integral y precisa información sobre el uso y el alcance de las técnicas y poderes de Vigilancia de las Comunicaciones de acuerdo con sus obligaciones de Transparencia; publicar informes

periódicos y otra información relevante para la Vigilancia de las Comunicaciones; y hacer determinaciones públicas sobre la legalidad de esas acciones, incluido el grado en que cumplen con estos Principios. Deben establecerse mecanismos de supervisión independientes además de cualquier supervisión ya proporcionada a través de otra rama del gobierno.

Principio 11: Integridad de las comunicaciones y los sistemas.
Con el fin de garantizar la integridad, la seguridad y la privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que comprometer la seguridad con fines estatales casi siempre compromete la seguridad de manera más general, los Estados no deberían obligar a los proveedores de servicios o vendedores de hardware o software a desarrollar capacidades de vigilancia o monitoreo. en sus sistemas, o para recopilar o retener información particular únicamente para fines de Vigilancia de Comunicaciones del Estado. Nunca se debe exigir a los proveedores de servicios la retención o recopilación de datos a priori . Las personas tienen derecho a expresarse anónimamente; Por lo tanto, los Estados deberían abstenerse de obligar a la identificación de los usuarios.

Principio 12: Salvaguardas para la cooperación internacional.
En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar buscar asistencia de proveedores de servicios extranjeros y Estados. En consecuencia, los tratados de asistencia judicial recíproca (MLAT) y otros acuerdos celebrados por los Estados deben garantizar que, cuando las leyes de más de un estado puedan aplicarse a la Vigilancia de las Comunicaciones, se aplique el estándar disponible con el mayor nivel de protección para las personas. Cuando los Estados soliciten asistencia para la aplicación de la ley, debe aplicarse el principio de doble incriminación. Los estados no pueden utilizar los procesos de asistencia legal mutua y las solicitudes extranjeras de información protegida para eludir las restricciones legales nacionales sobre la vigilancia de las comunicaciones. Los procesos de asistencia legal mutua y otros

acuerdos deben estar claramente documentados, disponibles al público,

Principio 13: Salvaguardas contra el acceso ilegítimo y el derecho a un recurso efectivo
Los Estados deberían promulgar leyes que penalicen la vigilancia ilegal de las comunicaciones por parte de actores públicos o privados. La ley debería proporcionar sanciones civiles y penales suficientes y significativas, protecciones para los denunciantes y vías de reparación por parte de los afectados. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como evidencia o de lo contrario no se considera en ningún procedimiento, como lo es cualquier evidencia derivada de dicha información. Los estados también deberían promulgar leyes que establezcan que, después de que el material obtenido a través de la Vigilancia de las Comunicaciones se haya utilizado para el propósito para el cual se proporcionó la información, el material no debe conservarse, sino destruirse o devolverse a los afectados."

La Ley de Seguridad Nacional en su Artículo 30 establece que: "La información sólo podrá ser recabada, compilada, procesada y diseminada con fines de Seguridad Nacional por las instancias autorizadas.

Por su parte el Artículo 34 establece que: "De conformidad con lo dispuesto por el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente Ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional. Se entiende por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología.

Artículo 42.- Los datos que se obtengan de las actividades autorizadas mediante resolución judicial será información reservada que sólo podrá conocer el Director General del Centro, las personas que designe el Consejo y los jueces federales competentes.

Artículo 48.- La información y los materiales de cualquier especie que sean producto de una intervención de comunicaciones privadas autorizadas conforme a las disposiciones de este Capítulo, tendrán invariablemente el carácter de reservados.

Su difusión no autorizada implicará responsabilidad en los términos de la presente Ley, sin perjuicio de lo dispuesto en otros ordenamientos legales aplicables.

Artículo 64.- En ningún caso se divulgará información reservada que, a pesar de no tener vinculación con amenazas a la Seguridad Nacional o con acciones o procedimientos preventivos de las mismas, lesionen la privacidad, la dignidad de las personas o revelen datos personales."

Ahora bien de conformidad con información vertida en medios de comunicación de una investigación de El Diario, se dio a conocer que el Gobierno del Estado de Chihuahua cotizo un equipo tecnológico de espionaje masivo y labores de espionaje, con un costo de aproximadamente 125 millones de pesos. Moneda nacional. Cotización solicitada por el Secretario de Seguridad Pública Estatal y que consta de seis sistemas y soluciones tecnológicas para combatir el terror y el crimen; sin embargo, van incluidas aplicaciones utilizadas en la invasión de cuentas personales de redes sociales y teléfonos celulares, orientadas a la "búsqueda de conexiones sociales, grupos y personas influyentes" y consiste en lo siguiente:

1. *Sistema Activo Zeus como componente principal,*
2. *Software TGR Dashboard,*
3. *Securecube Phonelog,*
4. *Cellebrite Ufed Touch Ultimate Standard,*

5. Cellebrite Ufed Cloud Analyzer y
6. Trapdoor, un conjunto de soluciones tecnológicas que ofrecen, además, "acceso a objetivos con información pública limitada" y mecanismos para "influenciar la opinión pública" o buscar "exposición a audiencias masivas".

Es preocupante que el Ejecutivo pretenda adquirir este tipo de tecnología y sin ningún control, esa responsabilidad de sancionar las malas prácticas en el uso y abuso, en donde el riego en el que se pueda violentar la privacidad de la vida íntima de las personas le corresponde al Poder Judicial y en estricto apego a los principios de necesidad y proporcionalidad, dado que una vigilancia sin ningún control o regulación representa una violación a los derechos de las personas. Así mismo, el incremento en el uso de este tipo de tecnologías y el justificar este tipo de acciones en donde el marco jurídico es obsoleto e inadecuado, permite la intrusión en el derecho a la privacidad. Por lo que se debe asegurar que la vigilancia de las comunicaciones debe de ser licitas que sean necesarias para la salva guarda de la nación, pero deben ser sujetas a las garantías contra los abusos, si no se tiene ningún control se puede violar los derechos de todos los ciudadanos, por ende, el Estado de Derecho..."(SIC)

Ahora bien, al entrar al estudio y análisis de la iniciativa en comento, quienes integramos la Comisión de Seguridad Pública y Protección Civil, formulamos las siguientes:

CONSIDERACIONES

I. Al analizar las facultades competenciales de este Alto Cuerpo Colegiado, quienes integramos esta Comisión de Dictamen Legislativo, no encontramos impedimento alguno para conocer del presente asunto.

II. Como se ha planteado en la iniciativa motivo del presente dictamen, el principal objetivo es exhortar al Ejecutivo del Estado, por medio de la Secretaria de Seguridad Publica para que no adquiera equipos de espionaje y que de esta manera se vulneren los Derechos Humanos.

III. La iniciativa presenta una inquietud sobre el posible espionaje que se pudiera llevar a cabo por el Gobierno del Estado, derivado de la publicación que hace un medio de comunicación con respecto a una aparente cotización para la adquisición de equipo especializado en la materia.

IV. Entendemos la inquietud del iniciador, el conflicto se presenta cuando en su iniciativa hace mención a que esta solicitud no debe de prevalecer en tanto no exista ordenamiento jurídico que regule el uso de este tipo de equipo especializado.

Al respecto es preciso acotar que en el Código Nacional de Procedimientos Penales, en el Artículo 253, Fracción III, indica claramente que sin autorización previa de un juez de control, no se podrá intervenir comunicaciones privadas, por lo que plantea implícitamente que existe la posibilidad de hacerlo y con ello lo

regula, pues también determina en cuales casos se podrá tener la autorización judicial para realizarlo.

De igual forma los artículos 291 al 303 del mismo ordenamiento nacional procedimental en materia penal, aplicable al Estado de Chihuahua, establece toda una serie de lineamientos para la utilización de este tipo de equipos y como se pueden intervenir las comunicaciones privadas.

V. Por su parte la Constitución Federal en el artículo 16, párrafo XII, indica: "*Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*

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. 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. La autoridad judicial federal no podrá otorgar estas autorizaciones 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.

Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indiciados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio."

Por ende, la vulneración a este apartado constitucional y a los lineamientos que establece el Código Nacional de Procedimientos Penales, constituye un delito en el Estado que se conoce como Violación a la Comunicación Privada:

> *"Artículo 327. A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de seis meses a dos años de prisión y de cien a mil días multa.*
>
> *A quien revele, divulgue, utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención*

de comunicación privada, se le impondrán de tres a doce años de prisión y de doscientos a mil días multa."

VI. Así mismo la Ley Federal de Telecomunicaciones y Radiodifusión contempla la posibilidad y obligación de que las compañías de teléfonos deban proporcionar la información necesaria que el Gobierno requiera en determinadas circunstancias, además de ordenar que dichas compañías deberán proporcionar información hasta de dos años atrás, con los fines que legalmente convengan al Estado.

VII. Por último y no menos importante, en el caso del Estado, también existe regulación para la adquisición de equipos especializados, como los mencionados en este documento, con fundamento en el artículo 73 Fracción, IV de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Chihuahua, que autoriza la contratación por adjudicación directa de bienes que "su contratación mediante el procedimiento de licitación pública ponga en riesgo la seguridad pública, en los términos de las leyes de la materia..."

VIII. Por lo tanto esta Comisión considera que la iniciativa se encuentra satisfecha, ya que el Ejecutivo está facultado, a través del órgano competente y mediante los lineamientos jurídicos preestablecidos, intervenir comunicaciones privadas, y si llega a excederse en su actuar, esta sobre limitación guarda una sanción punitiva.

IX. Así pues, en virtud de los considerandos anteriores, esta Comisión somete a la consideración de este Alto Cuerpo Colegiado el siguiente proyecto de:

A C U E R D O

ÚNICO.- La Sexagésima Sexta Legislatura del Honorable Congreso del Estado de Chihuahua, da por satisfecha la iniciativa presentada por el Diputado Omar Bazán Flores, integrante del Grupo Parlamentario del Partido Revolucionario Institucional, que pretendía exhortar al Poder Ejecutivo Estatal, a través de la Secretaría de Seguridad Pública, a fin de que se abstenga de adquirir equipos de espionaje, hasta en tanto existan lineamientos específicos para su utilización. Lo anterior en razón de que ya existen lineamientos para la adquisición y utilización de este tipo de equipos, de acuerdo a lo establecido en la fracción XII, del artículo 16, de la Constitución Política de los Estados Unidos Mexicanos; fracción III, del artículo 253 y los artículos 291 al 303 del Código Nacional de Procedimientos Penales, artículo 327 del Código Penal del Estado de Chihuahua y la fracción IV del artículo 73 de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Chihuahua.

ECONÓMICO.- Aprobado que sea, túrnese a la Secretaría para los efectos legales correspondientes.

Dado en el salón de Sesiones del Honorable Congreso del Estado de Chihuahua, a los 11 días del mes de septiembre de 2020.

H. CONGRESO DEL ESTADO
DE CHIHUAHUA

COMISIÓN DE SEGURIDAD PÚBLICA Y PROTECCIÓN CIVIL
LXVI LEGISLATURA
DCSPPC/026/2020

Así lo aprobó la Comisión de Seguridad Pública y Protección Civil, en reunión de fecha 08 de septiembre de 2020.

	INTEGRANTES	A FAVOR	EN CONTRA	ABSTENCIÓN
	DIP. PRESIDENTA GEORGINA ALEJANDRA BUJANDA RIOS			
	DIP. SECRETARIO DIP. GUSTAVO DE LA ROSA HICKERSON			
	DIP.VOCAL DIP. MARISELA SÁENZ MORIEL			
	DIP. VOCAL DIP. JESÚS VILLARREAL MACÍAS			
	DIP. VOCAL DIP. FERNANDO ÁLVAREZ MONJE			

Nota: La presente hoja de firmas corresponde al Dictamen de la Comisión de Seguridad Pública y Protección Civil, que recae de la iniciativa No. 1909, que busca exhortar al Ejecutivo del Estado, por medio de la Secretaria de Seguridad Publica para que no adquiera equipos de espionaje y que de esta manera se vulneren los Derechos Humanos.