

# UNIVERSIDAD AUTÓNOMA DE TLAXCALA

<b>MIDH</b>	Maestría Interinstitucional en Derechos Humanos
-------------	---

**Los derechos humanos y su relación con las nuevas tecnologías: análisis sobre la influencia que tuvieron las tecnologías de la información y comunicación (TIC) en el ejercicio del derecho a la privacidad y la protección de datos personales de activistas y defensores de derechos humanos en México, durante el sexenio 2012 – 2018.**

Tesis que para obtener el grado de Maestro en Derechos Humanos presenta

**Lic. Guillermo Emmanuel Pérez Ramírez**

Bajo la dirección académica del doctor Federico César Lefranc Weegan

Tlaxcala, Tlaxcala, 26 de Octubre de 2019

## Índice

<b>-Introducción</b> .....	I
Planteamiento del problema.....	I
Justificación.....	III
Hipótesis.....	VII
Delimitación del tema.....	VIII
Metodología.....	IX
Objetivos.....	X
<b>-Capítulo I. Aspectos Generales</b> .....	1
1.1. Cuestiones preliminares.....	1
1.2. Derechos Humanos.....	4
1.2.1 Definición.....	4
1.2.2 Fundamentación.....	7
1.2.2.1 Iusnaturalismo e Iuspositivismo.....	7
1.2.2.2 Nuevas corrientes.....	8
1.3. Tecnologías de la Información y la Comunicación.....	12
1.3.1 Conceptualización.....	12
1.3.1.1 Ciencia y tecnología.....	12
1.3.1.2 TIC.....	17
1.3.1.2.1 Definiciones.....	17
1.3.1.2.2 Características.....	21
<b>-Capítulo II. Derecho a la privacidad y a la protección de los datos personales: regulación y jurisprudencia, internacional y nacional</b> .....	23
2.1. Derecho Internacional.....	23
2.1.1 Europa.....	23
2.1.2 América.....	31
2.2. Derecho Interno.....	35
2.2.1 Regulación sobre las intervenciones a las comunicaciones privadas.....	39
2.2.2 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.....	41

<b>-Capítulo III. Pegasus, aspectos técnico – operativos sobre su uso ilegal en México, 2012 – 2018.....</b>	<b>44</b>
3.1. ¿Qué es Pegasus?.....	44
3.1.1 Sumario.....	44
3.1.2 Cómo funciona Pegasus.....	45
3.2. Cómo Pegasus llegó a México.....	46
3.2.1 Relatoría de hechos.....	46
3.2.1.1 Perfiles.....	47
3.2.1.2 Negociaciones y compra de Pegasus.....	50
3.3 Descripción del uso ilegal de Pegasus en contra de activistas, defensores de derechos humanos y periodistas, 2015 – 2017.....	57
3.3.1 El paciente cero y el descubrimiento de los primeros casos en México.....	58
3.3.2 Uso sistemático del software espía en México, 2015 – 2017.....	62
<b>-Capítulo IV. Discursos.....</b>	<b>71</b>
4.1. Ataques basados en ingeniería social.....	71
4.2 Declaraciones Públicas de autoridades.....	81
4.2.1 Enrique Peña Nieto.....	81
4.2.1.1 Parque Industrial Lagos de Moreno.....	81
4.2.1.2 Obra Línea 3, Guadalajara, Zapopan, Tlaquepaque.....	88
4.3 De la sociedad de la información a la sociedad del conocimiento.....	91
<b>Conclusiones.....</b>	<b>96</b>
<b>Bibliografía.....</b>	<b>i</b>

## INTRODUCCIÓN

### **Planteamiento del problema.**

El rápido e incesante avance científico y tecnológico que han registrado nuestras sociedades durante las últimas décadas ha despertado un sinnúmero de situaciones problemáticas relacionadas al cómo entendemos, comercializamos, usamos y legislamos dichos avances. Los progresos de la ciencia y la tecnología se suceden a una velocidad inusitada para la especie humana, provocando que la aplicación de sus productos se realice sin entender cabalmente sus repercusiones y posibles consecuencias.

El flujo constante de enormes cantidades de información a través de dispositivos tecnológicos al alcance de gran parte de la población mundial parece ser la señal de nuestros tiempos. Las llamadas “tecnologías de la información y la comunicación” (TIC) han abierto un universo de posibilidades para el intercambio, almacenamiento y distribución de datos de toda índole, desde conocimiento académico, hasta información financiera, pasando por el arte y el ocio; tal pareciera que todo se encuentra al alcance de nuestra mano.

Tal aseveración, con todos los beneficios que pudiera implicar, tiene una cara oscura: si yo puedo conseguir lo que quiera con facilidad, entonces, es posible que alguien más pretenda lo que yo tengo. Situación que alcanza connotaciones alarmantes cuando el sujeto que desea la información es el Estado y, lo que quiere, es la información privada de sus ciudadanos. La autoridad, con toda su maquinaria institucional y su monopolio del uso de la fuerza, con el cual persigue y castiga a quien afecta los derechos de los demás, justifica las intromisiones a la esfera de la privacidad de las personas bajo la excusa suprema de la seguridad y el orden social, y si bien, estas acciones pueden y deben estar plenamente reguladas por la autoridad, existe una delgada línea gris que puede conducir al abuso indiscriminado y a conductas ilegales que violan abiertamente los derechos humanos de las personas sometidas a esta vigilancia estatal.

El uso en ascenso de las tecnologías digitales y el intercambio masivo de datos entre la ciudadanía, principalmente a través del internet y los teléfonos móviles, ha abierto una “ventana de interés” para las actividades de vigilancia de los gobiernos, mostrando estos una genuina curiosidad por adquirir o desarrollar capacidades legales y / o tecnológicas que les

permitan obtener la información y datos que alojan o transmiten dichos dispositivos. La Red en Defensa de los Derechos Digitales señala el alcance de estas acciones: “El acceso al contenido de las telecomunicaciones de una persona, así como el análisis de los datos de localización, o el historial de comunicaciones de los usuarios de telecomunicaciones, otorga al Estado un alto poder invasivo y control sobre la persona vigilada”<sup>1</sup>. Este escenario presenta características que podrían llevar a acciones supra legales con consecuencias funestas para grupos de población vulnerables o de particular interés para las autoridades, tal es el caso de los periodistas, activistas y defensores de derechos humanos en nuestro país.

México tiene una larga y nutrida historia de violaciones sistematizadas a los derechos humanos de sus habitantes, incluyendo la vigilancia extrajudicial e ilegítima en contra de objetivos particulares<sup>2</sup>, sin embargo, las intromisiones a la privacidad de ciertos individuos con perfiles bien definidos (a saber, activistas y defensores de derechos humanos) que eran percibidos como problemáticos o conflictivos para ciertos tipos de autoridades, tuvo un punto álgido durante el sexenio del presidente Enrique Peña Nieto, es decir, del 2012 al 2018.

A pesar de existir varias denuncias o unos cuantos ejercicios académicos sobre el tema, este no salto realmente a la luz pública sino hasta el 19 de junio del 2017, cuando el New York Times publicó una nota periodística<sup>3</sup>, firmada por Azam Ahmed y Nicole Perlroth, en la cual se ponía de manifiesto la vigilancia / espionaje electrónico - digital que el gobierno mexicano había realizado a varios periodistas, activistas y defensores de los derechos humanos, así como a sus familiares, a través de un avanzado *software*, comprado a la empresa israelí “NSO Group”, creado originalmente para la investigación criminal y terrorista. El caso se hizo conocido bajo el nombre “Pegasus”, tomado del software utilizado para el espionaje digital.

---

<sup>1</sup> R3D, Red en defensa de los derechos digitales, “*El Estado de la Vigilancia, Fuera de control*”, Ciudad de México, Noviembre de 2016,. Disponible en: <https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016-FINAL1.pdf>, p. 4

<sup>2</sup> Ver: Comisión Interamericana de Derechos Humanos, “*Situación de Derechos Humanos en México*”, Organización de los Estados Americanos, 31 de diciembre de 2015, disponible en: <http://www.oas.org/es/cidh/informes/pdfs/mexico2016-es.pdf>, consultado el 25 de septiembre de 2019.

<sup>3</sup> Ahmed, A. y Perlroth, N. “*Using texts as lures, Government psyware targets mexican journalists and their families*”, New York Times, Nueva York, 19 de junio de 2017, disponible en: <https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html>, consultado el 13 de septiembre de 2019

Los reportajes posteriores a esta nota nos hacen creer que apenas estamos descubriendo la punta del iceberg, la violación a la privacidad y a la protección de datos que representa el espionaje digital abre un amplio campo de análisis, investigación y debate sobre los derechos humanos y su relación con la tecnología, es necesaria una discusión desde diversos frentes y disciplinas para ayudarnos a comprender cabalmente la situación. Determinar la influencia que ejercen las TIC en el ejercicio de los derechos humanos objeto de esta investigación es primordial para posteriormente tomar las mejores medidas para su regulación y aplicación en beneficio ya no sólo de activistas y defensores de los DDHH, sino de toda la población en su conjunto.

### **Justificación.**

Los derechos humanos, tal y como los entendemos ahora, son el resultado de un tiempo, lugar y circunstancias específicas, su génesis se encuentra en la modernidad europea y responden a las necesidades (y demandas) de la sociedad burguesa, teniendo como objetivo principal el imponer límites al poder absoluto que un Estado podía ejercer sobre sus soberanos, es por ello que el primer grupo de derechos humanos en ser reivindicados fueron los llamados derechos civiles y políticos, en los cuales se apelaba a la existencia de ciertas esferas de acción y ejercicio personales que la autoridad no tenía derecho a infringir o atravesar a voluntad. Como estandartes de dichos ideales se encontraban el derecho a la participación política, a la propiedad privada y la privacidad personal.<sup>4</sup>

Como se puede observar, la no intromisión injustificada del gobierno en el ámbito de lo privado se encuentra profundamente enraizada dentro de las premisas fundamentales que dieron origen a los derechos humanos, siendo parte inherente de los mismos, por lo tanto, la pugna por conservar esa libertad negativa sigue tan vigente en estos días como en el albor de los DDHH. Aun así, a pesar de la claridad e influencia de estos ideales, la realidad social y el progreso tecnológico avanzan a tal velocidad que los sistemas jurídicos y las regulaciones legales parecen quedarse rezagadas, desactualizadas e inertes ante las múltiples posibilidades que ofrecen las tecnologías de la información y el conocimiento en nuestro mundo contemporáneo.

---

<sup>4</sup> Peces Barba, G. *Curso de derechos fundamentales. Teoría General*, en Boletín Oficial del Estado, Universidad Carlos III, Madrid, 1995.

Sin embargo, antes de emprender el trabajo regulador del derecho, es de vital importancia el análisis y la ponderación de las distintas manifestaciones, opciones, variables y consecuencias que forman parte de la temática observada. La relación e influencia que tienen las TIC en el ejercicio de los derechos humanos en general, y a la privacidad y la protección de los datos personales en particular, son y serán en los años por venir, objeto de ininidad de discusiones y las conclusiones de las mismas marcaran en gran medida cómo concibamos y actuemos en nuestras relaciones diarias con la autoridad en sociedades cada vez más tecnologizadas, digitales e incluso, virtuales.

A pesar de la relativa novedad de la situación tratada, la relevancia de la misma para el ejercicio del derecho a la privacidad ha provocado que distintas voces, tanto académicas, como periodísticas e incluso institucionales, hayan comenzado a realizar, en los últimos años, investigaciones, estudios o pronunciamientos oficiales sobre la necesidad de analizar y regular el uso que los gobiernos del mundo les están dando a las TIC y sus repercusiones con respecto a sus ciudadanos.

En concordancia con el espíritu de estos tiempos, se debe señalar la gran labor que han ejercido los periodistas y los ciberactivistas en el reconocimiento de la problemática que implican el uso indiscriminado e ilegal de la tecnología con fines de vigilancia y espionaje en detrimento del derecho a la privacidad y la protección de datos personales.

El surgimiento de Wikileaks en diciembre de 2006 de la mano de Julian Assange, suele considerarse el punto de partida de la nueva era del periodismo digital y el surgimiento de los *leaks* o filtraciones extra gubernamentales<sup>5</sup>. Wikileaks se define a sí misma como una organización mediática, multi-nacional enfocada en el análisis y publicación de grandes bases de datos de material gubernamental oficial de carácter confidencial, censurado o restringido al conocimiento público, que involucra temas de guerra, espionaje y /o corrupción<sup>6</sup>. Han sido números “los cables” o filtraciones que dicha organización ha realizado con la temática de la vigilancia ilegal realizada por distintos gobiernos del mundo sobre sus ciudadanos, siendo la divulgación más reciente del 7 de marzo del 2017, relativa a

---

<sup>5</sup> Quian, Alberto “*El impacto político y mediático de Wikileaks*”, Editorial UOC (Oberta OUC Publishing, SL), Barcelona, Abril 2014.

<sup>6</sup> Wikileaks, About, disponible en: <https://wikileaks.org/What-is-WikiLeaks.html>, consultado el 16 de septiembre de 2018

la forma en la cual la Agencia Central de Inteligencia (CIA por sus siglas en inglés) de los Estados Unidos de Norteamérica realiza actividades de espionaje masivo en internet a partir de errores en la programación, para de esta forma infiltrarse en teléfonos móviles, tabletas y ordenadores y así acceder a la información contenida en ellos, ya sean documentos, intercambio de mensajería o la geo-localización en el mundo real<sup>7</sup>.

Comparables a la influencia de las filtraciones de Wikileaks se encuentran las hechas por Edward Snowden, ex técnico informático de la CIA y ex empleado de la Agencia Nacional de Seguridad (NSA por sus siglas en inglés) a los periódicos “The Guardian” y “The Washington Post”, en ellas, Snowden hizo públicas las herramientas que utilizaba el gobierno de los Estados Unidos de Norteamérica para realizar una vigilancia masiva, no solo a sus ciudadanos, sino a personas de todo el mundo, mediante los programas cibernéticos de PRISM y XKeyscore<sup>8</sup>. La información divulgada provocó una enorme convulsión política y social que afectó tanto a Instituciones americanas (el FBI, la NSA, etc.) como las relaciones diplomáticas entre países, por ejemplo, entre los EUA y China o entre el primero y Rusia. Eventualmente Snowden fue acusado por espionaje y robo de propiedad gubernamental, llevándolo a solicitar asilo político en Rusia, donde se encuentra actualmente.<sup>9</sup>

México fue aludido tangencialmente en los cables mencionados, junto a otros países de Latinoamérica, sin embargo, el suceso paradigmático respecto a vigilancia tecnológica – digital en nuestro país es sin duda el del caso *Pegasus* registrado el 19 de Julio de 2017 por el New York Times; en él, el gobierno mexicano fue acusado de usar un software inteligente anti terrorismo (valuado en aproximadamente 80 millones de dólares) para espiar a reconocidos periodistas, activistas y defensores de los derechos humanos, los cuales habían sido muy críticos con respecto a la administración del presidente Enrique Peña Nieto, entre ellos, abogados de los 43 desaparecidos de Ayotzinapa, un economista / activista que ayudó

---

<sup>7</sup> Jiménez Cano, Rosa, “*Así espía la CIA en Internet, según Wikileaks*”, El País, Madrid, 7 de marzo del 2018, disponible en: [https://elpais.com/internacional/2017/03/07/estados\\_unidos/1488902840\\_337837.html](https://elpais.com/internacional/2017/03/07/estados_unidos/1488902840_337837.html), consultado el 16 de septiembre de 2018

<sup>8</sup> Ver: Gellman, B., Blake, A. y Miller G., “*Edward Snowden comes forward as source of NSA leaks*”, The Washington Post, 9 de junio de 2013, disponible en: [https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459\\_story.html?utm\\_term=.84a966e21cf2](https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.84a966e21cf2), consultado el 16 de septiembre de 2018

<sup>9</sup> 20 minutos España y agencia EFE “*Cronología del caso Snowden, el joven que reveló el espionaje masivo de los Estados Unidos*”, 7 de julio de 2013, disponible en: <https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/>, consultado el 17 de septiembre de 2018.

a redactar la ley 3 de 3 (enfocada a la transparencia pública) e incluso a la reconocida periodista Carmen Aristegui, sin olvidar que los intentos de espionaje cibernético no se detuvieron a dichas personas, sino que se hicieron extensivos a sus familiares cercanos. Por otro lado, un nuevo informe realizado por Citizen Lab de la Universidad de Toronto, dado a conocer el 18 de septiembre de 2018, revela que el software espía israelí *Pegasus* continúa activo en México, con al menos 3 operativos en el territorio nacional.<sup>10</sup>

Los organismos internacionales de protección de los derechos humanos también se han pronunciado sobre la relación entre las tecnologías de la información, la vigilancia gubernamental y los derechos humanos. La Asamblea General de las Naciones Unidas ha declarado, en un documentado titulado “El derecho a la privacidad en la era digital”, que “la vigilancia y la interceptación ilegales o arbitrarias de las comunicaciones, así como la recopilación ilegal o arbitraria de datos personales, al constituir actos de intromisión grave, violan el derecho a la privacidad”, de igual forma “*observa con profunda preocupación* que, en muchos países, las personas y las organizaciones dedicadas a promover y defender los derechos humanos y las libertades fundamentales sufren con frecuencia amenazas, acoso e inseguridad, así como injerencias ilegales o arbitrarias en su derecho a la privacidad, como resultado de sus actividades...”<sup>11</sup>. También han existido declaraciones por parte de otros organismos, por ejemplo la “Declaración Conjunta sobre programas de Vigilancia y su Impacto en la Libertad de Expresión” en el 2013, del Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.

El apartado académico e informativo en Latinoamérica sobre el tema es ciertamente limitado, siendo la gran mayoría de los análisis sobre las TIC y los derechos humanos, realizados por grupos de la sociedad civil, por ejemplo, el informe “El estado de la vigilancia, fuera de control”<sup>12</sup> del 2016, hecho por la R3D red en defensa de los derechos digitales, o “El auge

---

<sup>10</sup> Ver: Marczak, B., Scott Railton, J. y otros. “*Hide and seek, tracking NSO Group’s Pegasus Spyware in Operations in 45 Countries*”, Munk School of Global Affairs and Public Policy, Universidad de Toronto, 19 de septiembre de 2018, disponible en: <https://citizenlab.ca/2018/09/hide-and-see-track-nso-groups-pegasus-spyware-to-operations-in-45-countries/>, consultado el 23 de septiembre de 2018

<sup>11</sup> Asamblea de las Naciones Unidas, “*El derecho a la privacidad en la era digital*”, ONU, 31 de octubre de 2016. Disponible en: <http://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf>, consultado el 16 de septiembre de 2018.

<sup>12</sup> R3D red en defensa de los derechos digitales, “*El Estado de la ...*” op. cit.

del software de vigilancia en América Latina”, de la ONG Derechos Digitales América Latina; también cabe mencionar la labor de la Comisión de Derechos Humanos del Distrito Federal, que llegó a dedicarle el número de junio de 2016 de su revista, a la relación entre las nuevas tecnologías y los derechos humanos<sup>13</sup>. Aquí radica la necesidad de comenzar el dialogo académico trans-disciplinar para subsanar el rezago que sufre nuestro país con respecto a la problemática.

## **Hipótesis**

Las tecnologías de la información y comunicación ejercieron una doble influencia en el desempeño del derecho a la privacidad y la protección de los datos personales de los activistas y defensores de los derechos humanos en México durante el sexenio 2012 - 2018, este efecto doble de las TIC consistió, por un lado, en una influencia de carácter negativa, la cual fungió como limitante a los derechos humanos arriba aludidos, colocándoles obstáculos importantes para su realización y, bajo ciertas circunstancias, ayudaban a violarlos flagrantemente. Al inverso, existía una influencia de índole positiva, la cual servía como potenciadora del disfrute del derecho a la privacidad y la protección de datos personales, esto mediante el uso de herramientas tecnológicas que fortalecían los aspectos vulnerables de dichos derechos y complicaban su transgresión a las autoridades. Debido a la naturaleza cambiante de las TIC y sus cualidades transitorias, los dos tipos de influencia no son mutuamente excluyentes, pudiendo convivir en un mismo caso, e incluso, en un mismo dispositivo.

La situación social de violaciones sistematizada de derechos humanos en el país durante el sexenio de Enrique Peña Nieto<sup>14</sup>, intervino en la forma en la que se percibió la influencia que ejercieron las TIC en el ejercicio del derecho a la privacidad y la protección de datos por parte del grupo de población analizado en este escrito, ya que en un país donde la desaparición forzada, la tortura y el abuso militar son comunes, las violaciones a los derechos digitales son minimizadas, incluso por quienes las sufren.

---

<sup>13</sup> Comisión de los Derechos Humanos del Distrito Federal, “Defensor, El uso de las nuevas tecnologías y los derechos humanos”, Ciudad de México, Junio de 2016, disponible en: [https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor\\_06\\_2016.pdf](https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf)

<sup>14</sup> Guevara Rosas, Erika, “Enrique Peña Nieto. El recuento de los daños”, Amnistía Internacional Américas, 30 de noviembre de 2018, disponible en: <https://www.amnesty.org/es/latest/news/2018/11/enrique-pena-nieto-el-recuento-de-los-danos/>, consultado el 25 de septiembre de 2019.

El conocimiento y desarrollo técnico-científico y económico que tiene un país (o región dentro del mismo), determina la conceptualización, percepción e identificación de la influencia que realizan las TIC sobre los derechos aquí analizados.

La intromisión arbitraria a la esfera de lo privado por parte de las autoridades, en el caso de los activistas y defensores de derechos humanos, siempre tuvo un fin político, ya sea para la consecución de información social relevante la cual estaba en posesión de la víctima, o para la desacreditación laboral y/o personal de la misma, en aras de frenar su actuación contraria a los fines del gobierno.

Es posible resumir las hipótesis de la siguiente forma:

-Si el estado mexicano cataloga a algún activista como potencial amenaza a sus intereses, entonces utilizará a las TIC para espiarlo digitalmente con algún fin político o de descrédito.

-Si las autoridades desean obtener información sobre un objetivo de la sociedad civil intentaran adquirir esa información mediante la intervención de las comunicaciones privadas de dicha persona, aprovechando debilidades tecnológicas en las TIC

-Si el contexto social de los derechos humanos en el país es percibido como en estado de crisis, entonces cambiará la percepción sobre la importancia de las TIC en el derecho a la privacidad.

### **Delimitación del tema: (geográfico – temporal)**

La delimitación del tema en este proyecto de investigación es clara, los casos analizados y la información referente a los mismos estarán contenidos dentro del territorio de la República Mexicana, durante el periodo de gobierno del presidente Enrique Peña Nieto, es decir, del 1 de diciembre de 2012 al 30 de Noviembre de 2018.

Ahora bien, en un primer momento podría parecer que el territorio por abarcar es amplio, por lo tanto conviene matizar dicha aseveración. Con la información que se dispone al momento de realizar este protocolo de tesis (noviembre de 2018), los casos con mayor certidumbre y de los cuales se cuenta con material probatorio corresponden a los del caso “*Pegasus*” (4), sucedidos en su gran mayoría en el área centro / metropolitana de México. El conocimiento y revelación de nuevas circunstancias o hechos relacionados a ese software (o con antecedes

directos al mismo) se suceden con el transcurso de los meses, mostrando enlaces o casos en los estados de Guerrero y Veracruz. El paso del tiempo va mostrando a la luz pública nueva información que podría arrojar elementos importante para este proyecto, por lo tanto, se apela a todo el territorio nacional para recabar mayores datos sobre un tema que, por ahora, da restringidos elementos concretos, pero que apunta a un cúmulo trascendente aún por revelarse.

### **Metodología (métodos generales)**

Para la presente tesis se plantea una investigación principalmente de índole cualitativa, dado que las reflexiones culturales, deducciones, razonamiento y establecimiento de relaciones, inician y se desarrollan a partir de las cualidades particulares del objeto de estudio de este escrito, sin embargo, debido al carácter técnico – tecnológico del mismo y a algunas de sus repercusiones observadas en primera instancia, será necesario retomar ciertos elementos de la investigación cuantitativa que ayudaran a dilucidar aspectos importantes sobre la situación analizada, a saber, el nivel de alcance en la población estudiada (concreto, e incluso potencial) y la cantidad de datos / información que ha obtenido sobre las personas víctimas del espionaje tecnológico.

Respecto al abordaje, éste será desde el análisis crítico del discurso en la vertiente de Teun Van Dijk, quien define este método como un “tipo de investigación analítica (...) que estudia primariamente el modo en que el abuso del poder social, el dominio y la desigualdad son practicados reproducidos, y ocasionalmente combatidos, por los textos y el habla en el contexto social y político (...) El ACD tiene sus correspondiente equivalencias en los desarrollos <<críticos>> de la psicología y de las ciencias sociales”,<sup>15</sup> en concordancia, el método crítico retomará elementos provenientes de la psicología social, particularmente del análisis sobre la persuasión, en este caso “los componentes desagregados del proceso comunicativo: emisor y receptor”, son vistos desde una interioridad mediacional psicológica qué permite argumentar las posibilidades de control y cambio de las personas. (...) en el

---

<sup>15</sup> Van Dijk, Teun, “El análisis crítico del discurso”, en *Anthropos*, Barcelona, 189, septiembre – octubre de 1999, p. 23

terreno del cambio actitudinal, como efecto de los mensajes que se emiten, justamente con esa intención”<sup>16</sup>

Para los métodos relacionados a las fuentes, se programa un modelo de investigación bibliográfica, en la cual, el primer paso consistirá en la recolección de la información a partir de diversas fuentes documentales, principalmente académicas y periodísticas, así como de los informes y estadísticas oficiales proporcionados por el gobierno mexicano; después se llevará a cabo la selección, análisis y reflexión de dichos materiales consultados. Ya que se busca la mejor calidad y fiabilidad de la información recabada y de las premisas que de estas se desprendan, se aplicará también un método comparativo entre las distintas fuentes y testimonios obtenidos.

### **Objetivos:**

#### *General.*

Analizar y determinar la influencia que ejercieron las tecnologías de la información y comunicación (TIC) en el desempeño efectivo del derecho a la privacidad y la protección de datos personales de activistas y defensores de derechos humanos en México, durante el sexenio de Enrique Peña Nieto (2012- 2018).

#### *Específicos.*

- Analizar la doble función de las TIC en el ejercicio del derecho a la privacidad: potenciadora y restrictiva
- Señalar la situación legal actual sobre la regulación de las TIC y su uso por parte de las autoridades
- Determinar cómo el contexto actual sobre violaciones a los derechos humanos en el país influyó en el uso y finalidad de las TIC por parte del gobierno mexicano

---

<sup>16</sup> Bautista López, Angélica, “Comunicación social”, en Arciga Bernal, S.; Juárez Romero, J.; Mendoza García J. (Coords.) *Introducción a la psicología social*, Universidad Autónoma Metropolitana, México 2013, p. 239

## CAPITULO I: ASPECTOS GENERALES

### 1.1. Cuestiones preliminares

La palabra *persona* tiene su origen en el arte romano del siglo I antes de Cristo, específicamente nace en medio de las representaciones teatrales<sup>17</sup>. Los actores romanos retomaron la costumbre que tenían los griegos de salir al escenario, cubierto el rostro, con una máscara. Dicho accesorio cumplía una doble función: primero, era una manifestación física que ayudaba a representar lo que actualmente llamamos el *personaje*, el papel que el actor desempeña en la obra; segundo, permitía amplificar el sonido de la voz humana debido a la forma en la que el aditamento estaba diseñado y construido. Gracias a esto, la limitada voz de un individuo en el escenario podía expandirse por el anfiteatro y ser escuchada por todo el público.

La mascarada usada por esos actores fue llamada *persona*, del latín, *per sonare*, *sonar a través de*, y ha pasado de esa forma primigenia hasta su significado actual. Los seres humanos seguimos siendo los actores en medio de la gran representación del mundo, y para interpretar nuestros papeles, aún nos valemos de creaciones artificiales para mejorar nuestro desempeño, sólo que nuestra máscara ahora es digital y está construida con cables, microchips, y electricidad. Los medios para magnificar nuestras voces y que éstas sean escuchadas por todo el mundo ya no se basan en cajas de resonancia, sino en aparatos electrónicos interconectados unos a otros durante todo el día, el zumbido en masa de esta conectividad es lo que llena ahora nuestro particular anfiteatro. La única diferencia estriba en que la delgada línea entre público y actores parece difuminarse estos días, ya un momento nos toca ocupar la palestra y ser los protagonistas de la conversación, para después regresar a nuestros asientos y pacientemente recibir la información que los otros envían, transmiten a través del aire electrificado hasta nosotros. Así, una y otra vez, el intercambio de información, de datos, marca nuestra cotidianidad. Yo para todos, todos para mí.

La relación que los seres humanos han tenido con sus creaciones de índole técnico se remonta a los albores mismos de su historia, “podría decirse que el día que se manifestó por primera

---

<sup>17</sup> Velázquez, José M., “*Curso elemental de psicología*”, Compañía General de Ediciones, S.A., Vigésima octava edición, México D.F., 1980, p. 383.

vez en los antropoides un gesto técnico, aquel día nació el que hoy llamamos hombre”<sup>18</sup>; ya Sigmund Freud hacía mención a esta peculiar unión, originada en la necesidad de compensar la fragilidad física con la cual el hombre llega al mundo: “con las herramientas, el hombre perfecciona sus órganos -tanto los motores como los sensoriales – o elimina las barreras que se oponen a su acción”<sup>19</sup>. Los lentes corrigen los desperfectos de nuestra visión, los telescopios y microscopios la mejoran, nos llevan a ver cosas que naturalmente nos estarían veladas: estrellas a años luz de distancias, infinidad de microorganismos que pululan en nuestros cuerpos. Palancas, poleas, motores nos proporcionan fuerza para modificar el escenario natural y adaptarlo a nuestras necesidades. Las máscaras de los griegos y los romanos permitieron que nuestras voces fueran escuchadas por decenas, tal vez cientos de personas, ahora los *smartphones*, computadoras, *tablets* y demás medios electrónicos cumplen esa función, pero con una intensidad aún mayor.

Durante su proceso evolutivo, la humanidad tuvo que competir contra grupos de animales mejor adaptados biológicamente a su entorno, sin embargo, nuestra especie tuvo un cúmulo de progresos únicos entre todos sus competidores que permitieron su subsistencia<sup>20</sup>, dos particularmente: 1) la liberación de las manos de la función propia de la locomoción, con la cual éstas se fortalecieron y pudieron afinar su eficacia en el manejo de herramientas; y 2) El desarrollo del cerebro, con lo cual se complejizó e hizo más lúcido y rápido en la toma de decisiones. Estas dos circunstancias devinieron en el empleo de armas artificiales para la caza y la defensa, su extraordinaria eficacia supuso el cambio paradigmático. El avance continuó, del empleo de herramientas se pasó a la confección y perfeccionamiento de las mismas.

Ciertamente, los seres humanos no son las únicas criaturas que se valen de instrumentos, sin ir más lejos, existen ejemplos claros de fabricación y utilización de estos en nuestros parientes más cercanos a la especie: los monos y los grandes simios. Sin embargo, “aunque los primates son lo bastante <<inteligentes>> como para utilizar utensilios, su anatomía y modo normal de existencia les impiden desarrollar amplias tradiciones de utilización de utensilios”<sup>21</sup>. El constante desarrollo de nuestra relación con la técnica y sus productos ha sido el punto de

---

<sup>18</sup> Galimberti, Umberto, “*Los mitos de nuestro tiempo*”, Debate, Barcelona, 2013, p. 231.

<sup>19</sup> Freud, Sigmund, “*El malestar en la cultura*”, Alianza Editorial, tercera edición, Madrid, 2013, pp. 88 – 89.

<sup>20</sup> Morris, Desmond, “*El mono desnudo. Un estudio del animal humano*”, Plaza & Jané, Barcelona, 1973, pp. 10 -12.

<sup>21</sup> Harris, Marvin, “*Antropología Cultural*”, Alianza Editorial, Tercera edición, Madrid, 2011. P.52

toque no sólo para asegurar nuestra supervivencia en este mundo, sino que ha venido a ser parte fundamental de nuestra misma esencia como seres.

Ahora bien, que la relación humano-técnica/herramienta este fuertemente afianzada en nuestra historia, no significa que la técnica sea el aspecto o elemento definitorio de la humanidad. Así se expresa Lefranc Weegan al respecto:

“Las manifestaciones técnicas no definen al ser humano sino el momento histórico. La rueda, la máquina de vapor, las naves espaciales o la telefonía celular no han transformado en realidad al ser humano.

Es decir, la capacidad técnica caracteriza al ser humano pero no lo determina; no somos los seres del espacio, como no fuimos antes los autómatas mecánicos”<sup>22</sup>

Lo humano sobrepasa la esfera de lo simplemente técnico, no es posible reducir la experiencia humana a los aportes que vienen de ese campo. Es innegable su contribución para facilitar nuestras vidas y otorgarnos mayor confort<sup>23</sup>, pero sería un error ponerlas como la única solución a todos nuestros problemas y encumbrarlas en el centro de nuestra existencia. La unión humano-técnica está lejos de ser armoniosa, y de hecho, en muchos casos es fuente de conflicto para nosotros. Retomando a Freud: “El hombre ha llegado a ser, por así decirlo, un dios con prótesis: bastante magnífico cuando se coloca todos sus artefactos, pero éstos no crecen de su cuerpo y a veces aun le procuran muchos sinsabores”<sup>24</sup>. El diálogo y la fascinación que los seres humanos hemos tenido con nuestras creaciones técnicas es complejo y con múltiples capas. Nuestras necesidades y anhelos son muchos, inmensos, y por más que desarrollemos paliativos o vías para subsanarlos, estas parecen insuficientes en algún momento.

Es en este punto, en el surgimiento del conflicto entre persona y técnica, que se inscriben las primeras líneas de este trabajo de investigación. La modernidad y el positivismo enarbolaron a la ciencia objetiva y al progreso técnico como los caminos auténticos para la culminación y satisfacción de todos los deseos “del hombre”, sin embargo, cuando esas promesas no se

---

<sup>22</sup> Lefranc Weegan, Federico, “Los sujetos de la SIC”, en *Derecho y TIC. Vertientes actuales*, UNAM, Instituto de Investigaciones Jurídicas, México, 2016, p. 36. Disponible en: <https://biblio.juridicas.unam.mx/bjv/detalle-libro/4065-derecho-y-tic-vertientes-actuales>, consultado el 2 de diciembre, 2018.

<sup>23</sup> Markus, Gabriel, “¿Por qué no existe el mundo?”, Océano Editorial, México D.F., 2016.

<sup>24</sup> Freud, op. cit, p. 90

cumplieron, llegó el inevitable desencanto ante este proyecto y sus premisas. A ese desencanto solemos llamarlo posmodernidad<sup>25</sup>. Sin embargo, la desilusión no fue repentina y rotunda. Cuando la tecnología digital, el internet y la inteligencia artificial se mostraron como los nuevos medios para resolver los grandes problemas del mundo contemporáneo, grupos de la sociedad celebraron su llegada<sup>26</sup>. La democracia, el pluralismo y el respeto a la persona se deban por sentado en esta realidad digital y globalizada. Naturalmente, este ambiente utópico no tardo en presentar fracturas<sup>27</sup>. Con este escenario llega el momento de agregar el tercer elemento a nuestro análisis: los derechos humanos. Podemos, a partir de este momento, hablar de una triada sobre la cual versaran los apartados siguientes: la relación persona, tecnología y derechos humanos. Definida la ecuación, materializada en la influencia de las TIC en el ejercicio del derecho a la privacidad, corresponde ahora la conceptualización de sus elementos clave.

## 1.2 Derechos humanos

### 1.2.1. Definición.

Partamos de un postulado simple, pero que en su aparente obviedad, esconde la esencia de varios de los contenidos de este escrito, a saber, que los derechos humanos, al igual que la ciencia y la tecnología, son constructos sociales, sólo que difieren, ocasionalmente, en sus fines. Los DDHH responden a los ideales y exigencias del concepto de dignidad que las sociedades humanas hacen en un tiempo y espacio determinado. En cuanto construcción humana, son resultado de un proceso artificial que no surgió espontáneamente del mundo natural. Es por ello que resulta significativa la afirmación de Agustín Squella de que, al hablar de los derechos humanos, lo hacemos “de una construcción, no de un hallazgo”<sup>28</sup>. Esta creación humana es pasmosamente reciente, “la significativa mayor parte de la historia no conoció los derechos humanos. La significativa mayor parte de los individuos que han vivido

---

<sup>25</sup> Consante, Alberto, “La memoria perdida de las cosas (crítica a la modernidad)”, en *Claves del pensamiento*, Vol. 1, No. 1, Scielo, México, 2007, Disponible en: [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S1870-879X2007000100005](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-879X2007000100005), consultada el 16 de marzo de 2019

<sup>26</sup> Ackoff L., Russel, “*Rediseñando el futuro*”, Limusa, México D.F., 2012.

<sup>27</sup> Byung-Chan, Han, “*La sociedad del cansancio*”, Herder, Barcelona, 2012.

<sup>28</sup> Squella Agustín y López Calera Nicolás, “*Derechos Humanos ¿invento o descubrimiento?*”, 1ra. Ed, Fundación Coloquio Jurídico Europeo, Madrid, 2010, p. 67

en este planeta, no disfrutó de los derechos humanos”<sup>29</sup>. El tomar conciencia del significado de dicha circunstancia nos coloca en una posición más adecuada para entender la conceptualización de los DDHH y su peculiar evolución. Recuperemos tres definiciones de derechos humanos para comenzar a hilar su núcleo conceptual, características y funcionamiento.

El Instituto de Investigaciones Jurídicas de la UNAM en su *Diccionario Jurídico Mexicano* nos dice que “los derechos humanos son el conjunto de facultades, prerrogativas, libertades y pretensiones de carácter civil, político, económico, social y cultural, incluidos los recursos y mecanismos de garantía de todas ellas, que se reconocen al ser humano, considerado individual y colectivamente”<sup>30</sup>

Por su parte, la UNESCO nos menciona que el objetivo de los derechos humanos es “la protección institucionalizada de los derechos de la persona humana contra los excesos del poder cometidos por los órganos del Estado, y el de promover paralelamente el establecimiento de condiciones humanas de vida, así como el desarrollo multidimensional de la personalidad humana”<sup>31</sup>. Destaco en esta aproximación la mención a que los DDHH, más allá de ser un instrumento jurídico para tutelar derechos fundamentales, buscan también la reproducción y establecimiento de un modelo de concebir al ser humano y la forma en la que este debe relacionarse con su pares y habitar el mundo. La contrastación de este discurso frente al de la ciencia en general, y de la tecnología en particular, es punto central en el análisis que se desarrollará a lo largo de estas líneas.

Para Pérez Luño estos derechos “[...] suelen venir entendidos como un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional”<sup>32</sup>. Dicha definición menciona tres elementos que se manifestaran de manera continua los cuales son: 1) momento

---

<sup>29</sup> *Ibíd.*, p. 77

<sup>30</sup> Rodríguez y Rodríguez, Jesús, *Dic. Juri. Mex.*, Tomo III, México 1983, p 223.

<sup>31</sup> UNESCO, *Les dimensions internationales des droits de l'homme*. Publicado por UNESCO, 1978, p.11, según cita de Alemany Verdaguer, Salvador, *Curso de derechos humanos*, 1a. ed., Bosch, Casa Editorial, S.A., España, 1984, p. 15.

<sup>32</sup> Pérez Luño, Antonio E., *“Los derechos fundamentales”*, 2a. ed., Tecnos, España, 1986, p. 46.

histórico concreto, 2) exigencias respecto a la dignidad, la libertad y la igualdad, y 3) reconocimiento positivo en los ordenamientos jurídicos. Respecto al punto número dos, conviene mencionar que los principios de dignidad, libertad e igualdad son los pilares sobre los cuales se sustentan los derechos humanos, aunque en ocasiones suele mencionarse primordialmente a la dignidad dado que esta recoge en su seno a las otras dos. Por ello, ya Villán Durán fundamentaba la existencia del Derecho Internacional de los Derechos Humanos en la dignidad del ser humano, dado que “es la única idea-fuerza que aglutina las diferentes concepciones culturales, filosóficas, políticas, ideológicas, religiosas, morales y sociales presentes en el mundo contemporáneo”<sup>33</sup>.

Respecto al concepto mismo de dignidad, la académica de la Universidad Nacional Autónoma de México, la Dra. Ariadna Estévez López, hace mención a que si bien la dignidad ha estado *impregnada* de cierto matiz o fondo metafísico, debe definirse “de acuerdo con el contexto histórico y territorial, y con componentes lo mismo axiológicos que materiales y culturales, por lo que aquellos derechos que garantizaban la dignidad de las personas en alguna época particular, no son necesariamente los mismos en el tiempo presente o en el futuro”<sup>34</sup>. La aseveración anterior reafirma la importancia del elemento contextual que subyace en los derechos humanos, es decir, su contenido y su forma son el resultado de un proceso social, que tiene un espacio, lugares y circunstancias (políticas, económicas, sociales) específicas, las cuales son susceptibles de cambios a lo largo del tiempo, ello a su vez implica que “no existen derechos fijos en el tiempo y el espacio”<sup>35</sup>.

Ahora bien, el postulado anterior también debe analizarse en su debido tenor para no caer en interpretaciones equívocas y una especie de relativismo con el cual se afirme que los derechos humanos son un constructo endeble y por lo tanto falto de legitimidad para defender la dignidad de los seres humanos. Por el contrario, la riqueza de elementos históricos, culturales, técnicos y sociales que nos da el análisis contextual de la fundamentación de los

---

<sup>33</sup> Villás Duran, Carlos “El derecho internacional de los derechos humanos” en *Curso de Derecho Internacional de los derechos humanos*, Editorial Trotta, Madrid España, 2002

<sup>34</sup> Estévez López, Ariadna, “*Los derechos humanos*”, disponible en: [http://www.academia.edu/25038679/Derechos\\_humanos](http://www.academia.edu/25038679/Derechos_humanos) consultado el 9 de noviembre, 2018

<sup>35</sup> *Ibidem*

derechos humanos nos acercan a una cosmovisión más grande, más fuerte y más *humana* de este esfuerzo colectivo para asegurar una vida digna a todas las personas<sup>36</sup>.

### 1.2.2. *Fundamentación.*

#### 1.2.2.1 Iusnaturalismo e Iuspositivismo

Las dos corrientes principales en la fundamentación de los derechos humanos, son antagónicas en una primera instancia, el iusnaturalismo y el iuspositivismo sirven a manera de arquetipos sobre los cuales se irán desarrollando posturas más elaboradas que posteriormente abogarán por puntos intermedios e ideas mixtas. Históricamente, el iusnaturalismo es el primero en surgir, con raíces que se remontan al derecho natural, la escuela filosófica escolástica de la Edad Media e incluso más atrás, en la filosofía griega clásica<sup>37</sup>. Es una primera aproximación y justificación a la idea de los derechos humanos, concepto que aún no ostenta tal nombre, pero que da sus primeros pasos para asentarse.

Para Labrada Rubio, dentro del iusnaturalismo los fundamentos de los derechos humanos “no se encuentran en la ley positiva, sino en la naturaleza del hombre, en su razón o en otra realidad superior a la ley positiva humana”<sup>38</sup>. Para contextualizar lo que Labrada Rubio expone es conveniente mencionar que esta corriente suele dividirse en dos vertientes principales: el iusnaturalismo clásico y el iusnaturalismo racionalista; el primero parte más bien de la creencia en la existencia de una ley natural, de un *orden natural de las cosas* en concordancia con el pensamiento judeo-cristiano, “el iusnaturalismo medieval puede resumirse en un enorme y sostenido esfuerzo (...) por cohonstar el plano natural y el sobrenatural”<sup>39</sup>; por otro lado el iusnaturalismo racionalista busca el fundamento ya no en una dimensión supra-humana sino que lo coloca en la razón humana misma. John Locke

---

<sup>36</sup> Serrano, Sandra y Vázquez, Daniel, “*Fundamentos Teóricos de los Derechos Humanos*” Comisión de Derechos Humanos del Distrito Federal, México, D.F., s.f. p. 217. Disponible en: [https://cdhdf.org.mx/serv\\_prof/pdf/fundamentosteoricosdelosderechos.pdf](https://cdhdf.org.mx/serv_prof/pdf/fundamentosteoricosdelosderechos.pdf), consultada 10 de diciembre de 2018.

<sup>37</sup> Soriano Flores, Jesús, “*Elementos históricos y jurídicos para la conceptualización contemporánea de los derechos humanos*”, Anuario de Derechos Humanos del Instituto de la Judicatura Federal, México, 2017, p. 369 - 370

<sup>38</sup> Labrada Rubio, Valle, “*Introducción a la teoría de los derechos humanos: fundamento, historia, Declaración Universal*” de 10.XII.1948, 1a. edición, Civitas, S.A., España, 1998

<sup>39</sup> Muñoz de Baena, José Luis, “Fundamentos filosóficos de los derechos humanos” en *Pasado, presente y futuro de los derechos humanos*, Comisión Nacional de los Derechos Humanos, México, 2004.

junto a la teoría del contrato social son dos de los elementos principales en la postura racionalista<sup>40</sup>.

El iuspositivismo aparece como una reacción a estas concepciones, en cierta forma buscando la expulsión del apartado metafísico en el derecho<sup>41</sup>. Para los partidarios de esta corriente sólo se puede hablar de derechos cuando estos se encuentran plasmados y reconocidos en una norma jurídica positiva. Hablamos de una concepción vehementemente materialista del derecho, en tanto que niega toda posibilidad de derechos que no se encuentren reconocidos como tales en un ordenamiento jurídico. El positivismo jurídico se enraizó en el pensamiento occidental durante el siglo XIX, época que asistió a la gestación de las grandes codificaciones en el ámbito europeo y norteamericano<sup>42</sup>.

El iusnaturalismo y el iuspositivismo fueron durante varios años las dos vías principales para justificar y fundamentar los DDHH, sin embargo, con el paso del tiempo los modelos clásicos fueron incapaces de respuestas a sociedades en crisis, abriendo la puerta a nuevos esquemas, en palabras de José Martínez de Pisón: “[el] ocaso y fracaso de las fundamentaciones absolutas o “fuertes” en relación a los derechos del hombre (..) ha abierto una vía a otro tipo de justificaciones que insisten más en los elementos discursivos, consensuales o procedimentales.”<sup>43</sup>. El siguiente apartado está dedicado a la exposición de estas posturas.

#### 1.2.2.2 Nuevas Corrientes

Tal vez nada hable mejor de una crisis (y las posibilidades que eso conlleva) que cuando se duda de la necesidad de justificar aquello que está en trance. Norberto Bobbio puso sobre la mesa si en realidad era importante fundamentar los derechos humanos. Antes de él ya habían existido críticas a las fundamentaciones clásicas, proveniente, por ejemplo, de Karl Marx o Jeremy Bentham<sup>44</sup>, pero tal pareciera que se daba por sentado la *necesidad* de una

---

<sup>40</sup> Locke considera que los seres humanos se reúnen en sociedad para defender más fácilmente sus derechos naturales. Ver: Locke, John, “*Ensayo sobre el gobierno civil*”, Ediciones Nuevo Mar, México D.F., 1984

<sup>41</sup> Muñoz Baena, “*Fundamentos filosóficos...*” op. cit. P. 113

<sup>42</sup> Ídem.

<sup>43</sup> Martínez de Pisón, José, “*Derechos Humanos. Un ensayo sobre su historia, su fundamento y su realidad*”, editorial Egido, 1997

<sup>44</sup> Cruz Parceros, Juan A., “Crisis de la Fundamentación de los Derechos Humanos en el siglo XIX”, en Margarita Moreno-Bonnett y María del refugio (Coords.), *La Génesis de los derechos humanos en México*, Universidad Nacional Autónoma de México, México, D.F., 2006.

fundamentación, ahora Bobbio, daba la vuelta a la cuestión en 1964 durante su conferencia titulada “Sobre el fundamento de los derechos del hombre” en donde manifestaba que: “el problema de fondo relativo a los derechos del hombre es hoy no tanto el de justificarlos, como el de protegerlos”<sup>45</sup>, el problema del fundamento de los derechos humanos terminó, o mejor dicho, tuvo su *solución* cuando la Asamblea General de las Naciones Unidas aprobó la Declaración Universal de los Derechos Humanos en 1948, es decir el problema ya no recaer en justificar los DDHH, sino en garantizarlos de la forma adecuada.

Ciertamente la afirmación de Bobbio contiene elementos incuestionables (la importancia primordial que supone la correcta garantía de nuestros derechos humanos), sin embargo, también tiene un dejo de provocación e instigación, la cual despertó la necesidad de encontrar nuevos fundamentos acordes a los tiempos que corrían. El mismo Bobbio ya esboza su particular visión al decir que “hablar sobre la fundamentación de los derechos humanos, no depende de algo objetivo, sino del consenso al que intersubjetivamente se llegue”<sup>46</sup>. Como ya mencionaba Martínez de Pisón, una gran parte de las nuevas fundamentaciones de los derechos humanos tiene en la idea del consenso una de sus cartas principales. Esta postura va más allá de intentar una fundamentación absoluta y total, por el contrario acepta que los derechos humanos son una creación humana en la que grupos sociales han acordado que es necesaria su existencia a partir de ciertos parámetros y requerimientos establecidos por ellos mismos.

En una primera instancia se puede establecer cierto paralelismo entre la idea del consenso y la teoría del contrato social, en esencia ambas se refieren a un acuerdo entre los miembros de un grupo humano, la diferencia estriba en el alcance de dicho acuerdo. Bidart Campos arroja cierta luz en este caso cuando habla de una fundamentación empírica o pragmática de los DDHH y de la cual dice: “este fundamento ofrece dos caras: una nos muestra que él radica en la necesidad preocupante de tutelar al hombre frente al Estado y a sus semejantes para

---

<sup>45</sup> Bobbio, Norberto, “*El tiempo de los derechos*”, Editorial Sistema, Madrid, 1996, p. 61

<sup>46</sup> Bobbio, Norberto, “Su fundamento dei diritti dell uomo”, *Il Problema della guerra e le vie della pace*, Bologna, Il Mulino, 1979. P.121 Traducción: Javier Saldaña.

sacarlo de la indefensión y de la amenaza, otra nos muestra que el sustento reside nada más en el consenso social en torno a los derechos”<sup>47</sup>.

Dentro de estas vertientes nuevas, Vidaurri Aréchiga y Soriano Flores hacen mención a una corriente historicista o de fundamentación histórica<sup>48</sup>, la cual emparenta con el camino que sea ha venido trazando. Retomando a Bidart Campos, este modelo se distingue al decir que “es la historicidad de los derechos, desconectándolos de cualquier clase de fundamentación en la naturaleza, por más lejana que sea, cree que el único fundamento de los derechos –muy relativo y circunstancial por cierto- es su aceptación histórica”<sup>49</sup>. Si bien el énfasis se coloca en el apartado histórico de los derechos, existen dos puntos que resaltar: 1) al igual que las posturas anteriores, esta visión se aparta de las fundamentaciones clásicas en la naturaleza, es decir las visiones absolutas, y 2) la historia también es un producto del pensamiento humano y por ello mismo se ha llegado a un acuerdo común para definirla y conceptualizarla de cierta manera, por ello, si aceptamos el fundamento historicista, también se acepta tácitamente el consenso social que ha determinado y valorado ese trayecto histórico específico.

Finalmente, hay un señalamiento en el postulado de Bidart que merece un comentario especial: el autor al momento de mencionar que el único fundamento de los derechos se encuentra en su aceptación histórica, remarca que ese fundamento es “muy relativo y circunstancial”; el relativismo es un concepto que suele atribuirse al discurso de la “posmodernidad”, al igual que la negación o el desuso de concepciones absolutas respecto a la realidad o la sociedad contemporánea<sup>50</sup>. Si seguimos el modelo propuesto en este escrito, resulta de lo más natural que las explicaciones y justificaciones relacionadas a los derechos humanos se alimenten de las diversas manifestaciones ideológicas, culturales y/o científicas que permean el contexto particular en el cual se dan estas cavilaciones, sin embargo, la

---

<sup>47</sup> Bidart Campos, Germán J., *“Teoría general de los derechos humanos”*, 2ª reimpresión, Instituto de Investigaciones Jurídicas de la UNAM, México, 1993. P.90

<sup>48</sup> Vidaurri Aréchiga, Manuel y Soriano Flores, José, *“Derechos Humanos, Concepto y Fundamento”*, en *Investigaciones Jurídicas* no.79, Universidad Autónoma de Guanajuato, 2007

<sup>49</sup> Bidart Campos, German J. *“Teoría general...”* op. cit. P.89

<sup>50</sup> Lampert, Ernâni, *“Posmodernidad y universidad: ¿una reflexión necesaria?”*, Perfiles educativos, vol. 30, México, Enero 2008, pp. 79-93, Disponible en: [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0185-26982008000200005](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-26982008000200005), consultado el 24 de noviembre de 2018.

naturaleza de los derechos humanos ha alcanzado un desarrollo en el cual las influencias que recibe son para enriquecer y no para restar, es progresiva en todo momento y no admite regresión, intentando eliminar todo posible rastro de relativismo moral que termine en perjuicio de nosotros.

Para las consideraciones finales de este apartado, me gustaría regresar a la Dra. Estévez, especialmente a esta idea:

“(…) aquellos derechos que garantizaban la dignidad de las personas en alguna época en particular, no son necesariamente los mismos en el tiempo presente o en el futuro. Lo anterior significa que no existen derechos fijos en el tiempo y el espacio”<sup>51</sup>

Líneas arriba mencionaba cierta sombra de relativismo concerniente al discurso posmodernista y su negativa a las verdades absolutas que encontró cabida en las formulaciones de la fundamentación de los derechos humanos basadas en el consenso (incluyo aquí la postura historicista), las cuales compartían la negación a continuar utilizando las fundamentaciones absolutas del iusnaturalismo y el iuspositivismo. Hay que remarcar que no existe nada intrínsecamente censurable en esos enfoques no absolutistas, sin embargo existe el riesgo de caer en interpretaciones erróneas con relación al relativismo, un ejemplo servirá para esclarecer la situación, pensemos: si lo que “entendemos” por dignidad va cambiando en el tiempo y en el espacio, y por lo tanto, los derechos que la garantizan no se encuentran de ninguna manera fijos, entonces, ¿es posible que en un futuro derechos que por ahora damos por sentado, desaparezcan?, ¿lo que hoy consideramos evidente será dejado de lado mañana?, ante estos cuestionamientos sólo queda decir que uno de los principios de los DDHH es el de progresividad<sup>52</sup>, estos derechos no admiten regresiones, por lo tanto siempre habrá más derechos, nunca menos. Es inevitable pensar que las comunidades humanas cambiarán en el futuro y con ellas muchas ideas suyas, es más, es totalmente plausible que surjan situaciones que den pie a problemáticas nuevas<sup>53</sup> que requieran derechos y fundamentaciones de los mismos que nosotros ahora no podemos prever, pero eso no

---

<sup>51</sup> Estévez, Ariadna, op. cit.

<sup>52</sup> Mac-Gregor Poisot, Eduardo F; Caballero Ochoa, José *et al.* “Estándares sobre principios generales”, en Derechos Humanos en la Constitución: Comentarios de Jurisprudencia Constitucional e Interamericana, Suprema Corte de Justicia de la Nación, México, D.F. 2013, pp. 42-43

<sup>53</sup> Oppenheimer, Andrés, “¡Sálvense quien pueda! El futuro del trabajo en la era de la automatización”, Debate, Madrid, 2018.

significa que los nuevos derechos desplacen a los ya existentes “los nuevos derechos que van surgiendo no extinguen a los anteriores, al contrario (...) se van sumando en una concepción expansiva”<sup>54</sup>.

La clave para destrabar esta discusión se encuentra en la Declaración Universal de los Derechos Humanos, instrumento paradigmático para la interpretación que hoy damos a los DDHH y sobre la cual descansan los diversos instrumentos contemporáneos que se han creado para su protección. En su preámbulo se invoca a la dignidad humana como eje rector de este modelo de protección a la persona de “los actos de barbarie” que han aquejado a la familia humana. Después de las atrocidades observadas durante la Segunda Guerra Mundial, la comunidad internacional necesitó de invocar un concepto que respondiera o advirtiera sobre las consecuencias de permitir que actos de semejante índole sucedieran una vez más.<sup>55</sup> Es imposible negar la magnitud de los hechos contenidos en ese momento histórico, y toda construcción de justicia y ética que se realice sin considerarlo fallaría en su núcleo mismo. Lefranc Weegan al respecto reflexiona:

“por eso no es cierto que se pueda empezar desde el olvido. Que nuestras sociedades puedan continuar su desarrollo como si ningún crimen se hubiera cometido. Porque se cometieron actos de barbarie ultrajantes para la conciencia de la humanidad. Actos que no deben ser olvidados. Por eso es importante indagar por el sentido de que puede tener la dignidad humana, sin omitir los crímenes y sin volver invisibles a las víctimas”<sup>56</sup>

### 1.3 Tecnologías de la información y la comunicación.

#### 1.3.1. Conceptualización TIC

##### 1.3.1.1 Ciencia y Tecnología

---

<sup>54</sup> Gross Espiell, Héctor “Nuevas tendencias del constitucionalismo en América Latina”, en *Tendencias del constitucionalismo en Iberoamérica*, Universidad Nacional Autónoma de México, México, 2009

<sup>55</sup> Lefranc Weegan, Federico, “Los límites de la interpretación de la dignidad humana. La presencia Kantiana en su concepción jurídica actual”, Tesis Doctoral, Universitat Atonoma de Barcelona, Diciembre de 2009, p 20

<sup>56</sup> *Ibíd.* P. 245

Hasta este momento se ha referido a las TIC como productos de la ciencia y la tecnología, por ello, considero conveniente conceptualizar primero estas últimas para después tener una base más sólida sobre la cual aterrizar la idea de las TIC. Aclarado lo anterior, me gustaría comenzar con el acercamiento a la ciencia que nos da el filósofo, Mario Bunge:

“Mientras los animales inferiores sólo están en el mundo, el hombre trata de entenderlo; y sobre la base de su inteligencia imperfecta pero perfectible, del mundo, el hombre intenta enseñorearse de él para hacerlo más confortable. En este proceso, construye un mundo artificial: ese creciente cuerpo de ideas llamado "ciencia", que puede caracterizarse como conocimiento racional, sistemático, exacto, verificable y por consiguiente falible. Por medio de la investigación científica, el hombre ha alcanzado una reconstrucción conceptual del mundo que es cada vez más amplia, profunda y exacta”<sup>57</sup>

De dicha reflexión se extraen tres ideas centrales: 1) La ciencia es una construcción netamente humana que toma como punto de partida el mundo que lo rodea. Es, por naturaleza, artificial; 2) Sirve para un doble propósito: entender el mundo y modificarlo para hacerlo más cómodo para nuestra especie. Cabría aquí remarcar que la ciencia, o mejor dicho, su papel, no es el de mejorar al mundo *per se*, en sí mismo, es decir, en cuanto producción artificial no busca hacer más eficiente el funcionamiento de la naturaleza, sino que su fin, (su intencionalidad) es otro, a saber, acoplar el mundo material a nuestros deseos y necesidades; 3) Se caracteriza por ser un conocimiento de tipo racional, sistemático, exacto, verificable y mejorable. El último aspecto es crucial, el hecho de que todo conocimiento científico sea perfectible significa que, en esencia, su certeza siempre puede ser puesta en duda. Ya Karl Popper nos hablaba sobre la cualidad de *falsabilidad* en la ciencia<sup>58</sup>. Esta condición, obligatoria en toda proposición científica, implica que la ciencia empírica es siempre conjetural o aproximada, nunca quedando verificada concluyentemente, por lo tanto, sus explicaciones son provisionales y tendientes a ser reemplazadas por otras que expliquen aquellos hechos no previstos en las premisas previas.

---

<sup>57</sup> Bunge, Mario, “*La ciencia. Su método y su filosofía*”, Nueva Imagen, Segunda Edición, México, 2012, p. 6

<sup>58</sup> Popper, Karl, “*Conjeturas y refutaciones. El desarrollo del conocimiento científico*”, Paídos, Buenos Aires, 1983

Colocando la atención ahora en el componente social que se encuentra en la ciencia y que se manifiesta a lo largo de todos sus procesos, Mendelsohn, considera que esta es:

"una actividad de seres humanos que actúan e interactúan, y por tanto una actividad social. Su conocimiento, sus afirmaciones, sus técnicas, han sido creados por seres humanos y desarrollados, alimentados y compartidos entre grupos de seres humanos. Por tanto el conocimiento científico es esencialmente conocimiento social. Como una actividad social, la ciencia es claramente un producto de una historia y de un proceso que ocurre en el tiempo y en el espacio y que involucra actores humanos. Estos actores tienen vida no sólo dentro de la ciencia, sino en sociedades más amplias de las cuales son miembros."<sup>59</sup>

Queda manifiesto que la ciencia toda es un producto que nace y se alimenta de interacciones humanas, no sólo eso, sino que dichas interacciones ocurren en contextos determinados, es decir, suceden en espacios y tiempos concretos, con toda la carga histórica y cultural que eso conlleva. La ciencia no es una creación en abstracto, nacida en el vacío y libre de ataduras de la realidad social, al contrario, está firmemente enraizada en ella, persiguiendo fines y objetivos bien definidos: "Los procesos de producción, difusión y aplicación de conocimientos propios de la actividad científica son inexplicables al margen de los intereses económicos, políticos, militares, entre otros que caracterizan los diversos contextos sociales"<sup>60</sup>. Ahora bien, no deben extrapolarse estos postulados y asegurar categóricamente que no hay nada de objetivo o neutral en el quehacer científico, al contrario, la ciencia tiende a la objetividad y la neutralidad en la producción de su conocimiento. Para comprender mejor esta aparente disonancia, habría que concebir a la ciencia como un ser bicéfalo, es a la vez actividad y saber<sup>61</sup>; la primera refiere al acto (material e intelectual) de *hacer* ciencia, el segundo es el conjunto de los resultados del mismo. Ambos se realizan en comunidades culturales las cuales influyen en su concepción, realización, presentación y aplicación. Las

---

<sup>59</sup> Mendelsohn, Everett, "The social construction of scientific knowledge", en Mendelsohn, et al, (comps), *The social production of scientific knowledge*, Reidel Publishing Company, Dordrecht y Boston, 1977, p.3. Traducción de Jorge Núñez Jover.

<sup>60</sup> Núñez Jover, Jorge, "Rigor, objetividad y responsabilidad social: la Ciencia en el encuentro entre Ética y Epistemología", en *La ciencia y la tecnología como procesos sociales. Lo que la educación científica no podría olvidar*, Organización de los Estados Iberoamericanos, s.f. disponible en: <https://www.oei.es/historico/salactsi/nunez05.htm>, consultado el 3 de julio, 2019.

<sup>61</sup> Ídem.

valoraciones sociales, históricas y técnicas ejercerán un enorme papel en decidir el qué se investiga, cómo se hace y para qué, sin embargo los descubrimientos y resultados empíricos deben buscar un mínimo de certeza y objetividad. Agazzi concluye que “la ciencia no puede ser neutral como actividad mientras lo es y debe serlo como saber”<sup>62</sup>.

Finalicemos este apartado con una definición que retoma las características dilucidadas anteriormente: La ciencia es una construcción humana, socialmente contextualizada, que a partir del mundo material en el que se encuentran, busca entender, explicar y modificar la naturaleza para satisfacer necesidades concretas y hacer más cómoda la existencia en el mundo de sus actores. Su conocimiento es de índole racional, sistemático, exacto, verificable y falible, siempre susceptible de mejora. Sus nociones, modelos y productos se informan y manifiestan en diversos campos de la experiencia humana.

Como se deja ver en los párrafos anteriores, la ciencia tiende a una aplicación práctica del cúmulo de conocimientos emanados de la investigación. Es posible referirse al concepto de tecnología como al conocimiento utilizable o utilizado a escala social con el objeto de transformar elementos materiales y simbólicos en bienes y servicios<sup>63</sup>, sin embargo, no es conveniente reducir a la tecnología como un simple remanente de la ciencia, apenas un apéndice meramente ejecutivo del denso y arduo proceso de la investigación dura y el razonamiento complejo<sup>64</sup>. Nada más alejado de la realidad, la técnica y la tecnología son campos igual de complejos, con multitud de aristas y capas de profundidad en ellas, y su influencia en el desarrollo del ser humano y su sociedad ha sido inmensa. Acertadamente comenta Manuel Castells, al hablar de Bijker y del dilema del determinismo tecnológico, que “tecnología *es* sociedad y ésta no puede ser comprendida o representada sin herramientas técnicas”<sup>65</sup>.

---

<sup>62</sup> Agazzi, Evandro, “*El bien, el mal y la ciencia*”, Tecnos, Madrid, 1996, p. 71

<sup>63</sup> Suárez, Francisco, “La dependencia científica y su relación con la dependencia cultural y tecnológica”, en *Autonomía nacional o dependencia: la política científico-tecnológica*, Paídos, Buenos Aires, 1975.

<sup>64</sup> Prince, De Solla, “*Ciencia y tecnología: Distinciones e interacciones*”, Estudios sobre sociología de la Ciencia, Editorial Alianza Universidad, Madrid, 1980.

<sup>65</sup> Castells, Manuel, “*La era de la información. Economía, sociedad y cultura*” Vol. 1, Siglo XXI, México, 1996, Disponible en: <http://www.economia.unam.mx/lecturas/inae3/castellsm.pdf>, consultado el 7 de julio de 2019.

Un buen primer paso para comprender a la tecnología es marcar su relación y diferenciación con la técnica. Regreso a Agazzi para arrojar luz en este punto; con respecto a la técnica, él reflexiona:

“En sentido lato, la técnica puede ser considerada, como una acumulación de procedimientos operativos útiles desde el punto de vista práctico para la consecución de fines particulares. Habitualmente son descubrimientos sometidos a verificación y mejorados a través de la experiencia de muchas generaciones, y constituyen un saber cómo (se hacen ciertas cosas), sin implicar necesariamente un saber por qué (se hacen así), en el sentido de que su eficacia y su éxito emergen empíricamente, o sea, en la práctica concreta, sin que se esté en posición (o al menos sin que se deba estarlo) de dar las razones o el porqué de ese éxito.”<sup>66</sup>

Al leer estas líneas se observa un primer elemento que distingue a la técnica de la ciencia, esta busca siempre una explicación, el porqué de las cosas, averigua las relaciones entre hechos y fija las leyes que los rigen, mientras que la técnica bien puede prescindir de ello. Ultimadamente su objetivo no es conocer los fundamentos de la naturaleza, sino las formas eficaces para modificarla. Esta peculiaridad, sostiene Agazzi, posibilita que, si uno quisiera, pudiera hablarse de una historia de la técnica en la que sea posible prescindirse casi por completo de la ciencia: “en cuanto el progreso técnico prosigue por propia fuerza según la lógica de la eficacia, sin necesidad de conocer el porqué de esa eficacia y, en el fondo, sin ni siquiera plantearse la pregunta”<sup>67</sup>. Claro está, que técnica y ciencia puedan crecer y desarrollarse por caminos separados no significa que este haya sido el curso que tomaron. Teniendo más puntos en común que diferencias, la unión entre estas dos ideas solo era cuestión de contar con un escenario propicio, el cual llegó con el Renacimiento. Con la nueva ciencia surgida en ese periodo, sus ideas y su cumulo de conocimientos detallados y precisos, se comienza a formar un saber que no se conforma ya con la mera explicación o funcionamiento de los ejercicios empíricos exitosos de prácticas o instrumentos, sino que ahora se pueden proyectar instrumentos y prácticas completamente nuevos, aun no inventados, se instaura una nueva etapa en la relación conocimiento-aplicación<sup>68</sup>. La ciencia

---

<sup>66</sup> Agazzi, *op. cit.* p.97

<sup>67</sup> *Ibíd.* P. 98.

<sup>68</sup> *Ibíd.* P. 101

influirá directamente en la creación de instrumentos, estos cada vez más especializados y que aprovechan los descubrimientos científicos además de contar con objetivos claramente establecidos. Lo anterior marca el origen y fundamento de lo que llamamos tecnología.

No debemos olvidar que estas distinciones son para fines analíticos ya que en el quehacer científico-técnico diario esas distinciones son más bien borrosas y en muchos casos irrelevantes. Sin embargo, podemos observar que es con la tecnología, más que con la simple técnica, que la ciencia estrecha sus nexos y expande sus posibilidades. Esa relación no es una simple subordinación, de la tecnología a la ciencia, por el contrario, es un diálogo, en el que por momentos la tecnología funge como una *ciencia aplicada* y en otros contribuye activamente al proceso de generación del conocimiento, ayudando a la solución de problemas cognoscitivos gracias a la proyección y construcción oportuna de instrumentos específicos<sup>69</sup>. La tecnología no es pasiva ni un simple derivado, sus conceptos y accionar son propios de un campo complejo, surgido de las interacciones humanas.

### 1.3.1.2 TIC

#### 1.3.1.2.1 Definiciones

Con la información anterior, ahora nos encontramos en una situación más propicia para identificar y comprender a las TIC. Me gustaría iniciar con la definición propuesta por el investigador Arthur Serra ya que toca muchas de las ideas expuestas en los párrafos precedentes, para él las TIC:

“son conocimiento, no “herramientas”. La cultura moderna heredera de la tradición griega nos ha acostumbrado a diferenciar conocimiento de técnica. El conocimiento (teoría) ha sido identificado tradicionalmente con la contemplación de la verdad. La técnica, por su parte, con el arte de construir útiles, con el saber práctico. Esta visión occidental extendida ya a todo el mundo, está hondamente arraigada en nuestro sistema universitario (...) De hecho, la tecnología ha sido la última rama del conocimiento en ser aceptada en el mundo académico. Quizás es por ello que la visión tradicional de la tecnología, que la considera todavía una simple “herramienta”, o en el mejor de los casos en un saber práctico bajo la tutela de la ciencia, pervive también

---

<sup>69</sup> *Ibíd.* P. 102

entre los teóricos de la nueva sociedad digital y se ha dejado traslucir en los primeros análisis de la sociedad del conocimiento. Así, los autores iniciales que empezaron hace solo unas décadas a analizar el fenómeno, (D. Bell(1973), M. Castells (1990, 1997...)) han asumido consciente o inconscientemente esta división y jerarquía de saberes.”<sup>70</sup>

De la lectura anterior subyace una idea que considero fundamental para esta investigación: el papel de las TIC no es el de simples utensilios, es decir, no son *pasivas*, por lo tanto, sus conceptos, aplicaciones y repercusiones conllevan un *discurso activo* que es susceptible de análisis crítico. Se debe modificar el pensamiento que concibe a las herramientas (técnicas, tecnológicas) como objetos secundarios en la formación del aparato sociológico-cultural de nuestras comunidades en general, y del ejercicio de los derechos humanos en particular. No es que los aparatos tecnológicos tengan por si mismos un discurso, sino que, siendo parte de un proceso de socialización humano, tienen en su fondo un *proyecto* o intencionalidad. La predilección de una herramienta sobre otra, es ya un mensaje importante que se intensifica cuando observamos la *forma* en la que dicho instrumento se usa, y sobre todo *para qué*. La influencia de estos aparatos nacidos en la ciencia y la tecnología así como el discurso que enarbolan (muchas veces de manera velada) es primordial para una cabal defensa de nuestros derechos humanos en sociedades cada vez más dependientes de las ciencias aplicadas.

Profundizaremos en estos aspectos más adelante, por ahora avancemos en la conceptualización de las Tecnologías de la Información y la Comunicación; para la Comisión Económica para América Latina y el Caribe éstas son:

“sistemas tecnológicos mediante los que se recibe, manipula y procesa información, y que facilitan la comunicación, entre dos o más interlocutores. Por tanto, las TIC son algo más que informática y computadoras, puesto que no funcionan como sistemas aislados, sino en conexión con otras mediante una red. También son algo más que tecnologías de emisión y difusión (como televisión y radio), puesto que no sólo dan cuenta de la divulgación de la información, sino que además permiten una

---

<sup>70</sup> Serra, Arthur, “Investigación en Internet y nuevos modelos de desarrollo: El proyecto i2CAT”, en Finkelievich, Susana (Coord.) *Desarrollo Local en la Sociedad de la Información: Municipios e Internet*, Editorial La Crujía, Buenos Aires, 2005.

comunicación interactiva. El actual proceso de “convergencia de TIC” (es decir, la fusión de tecnologías de información y divulgación, las tecnologías de la comunicación y las soluciones informáticas) tiende a la coalescencia de tres caminos tecnológicos separados en un único sistema que, de forma simplificada, se denomina TIC (o la “red de redes”)<sup>71</sup>

Por otro lado, Christopher Ballinas Valdés, en una publicación para el Tribunal Electoral del Poder Judicial de la Federación nos dice que las TIC:

“pueden considerarse como un conjunto de aparatos, redes y servicios integrados en un sistema de información interconectado y complementario. Más ampliamente, el concepto de TIC se refiere al almacenamiento, procesamiento, recuperación y distribución de la información por medio de procesos informáticos —es decir, procesos microelectrónicos computarizados—, así como telemáticos —que se refiere a la organización y transmisión de mensajes computados a través de redes integradas de telecomunicación mediante la digitalización, la fibra óptica, o vía satelital (Jaramillo 1986)—. Las herramientas para estas actividades incluyen una amplia gama de instrumentos, tales como las computadoras y los dispositivos personales, así como los medios de comunicación electrónicos “convencionales”, como el radio, la televisión y el teléfono, entre otros.”<sup>72</sup>

En ambas definiciones pueden observarse algunos elementos en común: 1) siempre se refieren a las TIC en plural, es decir, no existe una forma homogenizada o monopolizadora de las TIC, estas son diversas y están agrupadas en conjuntos o sistemas; 2) estos grupos de aparatos están conectados unos a otros en una aparente horizontalidad, donde ninguno destaca sobre los otros; 3) el flujo de la información es la constante en todos estos utensilios, la información es tanto recibida como enviada, el usuario, por lo tanto, es al mismo tiempo

---

<sup>71</sup> Comisión Económica para América Latina y el Caribe (CEPAL), “*Los caminos hacia una sociedad de la información en América Latina y el Caribe*”, Naciones Unidas, Julio de 2003, p2. Disponible en: [https://repositorio.cepal.org/bitstream/handle/11362/1836/S0015K19\\_es.pdf](https://repositorio.cepal.org/bitstream/handle/11362/1836/S0015K19_es.pdf), consultado el 2 de junio de 2019.

<sup>72</sup> Ballinas Valdés, Christopher, “*Participación política y las nuevas tecnologías de la información y la comunicación*”, Tribunal Electoral del Poder Judicial de la Federación, México, 2011, p. 12

receptor y generador de contenidos; 4) es una fusión entre herramientas provenientes de la informática y la comunicación.

Para comprender mejor el último apartado, reproduzco a continuación un esquema de la CEPAL que ilustra claramente esta unión de campos:

**Gráfico 1.1.**

Convergencia de tecnologías de la información y comunicación



**Fuente:** Martin Hilbert “Toward a theory on the information society”; “Infraestructure”; “Strategies”; “Telecommunications regulation: technical standards”; “Financing a universal Information Society for all”; “e-Business: digital economics”; “e-Media”, Building an Information Society: A Latin American and the Caribbean Perspective (LC/L, 1845), Martin Hilbert y Jorge Katz (comps), Santiago de Chile, Comisión Económica para América Latina y el Caribe (Cepal) 2003<sup>73</sup>

En abarcar más y con mayor fidelidad puede resumirse este diagrama, pero no es lo único que podemos obtener de su análisis, también es posible ver cómo herramientas que un inicio tenían fines específicos fueron eventualmente encontrando puntos técnicos en común que desembocaron en aparatos multitareas. Realizar más funciones con menos recursos parecer ser otro resultado de esta evolución. De acuerdo con esto, podemos afirmar que las TIC son

<sup>73</sup> CEPAL, “Los caminos hacia una sociedad..” op cit. P. 2

“las innovaciones que surgen de la integración de dos o más tecnologías simbióticas cuando se intenta simplificar la estructura general del sistema tecnológico”<sup>74</sup>

#### 1.3.1.2.2 Características

El investigador, Julio Cabero, de la Universidad de Sevilla, agrupa las características de las TIC de la siguiente forma<sup>75</sup>:

-Inmaterialidad: no entendida como la inexistencia física de los medios o sus contenidos, sino en el sentido de que la materia prima sobre la cual se basa su actividad es la información, esta desarrollada en diversos códigos y formas: visuales, auditivas, audiovisuales, textuales de datos, etc. Todos ellos se pueden dar de forma individual o en combinación, tanto de manera estacionaria, como en movimiento.

-Interconexión: apela a la posibilidad de que tanto los medios tecnológicos como sus contenidos multimedia pueden combinarse y ampliar significativamente sus cualidades / capacidades individuales, con lo cual se puede llegar a la construcción de nuevas realidades expresivas y comunicativas.

-Interactividad: trastoca el control tradicional que solía ejercer el emisor en los medios tradicionales, ya que ahora el receptor desempeña un papel más activo en el tiempo y la modalidad de uso. El receptor es ahora parte importante en la construcción del mensaje así como en su transmisión.

-Instantaneidad: las TIC permiten romper las otrora difíciles barreras espaciales y temporales, poniéndonos en contacto directo y de forma prácticamente inmediata con personas, bancos de datos, contenidos multimedia, etc. De acuerdo con el autor, “convierten el problema de la transmisión o recepción de la información, al margen de los de acceso e ideológico y social, en uno exclusivamente, técnico, es decir, de la potencialidad tecnológica de los medios”<sup>76</sup>

---

<sup>74</sup> Sahal, Devendra, “*Technological guidepost and innovation avenues*”, Research Policy, vol. 14 No.2, Elsevier, Amsterdam, 1985. Traducción de Martin Hilbert.

<sup>75</sup> Cabero, Julio, “*Las nuevas tecnologías en la sociedad de la Información*”, Universidad de Sevilla, 2006, pp. 11 – 13 .Disponible en: [https://www.researchgate.net/publication/238672345\\_Las\\_nuevas\\_tecnologias\\_en\\_la\\_Sociedad\\_de\\_la\\_Inf\\_ormacion](https://www.researchgate.net/publication/238672345_Las_nuevas_tecnologias_en_la_Sociedad_de_la_Inf_ormacion), consultado el 6 de julio de 2019.

<sup>76</sup> Ídem

-Elevados parámetros de imagen y sonido: se refiere tanto a la calidad de la información en términos técnicos (número de colores definidos, tonalidad, representación de armónicos, elementos cromáticos, etc.) como a la fidelidad con la que se transfieren de un punto a otro.

-Penetración en todos los sectores de la vida humana: las TIC pasaron de usarse en ambientes militares, bancarios y de transferencia de comunicación de masas a prácticamente todos los campos de la civilización contemporánea

-Creación de nuevos lenguajes expresivos: la naturaleza de las TIC permiten nuevas realidades expresivas (ejemplo el lenguaje multimedia o hipermedia), con lo cual llega la necesidad de organizar y combinar de nuevas maneras los códigos, así como otorgarles a estos otros significados. Es posible que exista la necesidad de adquirir nuevos dominios alfabéticos.

-Ruptura de la linealidad expresiva: en estrecha relación con lo anterior, los mensajes en las TIC tienden a organizarse de una manera no lineal, sino más bien hipertextual. Esto implica nuevos modelos en los que prevalece “la desestructuración del discurso, la transferencia del peso de la comunicación de autor al texto, (...) y la construcción del significado de forma diferente en función de la navegación hipertextual realizada por el receptor”<sup>77</sup>

-Potenciación de una audiencia segmentaria y diferenciada: la diversidad de los medios tecnológicos y la especialización progresiva de sus contenidos tiende a la diferenciación y segmentación de las audiencias, esto en virtud de las características de los diversos receptores. Se observan dos tendencias cercanas surgidas esto: la creación de programas y contenidos que sean reflejos de los intereses de la audiencia conseguida, y a una paulatina tematización de los canales o vías de comunicación.

-Rapidez innovadora: el desarrollo y perfeccionamiento técnico de las TIC ocurren a una velocidad inusitada.

-Diversidad: existe una enorme variedad de las tecnologías de la información y la comunicación, además, cada una de ellas puede desempeñar diversas funciones gracias a la flexibilidad que brinda el *software* y su capacidad para modificar el *hardware*.

---

<sup>77</sup> Ídem

## **CAPITULO II. DERECHO A LA PRIVACIDAD: REGULACION Y JURISPRUDENCIA INTERNACION Y NACIONAL**

### **2.1 Derecho Internacional**

El derecho a la privacidad se encuentra contemplado en diversos instrumentos provenientes del derecho internacional de los derechos humanos. La Declaración Universal de los Derechos Humanos (1948) lo contiene en el artículo 12, y establece 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 reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”<sup>78</sup>. De igual forma es objeto de protección en el artículo 17 (derecho a la privacidad), a su vez íntimamente ligado al 19 (libertad de expresión)<sup>79</sup> del Pacto Internacional de Derecho Civiles y Políticos (1966); en el artículo 16 del Convención de los Derechos del Niño (1989)<sup>80</sup> y en los respectivos documentos regionales de DDHH de Europa, América y África. A continuación se realiza una revisión sobre la jurisprudencia que los tribunales de Europa y América han desarrollado sobre este derecho fundamental y su relación con la vigilancia a través de mecanismos electrónicos.

#### *2.1.1 Europa*

En la Unión Europea el derecho a la protección de la vida privada está contenido en artículo 8º del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (aprobado en 1950). Dicho artículo establece que: “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

---

<sup>78</sup> Declaración Universal de los Derechos Humanos. Art. 12. Asamblea General de las Naciones Unidas, 1948.

<sup>79</sup> “Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito [...] o por cualquier otro procedimiento de su elección”. Pacto Internacional de Derechos Civiles y Políticos, Art. 19. Asamblea General de las Naciones Unidas. 1966.

<sup>80</sup> “1. Ningún niño 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 a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias y ataques” Convención de los derechos del niño. Art.16. Asamblea de las Naciones Unidas, 1989.

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”<sup>81</sup>

El avance de las tecnologías informáticas en las décadas posteriores trajo consigo la necesidad de desarrollar un conjunto de normas más especializadas y precisas para enfrentar los desafíos relativos a la protección de datos de los ciudadanos europeos. De tal situación surgió en 1981 el “Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal”, conocido como el Convenio núm. 108. Este documento es el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos. Busca proteger a la persona en contra de los abusos que pudieran resultar de la recopilación y el tratamiento automatizado de los datos personales y a la vez, diseña una regulación para el flujo transfronterizo de los datos personales<sup>82</sup>. El Convenio 108 aplica tanto a los sectores privados como a los públicos.

Una característica destacable del citado convenio es que se encuentra abierto a la adhesión de otros Estados no miembros del Consejo de Europa, incluso países no europeos. México adoptó el Convenio 108 y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos (del 2001) mediante decreto en el Diario Oficial de la Federación el 12 de junio de 2018.<sup>83</sup>

El artículo 2º del Convenio 108 define datos personales como “cualquier información relativa a una persona física identificada o identificable”. El Tribunal Europeo de Derechos Humanos (TEDH) ha expresado en el caso *S. y Marper vs. Reino Unido* que la protección de los datos personales reviste una particular importancia para el disfrute de la vida privada y familiar de

---

<sup>81</sup> Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Art. 8. Consejo de Europa, 1950.

<sup>82</sup> Huber, Florian, “*Tecnologías de Información y Comunicación (TIC), protección de datos y derechos humanos en la jurisprudencia del Tribunal Europeo de Derechos Humanos*”, Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, México 2016, p. 82. Disponible en: <https://archivos.juridicas.unam.mx/www/bjv/libros/9/4065/8.pdf>, consultado el 8 de noviembre de 2018.

<sup>83</sup> Molet, Jorge, “*Adopción de México del Convenio 108 del Consejo de Europa, protección y flujo internacional de datos*”, *El Financiero*, México, 20 de junio de 2018, disponible en: <https://www.economista.com.mx/opinion/Adopcion-de-Mexico-del-Convenio-108-del-Consejo-de-Europa-proteccion-y-flujo-internacional-de-datos-20180620-0098.html>, consultado el 2 de julio de 2019.

una persona<sup>84</sup>. El concepto de vida privada engloba la privacidad de las telecomunicaciones, entre ellas la seguridad y privacidad de correo, teléfono, correo electrónico y otras formas de comunicación, así como la privacidad de la información, la cual toma en cuenta la privacidad en Internet<sup>85</sup>

La protección de la vida privada no solo queda en datos informáticos, sino que también considera elementos relacionados con la imagen de una persona<sup>86</sup>, es decir, todo retrato de una persona logrado, conservado y /o reproducido en un fotografía, video o cualquier otro medio electrónico cae dentro de la protección del artículo 8º de la Convención. Esto aplica de igual manera para la voz de una persona. Su grabación, uso, difusión o posterior análisis sin el debido consentimiento, significa una violación a su derecho al respeto de su vida privada.<sup>87</sup> Las conclusiones a las que ha llegado el Tribunal Europeo de Derechos Humanos subrayan “que ya desde la mera recopilación y el almacenamiento de información sobre la vida privada de un individuo se está ante una injerencia en el ámbito de protección del artículo 8º de la CEDH, independientemente del uso de tal información”<sup>88</sup>. Refiriéndose específicamente al impacto que pueden tener las técnicas científicas modernas en el ejercicio del derecho a la protección de la vida privada, el Tribunal Europeo pronunció, una vez más en el caso *S. y Marper vs. Reino Unido* que “la protección [...] se debilitaría inaceptablemente si el uso de técnicas científicas modernas [...] fuera permitido a cualquier costo y sin equilibrar cuidadosamente los beneficios potenciales del uso extensivo de tales técnicas contra importantes intereses de la vida privada.”<sup>89</sup>

De lo anterior se observa que el tratamiento arbitrario de los datos privados (lo cual abarca su recopilación, almacenamiento y uso) significa una violación al derecho a la privacidad. Sin embargo, este no es un derecho total o absoluto, y tanto en los instrumentos normativos como en la jurisprudencia del TEDH su puede encontrar los márgenes a los cuales se

---

<sup>84</sup> TEDH, *Caso S. y Marper vs. Reino Unido*, [GC], núms. 30562/04 y 30566/04, Sentencia de 4 de diciembre de 2008, § 41

<sup>85</sup> Huber, Florian, “*Tecnologías de...*” op. cit. P.85

<sup>86</sup> TEDH, *Caso Sciacca vs Italia*, núm. 50774/99, Sentencia de 11 de enero de 2015, §29

<sup>87</sup> TEDH, *Caso P.G. y J.H. vs. Reino Unido*, núm. 44787/98, Sentencia de 25 de septiembre de 2001, § 59.60

<sup>88</sup> Huber, Florian, “*Tecnologías de...*” op. cit. P.85. Ver: TEDH, *Caso Leander vs Suecia*, núm. 9248/81, Sentencia de 26 de marzo de 1987; TEDH, *Caso Kopp vs Suiza*, núm. 23224/94, Sentencia de 25 de marzo de 1998; TEDH, *Caso Amman vs. Suiza* [GC], núm. 27798/95, Sentencia de 16 de febrero de 2000, §69

<sup>89</sup> TEDH, *Caso S. y Marper vs. Reino Unido*, [GC], núms. 30562/04 y 30566/04, Sentencia de 4 de diciembre de 2008, § 112.

circunscribe cuando es necesaria su ponderación ante intereses legítimos en una sociedad democrática, a saber, cuando entra en conflicto con los derechos de otras personas (interés privado) o cuando su limitación es relevante para la sociedad en su conjunto (interés público).

Para que pueda existir una interferencia Estatal justificada y legal dentro de la esfera de los datos personales de un individuo, el Convenio Europeo de los Derechos Humanos estipula 3 condiciones indispensables que deben cumplirse: 1) Debe ser en conformidad con la ley; 2) Debe perseguir un fin legítimo; y 3) Ser una medida necesaria en una sociedad democrática. Relacionado con el primer punto, el Tribunal Europeo de Derechos Humanos indica que una intervención a la vida privada y los datos de una persona es en *conformidad con la ley* cuando se basa en una norma del derecho interno y ésta cumple con ciertos requisitos: la ley debe ser accesible a las personas interesadas y previsible en cuanto a sus efectos<sup>90</sup>; esa norma solo es considerada previsible si está formulada con la suficiente precisión para permitir a cualquier particular, en caso necesario con el asesoramiento adecuado, prever sus consecuencias para él<sup>91</sup>. Ahora bien, el grado de precisión de la ley puede variar de acuerdo a temas o circunstancias específicas. En el caso *The Sun Day times vs el Reino Unido*, el Tribunal menciona que “si bien la certeza es altamente deseable, puede traer una rigidez excesiva y la ley debe ser capaz de seguir el ritmo de las circunstancias cambiantes. En consecuencia, muchas leyes se expresan inevitablemente en términos que, en mayor o menor medida, son vagos y cuya interpretación y aplicación son cuestión de práctica”<sup>92</sup>

El *fin legítimo* se encuentra previsto en el artículo 8º Del Convenio Europeo de Derechos Humanos, y menciona los interés públicos y privados que pueden constituir un objetivo legítimo, dígase 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, y la protección de los derechos y las libertades de los demás. El TEDH en el caso *Peck vs. Reino Unido*, relacionado con el derecho a la imagen personal, indicó que las

---

<sup>90</sup> Ver: TEDH, *Caso Amman vs Suiza* [GC] núm. 27798/95, Sentencia de 16 de febrero de 2000, § 50; TEDH, *Caso Kopp vs Suiza*, núm. 23224/94, Sentencia de 25 de marzo de 1998, § 55; TEDH, *Caso Iordachi, y otros vs Moldavia* núm. 25198/02, Sentencia de 10 de febrero de 2009, §50.

<sup>91</sup> Ver: TEDH, *Caso Amman vs Suiza* [GC] núm. 27798/95, Sentencia de 16 de febrero de 2000, § 56; TEDH, *Caso Malone vs Reino Unido*, núm. 8691/79, Sentencia de 2 de agosto de 1984, § 66; TEDH, *Caso Silver y otros vs Reino Unido*, núms. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, Sentencia de 25 de marzo de 1983, §88.

<sup>92</sup> TEDH, *Caso The Sun Day Times vs. Reino Unido*, núm. 6538/74, Sentencia de 26 de abril de 1979, § 49

autoridades violaron el artículo 8° cuando la policía cedió las imágenes grabadas en un CCTV, de una persona que intentó suicidarse en un espacio público, a los medios de comunicación, los cuales posteriormente transmitieron las escenas al público en general. El Tribunal no encontró un objetivo legítimo en dicha acción y por ello dictó la sentencia en contra de las autoridades policiales.<sup>93</sup> Por último, con respecto a la idea de *medida necesaria en una sociedad democrática*, esta implica que toda interferencia debe corresponder a una necesidad social imperiosa y a su vez, debe ser proporcional al fin legítimo perseguido<sup>94</sup>. Por ejemplo, durante el caso *Leander vs. Suecia*, sobre el nivel de escrutinio secreto que se realizaba a individuos que solicitaban empleo en puestos relevantes para la seguridad nacional de ese país, el TEDH resolvió que el Estado tenía derecho a considerar que, con respeto al caso del demandante, los intereses de la seguridad nacional prevalecían sobre el derecho a la privacidad de los individuales<sup>95</sup>

Dentro de la jurisprudencia del TEDH se encuentra en diversas ocasiones el tema de la vigilancia de la comunicación privada por parte de las autoridades gubernamentales, entre ellas los servicios secretos, la policía y las autoridades judiciales. En los pasados 30 años el Tribunal Europeo ha señalado y condenado reiteradamente las faltas en las que diversos Estados Europeos han incurrido por vigilancia electrónica y la respectiva violación a sus leyes nacionales regulatorias sobre la materia o por la falta de las mismas<sup>96</sup>. La interceptación y grabación de conversaciones mediante dispositivos electrónicos por parte de la policía ha sido objeto de los casos *Malone vs Reino Unido*<sup>97</sup>, *Kahn vs. Reino Unido*<sup>98</sup> y *A. vs. Francia*<sup>99</sup>. En esos juicios el TEDH encontró violaciones al artículo 8° de la CEDH por realizar acciones en contra de lo dispuesto por la ley estipulada en el derecho interno de los respectivos países;

---

<sup>93</sup> TEDH, *Caso Perks vs. Reino Unido*, núm. 44647/98, Sentencia de 28 de enero de 2003, § 85 - 87

<sup>94</sup> TEDH, *Caso Leander vs. Suecia*, núm. 9248/81, Sentencia de 26 de marzo de 1987, § 58

<sup>95</sup> TEDH, *Caso Leander vs. Suecia*, núm. 9248/81, Sentencia de 26 de marzo de 1987, § 67

<sup>96</sup> Huber, Florian, "Tecnologías de..." op. cit. P.93

<sup>97</sup> TEDH, *Caso Malone vs Reino Unido*, núm. 8691/79, Sentencia de 2 de agosto de 1984. El Tribunal falló en contra del Estado por interceptar conversaciones y guardar los registros de números marcados en un teléfono durante el contexto de un juicio por posesión de bienes robados.

<sup>98</sup> TEDH, *Caso Khan vs. Reino Unido*, núm. 622/10, Sentencia de 20 de diciembre de 2011. En este caso una persona fue objeto de vigilancia Estatal por medio de un dispositivo de interceptación mientras se realizaba un proceso legal relacionado al delito de tráfico de drogas.

<sup>99</sup> TEDH, *Caso, A. vs. Francia*, núm. 14838/98, Sentencia de 23 de noviembre de 1993. En una investigación preliminar sobre una supuesta contratación para realizar un asesinato, el demandante fue objeto de una grabación acústica por parte de un particular, con asistencia de la policía.

mientras que en el caso *P.G y J. H. vs Reino Unido*<sup>100</sup> se sancionó al Estado porque no existía una regulación específica acerca de las escuchas secretas por parte de la policía, mediante dispositivos electrónicos, cuando sucedieron los hechos. De manera similar, en *Vetter vs Francia*<sup>101</sup>, el TEDH sancionó a las autoridades francesas debido a la falta de claridad y precisión en las leyes de ese país a la hora de regular el alcance y la forma en la que se debería utilizar los dispositivos de interceptación. Por otro lado, en el caso *Draksas vs Lituania*, sobre una intervención telefónica a un político del partido liberal-demócrata lituano, el Tribunal encontró una violación al artículo 8° no porque la policía haya utilizado un aparato de interceptación y con ello realizado grabaciones, sino por la filtración de dichas grabaciones a la prensa y medios de comunicación, los cuales las hicieron públicas mientras se realizaba un juicio político en contra del expresidente de Lituania.<sup>102</sup>

Para el tema de la intervención y vigilancia electrónica acreditada por autoridades competentes, el TEDH declaró en el caso *Kruslin vs. Francia* (centrado en las escuchas telefónicas ordenadas por un juez de instrucción durante el contexto de un juicio) que existía una violación al art. 8° dado que la legislación francesa no señalaba con la debida claridad y precisión suficiente el alcance y la forma de ejercicio de la discreción de las autoridades con respecto a las escuchas telefónicas.<sup>103</sup> En el caso *Klaas vs Alemania*<sup>104</sup>, relacionado con el terrorismo, el Tribunal reflexiona acerca de los peligros de la vigilancia indiscriminada en aras de la seguridad nacional: “las sociedades democráticas hoy en día se encuentran amenazadas por formas muy sofisticadas de espionaje y por el terrorismo, con la consecuencia de que el Estado, para contrarrestar eficazmente esas amenazas debe ser capaz de llevar a cabo la vigilancia secreta de elementos subversivos que operan dentro de su jurisdicción<sup>105</sup>, sin embargo “[el Tribunal] siendo consciente del peligro, inherente en las

---

<sup>100</sup> TEDH, *Caso P.G. y J.H. vs. Reino Unido*, núm, 44787/98, Sentencia de 25 de septiembre de 2001. Las voces de demandantes en este caso fueron grabadas en una estación de policía bajo la sospecha de que habían intentado cometer un robo. También se instaló un dispositivo de intercepción clandestinamente en uno de los departamentos de los demandantes.

<sup>101</sup> TEDH, *Caso Vetter vs. Francia*, núm. 59842/00, Sentencia de 31 de mayo de 2005. El caso tiene su origen en la instalación de un dispositivo, por parte de la policía, en un departamento que visitaba continuamente el demandante, un sospechoso de asesinato.

<sup>102</sup> TEDH, *Caso Draksas vs. Lituania*, núm. 36662/04, Sentencia de 31 d julio de 2012, § 60

<sup>103</sup> TEDH, *Caso Kruslin vs. Francia*, núm. 11801/85, Sentencia de 24 de abril de 1990, §36.

<sup>104</sup> TEDH, *Caso Klaas vs. Alemania*, núm. 5029/71, Sentencia de 6 de septiembre de 1978.

<sup>105</sup> TEDH, *Caso Klass, vs. Alemania*, núm. 5029/71, Sentencia de 6 de septiembre de 1978, § 42.

medidas de vigilancia secreta, de debilitar o incluso destruir la democracia con la justificación de defenderla, afirma que los Estados contratantes no podrán, en nombre de la lucha contra el espionaje y el terrorismo, adoptar cualquier medida que consideren apropiada”.<sup>106</sup> La cuestión del terrorismo y la vigilancia también es eje central en *Uzun vs. Alemania*, caso que involucra la vigilancia ordenada por el Fiscal General, mediante GPS, al demandante, ello con el fin de investigar varios intentos de homicidio atribuidos a un movimiento terrorista, así como para prevenir posibles nuevos atentados con explosivos. El Tribunal en esta ocasión decretó que no había violación al artículo 8º, porque la vigilancia a esta persona tenía objetivos acordes a los intereses de la seguridad nacional y pública, la prevención del delito y la protección del derecho de las víctimas, por lo tanto, la interferencia era proporcional a los fines legítimos y necesaria en una sociedad democrática<sup>107</sup>

La vigilancia oculta o clandestina ejercida por los servicios secretos de los países europeos adscritos al CEDH también ha sido objeto de análisis por parte del TEDH, como se observa en *Asociación “21 de diciembre 1989” y otros vs. Rumania*. Ese caso tiene su origen en la vigilancia ejercida, en 1989, al presidente de una asociación para la defensa de los derechos de personas manifestantes en contra del gobierno rumano. El Tribunal decretó una violación al artículo 8º debido a la falta de garantías en el derecho interno de ese Estado para impedir que la información recopilada por los servicios secretos se conservara por 16 años más.<sup>108</sup> En concordancia con lo anterior, el TEDH indicó que las carencias en la legislación interna dejaban en grave vulnerabilidad al demandante de que sus líneas telefónicas fueran intervenidas.<sup>109</sup> Para el fallo referido, el Tribunal Europeo de Derechos Humanos invocó la sentencia *Rotaru vs Rumania* de la Gran Cámara, en donde ya se había indicado que la forma en la que el sistema rumano recopilaba y archivaba la información obtenida mediante sus servicios secretos, no otorgaba las garantías suficientes para asegurar la protección de la vida privada de las personas.<sup>110</sup> En otro caso, *Dumitru Popescu vs Rumania*<sup>111</sup>, posterior al de

---

<sup>106</sup> TEDH, *Caso Klass, vs. Alemania*, núm. 5029/71, Sentencia de 6 de septiembre de 1978, § 49.

<sup>107</sup> TEDH, *Caso Klass, vs. Alemania*, núm. 5029/71, Sentencia de 6 de septiembre de 1978, § 80

<sup>108</sup> TEDH, *Caso Asociación “21 de diciembre 1989” y otros vs. Rumania*, núms. 33810/07 y 18817/08, Sentencia de 24 de mayo de 2011, § 121

<sup>109</sup> TEDH, *Caso Asociación “21 de diciembre 1989” y otros vs. Rumania*, núms. 33810/07 y 18817/08, Sentencia de 24 de mayo de 2011, § 122.

<sup>110</sup> TEDH, *Caso Rotaru vs. Rumania* [GC], núm. 28341/95, Sentencia de 4 de mayo de 2000, § 43.

<sup>111</sup> TEDH, *Caso Dumitru Popescu vs. Rumania*, (núm. 2), núm. 71525/01, Sentencia de 26 de abril de 2007, § 84.

*Rotaru*, el TEDH remarca que a pesar de las modificaciones y enmiendas legislativas realizadas al Código de Procedimiento Penal, aún existían las bases para una posible vigilancia secreta, así como de medidas especiales de control bajo casos de supuesta amenaza a la seguridad nacional de Rumania.

*Shimovolos vs Rusia*<sup>112</sup> es un caso más en el que el Tribunal se ha pronunciado sobre el almacenamiento de datos personales en bases de datos pertenecientes a los servicios secretos. En el dictamen de este caso, el TEDH determinó una violación al artículo 8º porque las bases de datos, creadas a partir de una decisión ministerial, no eran públicas ni tampoco accesibles para la ciudadanía, además, no era posible conocer la razón por la cual las personas registradas en esa base estaban ahí, ni el tipo de información que se anexaba y resguardaba. De igual manera, se desconocía el tiempo o los medios usados para guardar la información. Todos los datos y su uso estaban a discreción de los agentes del gobierno, quienes ejercían total control sobre ellos.<sup>113</sup>

La jurisprudencia del Tribunal Europeo de Derechos Humanos señalada hasta ahora ha instaurado una serie de garantías indispensables para regular las intervenciones telefónicas u otras formas de vigilancia electrónica que realizan las autoridades europeas y, de esta forma, prevenir acciones arbitrarias que constituyan un abuso en contra del derecho a la vida privada y a la protección de los datos personales. Huber<sup>114</sup> sintetiza esas garantías de la siguiente manera: Para toda intervención o interceptación telefónica u otras medias de vigilancia, debe existir un sustento legal sobre la cual se respalde dicha acción. La base legal debe ser accesible al público en su totalidad y especificar el tipo y naturaleza de los delitos que dan origen a una orden de inicio del procedimiento. También se debe indicar con toda precisión la categoría de personas que pudieran ser objetos de la vigilancia, el límite en la duración de las escuchas telefónicas u otras medias, el procedimiento a seguirse para evaluar la legalidad de la medida, el uso de los datos obtenidos, así como su almacenamiento y circunstancias bajo las cuales pueden o deben borrarse las grabaciones, cintas y demás bases de datos. Las protecciones relativas a la forma en la que una interceptación se realiza tienen que ser mecanismos de control eficaces y seguros para garantizar el cumplimiento de la ley. Es

---

<sup>112</sup> TEDH, *Caso Shimovolos vs. Rusia*, núm. 30194/09, Sentencia de 21 de junio de 2011.

<sup>113</sup> TEDH, *Caso Shimovolos vs. Rusia*, núm. 30194/09, Sentencia de 21 de junio de 2011, § 69.

<sup>114</sup> Huber, Florian, “*Tecnologías de...*” op. cit. PP. 96 y 97.

necesario que toda supervisión esté en concordancia con los principios democráticos aceptados: en conformidad con la ley, fin legítimo y medida necesaria en una sociedad democrática, asimismo, la supervisión deberá efectuarse por una autoridad independiente a la que realiza las acciones de vigilancia.

### 2.1.2. América.

La Corte Interamericana de Derechos Humanos (Corte IDH) se ha pronunciado sobre los requerimientos de Necesidad y Proporcionalidad cuando una medida tomada por las autoridades de un Estado americano pueda potencialmente intervenir en el ejercicio de un derecho humano. En *Kimel vs. Argentina*,<sup>115</sup> el demandante, el señor Eduardo Gabriel Kimel, investigador, escritor e investigador histórico, fue demandado por un Juez bajo el cargo de calumnia, ya que en “La masacre de San Patricio”, libro escrito por Kimel, se criticaban las investigaciones sobre dicho evento al igual que las acciones de las autoridades, incluido el juez demandante. En la sentencia del juicio, la Sala IV de la Cámara de Apelaciones de Argentina condenó al señor Kimel, por el delito de calumnia, a un año de prisión y una multa de 20 mil pesos argentinos.<sup>116</sup> En el fondo del caso se encontraba el conflicto entre la libertad de expresión sobre temas de interés público y la protección de la honra de los funcionarios públicos.<sup>117</sup>

Durante el análisis del tema, la Corte IDH examinó los grados de lesividad que representaban las alternativas existentes para alcanzar el fin legítimo perseguido en el caso y así determinar si cumplían con el requisito de necesidad,<sup>118</sup> para ello retoma las precisiones hechas en el caso *Chaparro Álvarez y Lapo Íñiguez vs Ecuador*, en cuyo párrafo 93, consagrado a los requerimientos que debe cumplir toda restricción al derecho a la libertad, indica:

[N]o es suficiente que toda causa de privación o restricción al derecho a la libertad esté consagrada en la ley, sino que es necesario que esa ley y su aplicación respeten

---

<sup>115</sup> Corte IDH, *Caso Kimel vs. Argentina*. Fondo, reparaciones y costas, Serie C. Núm. 177, Sentencia de 2 de mayo de 2008.

<sup>116</sup> Corte IDH, *Caso Kimel vs. Argentina*. Fondo, Reparaciones y costas, Serie C. Núm. 177, Sentencia de 2 de mayo de 2008, § 2.

<sup>117</sup> Corte IDH, *Caso Kimel vs. Argentina*. Fondo Reparaciones y costas, Serie C. Núm. 177, Sentencia de 2 de mayo de 2008, § 51

<sup>118</sup> Corte IDH, *Caso Kimel vs. Argentina*. Fondo, reparaciones y costas, Serie C. Núm. 177, Sentencia de 2 de mayo de 2008, § 51

los requisitos que a continuación se detallan, a efectos de que dicha medida no sea arbitraria: i) que la finalidad de las medidas que priven o restrinjan la libertad sea compatible con la Convención. [...] ii) que las medidas adoptadas sean las idóneas para cumplir con el fin perseguido; iii) que sean necesarias, en el sentido de que sean absolutamente indispensables para conseguir el fin deseado y que no exista una medida menos gravosa respecto al derecho intervenido entre todas aquellas que cuentan con la misma idoneidad para alcanzar el objetivo propuesto. [...] y iv) que sean medidas que resulten estrictamente proporcionales, de tal forma que el sacrificio inherente a la restricción del derecho a la libertad no resulte exagerado o desmedido frente a las ventajas que se obtienen mediante tal restricción y el cumplimiento de la finalidad perseguida.<sup>119</sup>

La Corte vuelve a retomar este párrafo cuando examina la proporcionalidad de la acción: “En este último paso del análisis se considera si la restricción resulta estrictamente proporcional, de tal forma que el sacrificio inherente a aquella no resulte exagerado o desmedido frente a las ventajas que se obtienen mediante tal limitación”, para después agregar:

La Corte ha hecho suyo este método al señalar que: “para que sean compatibles con la Convención las restricciones deben justificarse según objetivos colectivos que, por su importancia, preponderen claramente sobre la necesidad social del pleno goce del derecho que el artículo 13 de la Convención garantiza y no limiten más de lo estrictamente necesario el derecho proclamado en dicho artículo. Es decir, la restricción debe ser proporcional al interés que la justifica y ajustarse estrechamente

---

<sup>119</sup> Corte IDH, *Caso Chaparro Álvarez y Lapo Íñiguez vs. Ecuador*. Excepciones preliminares, Fondo, Reparaciones y Costas, Serie C, núm. 170. Sentencia de 21 de noviembre de 2007. § 93

al logro de ese legítimo objetivo, interfiriendo en la menor medida posible en el efectivo ejercicio del derecho a la libertad de expresión” [59]<sup>120 121</sup>

El organismo jurisdiccional interamericano complementa su reflexión sobre la necesidad y proporcionalidad que deben guardar las acciones de las autoridades cuando estas potencialmente podrían comprometer el ejercicio de un derecho humano, con la ponderación de derechos en aparente pugna. La Corte declaró en el párrafo 84 del caso *Kimel vs Argentina* que al ponderar la restricción de un derecho en favor de otro, debe analizarse i) el grado de afectación de uno de los bienes en juego, determinando si la intensidad de la afectación fue grave, intermedia o moderada; ii) la importancia con respecto a la satisfacción del bien contrario, y ii) si esta satisfacción justifica realmente la restricción del otro<sup>122</sup>

La interceptación y grabación de conversaciones por parte de autoridades gubernamentales es la base del caso *Tristán Donoso vs. Panamá*<sup>123</sup>. Los hechos giran en torno al abogado Tristán Donoso quien asistía legalmente a Walid Zayed, detenido en el marco legal de un proceso por lavado de dinero. El señor Zayed alegó que había recibido visitas exigiendo dinero a cambio de su libertad, por lo tanto, pidió grabar, con ayuda de las autoridades, las presuntas extorsiones dentro del cuartel de la policía de Colón. Posteriormente, el Fiscal solicitó autorización al Procurador para grabar los teléfonos residenciales de la familia Zayed y para autorizar a la Policía Nacional de Colón a grabar y filmar las conversaciones y encuentros que sostuviera Walid Zayed, exceptuando familiares y abogados defensores<sup>124</sup>. Dos días antes de esta solicitud, se realizó una llamada entre el señor Donoso y el padre del acusado. Esta conversación fue intervenida, grabada y ulteriormente divulgada por

---

<sup>120</sup> Nota 59 en el original: Cfr. Corte IDH, La Colegiación de Periodistas (Arts. 13 y 29 Convención Americana Sobre Derechos Humanos). Opinión Consultiva OC-5/85, Serie A núm. 5 13 de noviembre de 1985 § 46; *Caso Herrera Ulloa vs. Costa Rica*. Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C. núm. 107, Sentencia de 2 de julio de 2004, § 121 y 123; *Caso Palamara Iribarne vs. Chile*, Fondo, Reparaciones y Costas. Serie C, núm. 155, Sentencia de 22 de noviembre de 2005 § 85, y *Caso Claude Reyes y otros vs. Chile*. Fondo, Reparaciones y Costas, Serie C, núm. 151, Sentencia de 19 de septiembre de 2006, § 94.

<sup>121</sup> Corte IDH, *Caso Kimel vs. Argentina*. Fondo, reparaciones y costas, Serie C. Núm. 177, Sentencia de 2 de mayo de 2008, § 83.

<sup>122</sup> Corte IDH, *Caso Kimel vs. Argentina*. Fondo, reparaciones y costas, Serie C. Núm. 177, Sentencia de 2 de mayo de 2008, § 84.

<sup>123</sup> Corte IDH, *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, Fondo, Reparaciones y Costas, Serie C. núm. 193, Sentencia de 9 de enero de 2009.

<sup>124</sup> Corte IDH, *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, Fondo, Reparaciones y Costas, Serie C. núm. 193, Sentencia de 9 de enero de 2009, § 39

Procurador José Antonio Sossa Rodríguez. El demandante señala que estas acciones violaron el artículo 11, protección de la honra y de la dignidad,<sup>125</sup> de la Convención Americana sobre Derechos Humanos.

Sobre el tema, la Corte IDH declara que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas y arbitrarias cometidas tanto por terceros como por las autoridades públicas. Y si bien, las conversaciones telefónicas no están expresamente mencionadas o previstas en el artículo 11 de la Convención, debe entenderse que se tratan de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de la protección del derecho a la vida privada. Sin embargo, acota, este derecho no es absoluto y, por lo tanto, es susceptible de restricciones por parte de los Estados. Las injerencias resultado de las restricciones nunca deben ser abusivas o arbitrarias, para ello deben estar previstas en la ley, perseguir un fin legítimo y cumplir cabalmente con los requisitos de idoneidad, necesidad y proporcionalidad, esto es, deben ser necesarias en una sociedad democrática<sup>126</sup>

Más adelante, la Corte señala que la conversación divulgada entre el señor Adel Zayed y el abogado Donoso era de carácter privado, en donde ninguna de las dos personas consistió que fuera conocida por terceros. Aún más, dado que dicha llamada telefónica se llevó a cabo entre presunta víctima y su cliente, debería reservar un grado mayor de protección, por implicar secreto de tipo profesional.<sup>127</sup>

La Corte IDH sentencio al Estado panameño no por la interceptación y grabación telefónica, ya que las pruebas determinaron que el origen de la grabación era privado, es decir fue

---

<sup>125</sup> El artículo 11 dispone 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 en contra de esas injerencias o esos ataques. Convención Americana sobre Derechos Humanos. Organización de los Estados Americanos, 1969

<sup>126</sup> Corte IDH, *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, Fondo, Reparaciones y Costas, Serie C. núm. 193, Sentencia de 9 de enero de 2009, § 55 y 56

<sup>127</sup> Corte IDH, *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, Fondo, Reparaciones y Costas, Serie C. núm. 193, Sentencia de 9 de enero de 2009, § 75.

realizada por un particular y no por las autoridades<sup>128</sup>, pero sí lo hizo por la divulgación de la conversación.<sup>129</sup>

En *Escher y otros vs. Brasil*, la Corte IDH, al interpretar el art. 11 de la Convención, extiende el ámbito de la protección a la no injerencia arbitraria en las conversaciones privadas, aplicándolo no solo al contenido de dichas conferencias, sino también a los metadatos que las identifican. Expresa:

[E]l artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación.<sup>130</sup>

Queda así enmarcado el deber de las autoridades de respetar y proteger, a la vez, la privacidad de las conversaciones y los datos concomitantes a las mismas que pudieran arrojar información relevante sobre la identidad de las personas participes o poner en riesgo su intimidad personal.

## 2.2. Derecho Interno

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) protege tanto el derecho a la privacidad como a la protección de los datos personales. En el primer párrafo se lee: “Nadie puede ser molestado en su persona, familia, domicilio, papeles o

---

<sup>128</sup> Corte IDH, *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, Fondo, Reparaciones y Costas, Serie C. núm. 193, Sentencia de 9 de enero de 2009, § 64.

<sup>129</sup> Corte IDH, *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, Fondo, Reparaciones y Costas, Serie C. núm. 193, Sentencia de 9 de enero de 2009, § 83.

<sup>130</sup> Corte IDH, *Caso Escher vs. Brasil*. Excepciones preliminares, Fondo, Reparaciones y Costas, Serie C. núm. 200, Sentencia de 6 de julio de 2009, § 114

posiciones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento”, más adelante, en el segundo párrafo se decreta que:

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 derechos de terceros.<sup>131</sup>

En el mismo artículo también se estipula la protección sobre las comunicaciones privadas y los requerimientos legales para su interceptación. Dice:

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.

[...]

---

<sup>131</sup> Constitución Política de los Estados Unidos Mexicanos. Art. 16, Párrafo segundo.

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.<sup>132</sup>

Las salvaguardas que la Constitución establece para la protección al derecho a la privacidad en las comunicaciones electrónicas son claras al precisar la necesidad de una autorización judicial federal para iniciar un proceso de interceptación, al igual que la especificación sobre el tipo de intervención, los sujetos bajo este régimen y la duración del mismo. En concordancia con lo anterior, se destaca el deber de fundamentación y motivación que deben cumplir las autoridades para emprender las intervenciones estatales.

Sobre la cuestión, la Suprema Corte de Justicia de la Nación (SCJN) ha manifestado que la protección constitucional sobre las comunicaciones privadas incluye todas las formas existentes de comunicación y también contempla a aquellas que sean fruto de la evolución tecnológica, incluidas las formas de comunicación a través del internet.<sup>133</sup>

Ahondando en el nivel de protección con respecto a los datos y no solo a las conversaciones, la SCJN, en el Amparo en Revisión 1621/2010, expresa que:

El objeto de protección constitucional del derecho a la inviolabilidad de las comunicaciones privadas [...] no hace referencia únicamente al proceso de comunicación, sino también a aquellos datos que identifican la comunicación. A fin de garantizar la reserva que se predica de todo proceso comunicativo privado, resulta indispensable que los datos externos de la comunicación también sean protegidos. Esto se debe a que, si bien es cierto que los datos no se refieren al contenido de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre las circunstancias en que se ha producido la comunicación, afectando así, de modo directo o indirecto, la privacidad de los comunicantes. Estos datos, que han sido denominados habitualmente como "datos de tráfico de las comunicaciones", deberán ser objeto de análisis por parte del intérprete, a fin de determinar si su interceptación y

---

<sup>132</sup> Constitución Política de los Estados Unidos Mexicanos. Art. 16, Párrafos 12, 13 y 15

<sup>133</sup> SCJN, Primera Sala. *Amparo en Revisión 1621/2010*, Semanario Judicial de la Federación y su Gaceta, Novena época, t. XXXIV, agosto de 2011; y SCJN, Primera Sala, *Contradicción de Tesis 194/2012*, Semanario Judicial de la Federación y su Gaceta, Libro XVII, t. 1, Febrero de 2013

conocimiento antijurídico resultan contrarios al derecho fundamental en cada caso concreto. Así, de modo ejemplificativo, el registro de los números marcados por un usuario de la red telefónica, la identidad de los comunicantes, la duración de la llamada telefónica o la identificación de una dirección de protocolo de internet (IP), llevados a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las comunicaciones, puede provocar su vulneración.<sup>134</sup>

Dentro de este contexto, en la Contradicción de Tesis 194/2012, surgida por el desacuerdo en el que se encontraban dos tribunales con respecto a si cuando la autoridad ministerial o los agentes a su mando revisan, extraen o utilizan los datos contenidos en un aparato celular constituye una violación a la intervención de comunicaciones privadas, la SCJN manifestó que:

Los archivos electrónicos almacenados en teléfonos celulares merecen la protección que se les otorga a las comunicaciones privadas, ya que actualmente, a través de esos medios, pueden resguardarse datos privados e íntimos de las personas, en forma de texto, audio, imagen o video, los cuales, de revelarse a terceros, pueden llegar a afectar la intimidad y privacidad de alguien, en ocasiones, con mayor gravedad y trascendencia que la intervención a una comunicación verbal o escrita, o incluso a un domicilio particular; luego, no existe razón o disposición constitucional alguna que impida extender la garantía de inviolabilidad de las comunicaciones privadas a los teléfonos celulares que sirven para comunicarse, además de verbalmente, mediante el envío y recepción de mensajes de texto, y de material audiovisual, así como para conservar archivos en los formatos ya referidos y acceder a cuentas personales en Internet, entre otras funciones afines, máxime que la Constitución Federal no limita su tutela a las formas escritas y verbales de comunicación, sino que alude a las comunicaciones privadas en general<sup>135</sup>

Retomando el Amparo en Revisión 1621/2010, la Suprema Corte considera que el derecho a la inviolabilidad de las comunicaciones se vulnera en el instante mismo que se escucha,

---

<sup>134</sup> SCJN, Primera Sala. *Amparo en Revisión 1621/2010*, Semanario Judicial de la Federación y su Gaceta, Novena época, t. XXXIV, agosto de 2011.

<sup>135</sup> SCJN, Primera Sala, *Contradicción de Tesis 194/2012*, Semanario Judicial de la Federación y su Gaceta, Libro XVII, t. 1, Febrero de 2013, p. 397

graba, almacena, lee o registra una conversación privada sin el debido consentimiento de las personas involucradas, separadamente de que el contenido de la conversación sea difundido públicamente, por lo tanto, un correo electrónico se estima intervenido o interceptado ilegalmente cuando se viola la clave de seguridad (contraseña), con independencia del análisis del contenido del correo electrónico.<sup>136</sup>

Mientras que en estos razonamientos la Corte extiende el derecho a la privacidad, la inviolabilidad de las conversaciones privadas y a la protección de los datos personales, no todos los tipos de datos o metadatos son objeto de la misma protección. En la acción de inconstitucionalidad 32/2012<sup>137</sup> la mayoría de los magistrados resolvieron que era constitucional una disposición que, sin necesidad de tener autorización judicial federal, facultaba a la entonces Procuraduría General de la República (PGR) a conocer y monitorear la localización geográfica, en tiempo real, de un teléfono móvil.

### 2.2.1 Regulación sobre la intervención a las comunicaciones privadas

México no dispone de una regulación específica para programas o herramientas intrusivas del tipo *Pegasus* (software malicioso), sin embargo, como ya se observó en el art. 16 de la CPEUM, sí se encuentra contemplada la opción de intervención e interceptación de las comunicaciones privadas por parte de las autoridades que dispongan de una autorización judicial federal. Concretamente, en la Tesis aislada resultado del Amparo en Revisión 964/2015,<sup>138</sup> la SCJN establece que las únicas autoridades con facultades para realizar actos de intervención son<sup>139</sup>:

**-El o la titular de la Procuraduría General de la República, así como las y los procuradores de las entidades federativas.** Se contempla en el Código Nacional de Procedimientos Penales que en los casos que el Ministerio Público considere necesario, se

---

<sup>136</sup> SCJN, Primera Sala. *Amparo en Revisión 1621/2010*, Semanario Judicial de la Federación y su Gaceta, Novena época, t. XXXIV, agosto de 2011

<sup>137</sup> SCJN, Pleno. *Acción de Inconstitucionalidad 32/2012*, p. 131

<sup>138</sup> SCJN, Segunda Sala, *Tesis 2ª XLIV/2016 (10ª)*, Semanario Judicial de la Federación, Décima Época. Agosto de 2016.

<sup>139</sup> Comprendidas durante el periodo que abarca esta investigación: 2012-2018. Con la llegada del Presidente Andrés Manuel López Obrador, el 1ro de Diciembre de 2018, la PGR devendría en la Fiscalía General de la República; el CISEN se transformaría en el Centro Nacional de Inteligencia (CNI) y la Policía Federal pasaría a ser parte de la Guardia Nacional.

puede realizar una intervención en las comunicaciones privadas para la investigación de un delito. Es en los artículos 291 a 302 que se establece el procedimiento, así como los requisitos y plazos correspondientes para la solicitud de autorización judicial. Respecto a que se entiende por intervención de comunicaciones privadas, dice:

(...) 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.<sup>140</sup>

Complementariamente y concerniente a delitos específicos, en la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro (Art. 24) y en la Ley contra la Delincuencia Organizada (Arts. 15 – 28), se encuentran regulaciones similares para la investigaciones específicas en esos escenarios.

**-La Policía Federal.** En el artículo 48 de la Ley de la Policía Federal se establece que la intervención de comunicaciones privadas solamente puede autorizarse “cuando se constate la existencia de indicios suficientes que acrediten que se está organizando la comisión de los delitos señalados en el artículo 51 de esta Ley.”<sup>141</sup>, los procedimientos y especificaciones se desarrollan del artículo 48 al 55. Los Artículos 219, 220 y 221, correspondientes al Capítulo Único, “Técnicas Especiales de Investigación”, sección segunda, del Reglamento de la Ley de la Policía Federal, conciernen a la intervención de comunicaciones privadas.

**-El Centro de Investigación y Seguridad Nacional (CISEN):** En la Ley de Seguridad Nacional se decretó en los artículos 33 al 49 los lineamientos a seguir para la interceptación de comunicaciones privadas, esta puede realizarse, previa autorización judicial federal, en casos de amenazas inminentes a la seguridad nacional, detalladas en el artículo 5 de la misma Ley: “actos tendentes a consumir espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional”<sup>142</sup>

---

<sup>140</sup> Código Nacional de Procedimientos Penales, Artículo 291, primer párrafo. Estados Unidos Mexicanos

<sup>141</sup> Ley de la Policía Federal, artículo 48. Estados Unidos Mexicanos

<sup>142</sup> Ley de Seguridad Nacional, artículo 5, numeral I. Estados Unidos Mexicanos

## 2.2.2 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Publicada en el Diario Oficial de la Federación el 26 de enero de 2017, esta ley regula y establece las bases, principios y procedimientos que deben seguirse para garantizar el derecho de toda persona a la protección de sus datos personales, específicamente para aquellos en posesión de sujetos obligados, entiéndase por sujetos obligados toda autoridad, entidad, órgano y organismos de los Poderes Ejecutivo, Legislativo y Judicial, así como órganos autónomos, partidos políticos, fideicomisos y fondos públicos en el ámbito federal, estatal y municipal.

La LGPDPSO define a los datos personales como “cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información”<sup>143</sup>, mientras que los datos personales sensibles son “aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como el origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual”<sup>144</sup>

El tratamiento de los datos personales es entendido como “cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales”<sup>145</sup>

En el artículo 6° de la ley se establecen las únicas circunstancias bajo las cuales se limitará el derecho a la protección de los datos personales, estas son: razones de seguridad nacional (en términos de la ley de la materia), disposiciones de orden público, seguridad y salud pública así como para proteger los derechos de terceras personas. El artículo 7° establece que

---

<sup>143</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 3°. Numeral IX

<sup>144</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 3°. Numeral X

<sup>145</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 3°. Numeral XXXIII

los datos sensibles, por regla general, no podrán ser objetos de tratamiento, salvo que se cuente con el expreso de su titular o en su defecto, se encuentre dentro de uno de los casos del artículo 22 de la LGPDPPSO, también se menciona que en casos involucrando a menores de edad, se deberá privilegiar el interés superior del niño, niña o adolescente.

En el capítulo I de la sesión segunda se encuentran los principios que deben regir el tratamiento de datos por parte de los sujetos obligados. El artículo 16 indica que los responsables deberán observar en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad durante el tratamiento de los datos personales. Por su parte, los artículos 18 y 19 dicen, respectivamente: “Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera”<sup>146</sup>; “El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad”<sup>147</sup>

En el ya mencionado artículo 22 se establece que uno de los escenarios en el que los responsables de tratamiento de datos no estarían obligados a recabar el consentimiento del titular es “cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente”<sup>148</sup>

El capítulo II de la LGPDPPSO, titulado “De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia” expone los límites a los que deben ajustarse estas instancias cuando hagan tratamiento de datos personales y las bases de datos que de estas resulten: “la obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de las 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

---

<sup>146</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 18.

<sup>147</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 19.

<sup>148</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 22, numeral III.

de seguridad nacional, seguridad pública, o para la prevención o persecución de delitos. Deberán ser almacenados en bases de datos establecidas para tal efecto.”<sup>149</sup>

Finalmente, el artículo 81 decreta que las comunicaciones privadas son inviolables, “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.”<sup>150</sup>

---

<sup>149</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 80

<sup>150</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 81, párrafo segundo

## CAPITULO III: PEGASUS, ASPECTOS TÉCNICO-OPERATIVOS SOBRE SU USO ILEGAL EN MÉXICO, 2012 – 2017

### 3.1. ¿Qué es Pegasus?

#### 3.1.1. Sumario.

En varias ocasiones se ha usado la palabra *malware* para referirse a *Pegasus*, pero ¿qué es un malware? dicho termino es la abreviatura de “Malicious Software” (programa malicioso), y hace referencia a un grupo de programas o códigos maliciosos cuyo objetivo es acceder a un dispositivo de forma inadvertida, sin que el usuario se dé cuenta de ello y mucho menos lo autorice. Existen diversos tipos de malware, entre los más comunes se encuentran el spyware (software espía), adware (software publicitario), phishing, virus, troyanos, gusanos, ransomware y secuestradores del navegador.<sup>151</sup>

El programa *Pegasus* pertenece a la categoría de los spywares. Fue desarrollado por la firma israelí de ciber-seguridad NSO Group con el objetivo de “piratear” cualquier teléfono celular que opere bajo los sistemas iOS y Android y con ello robar datos provenientes de los dispositivos infectados. El tipo de contenidos que este programa recauda incluye mensajes de texto, correos electrónicos, *key logs*<sup>152</sup>, audio e información proveniente de aplicaciones instaladas en el celular, como Facebook, WhastApp o Instagram. Este spyware también puede grabar conversaciones telefónicas y de video, además de tomar fotos usando la cámara del aparato<sup>153</sup>

De acuerdo a declaraciones de NSO Group hechas a Forbes<sup>154</sup>, la misión de esa empresa es hacer del mundo un lugar más seguro “al proporcionar a los gobiernos autorizados tecnología que les ayude a combatir el terrorismo y la delincuencia”, también declaran que la compañía

---

<sup>151</sup> Advast, “¿Qué es un malware?”, Advast Software, s.r.o., s/f, disponible en: <https://www.avast.com/es-es/c-malware>, consultado el 29 de junio de 2019

<sup>152</sup> De “keylogger” es una herramienta que permite registrar las pulsaciones en el teclado de un equipo. Ver: Malenkovich, Serge, “¿Qué es un keylogger?”, Kaspersky Latinoamerica, 9 de abril de 2013, disponible en: <https://latam.kaspersky.com/blog/que-es-un-keylogger-2/453/>, consultado el 29 de junio de 2019.

<sup>153</sup> Rouse, Margaret, “Definition Pegasus Malware”, TechTarget SearchSecurity, última actualización, 28 de junio de 2019, disponible el: <https://searchsecurity.techtarget.com/definition/Pegasus-malware>, consultado el 30 de junio de 2019.

<sup>154</sup> Fox-Brewster, Thomas, “NSO Group: Los espías israelíes que hackean iPhones con un solo SMS”, Forbes México, 18 de abril de 2017, disponible en: <https://www.forbes.com.mx/nso-group-los-espías-israelíes-que-hackean-iphones-con-un-solo-sms/>, consultado el 25 de mayo de 2019

“sólo vende a agencias gubernamentales autorizadas, y (...) que los acuerdos firmados con los clientes de la empresa requieren que los productos de la empresa sólo se utilicen de manera legal. Específicamente, los productos sólo pueden utilizarse para la prevención e investigación de delitos.”

### 3.1.2 *Cómo funciona Pegasus.*

La compañía de ciber-seguridad Lookout elaboró un reporte sobre las especificaciones técnicas y operativas bajo las cuales funciona el software *Pegasus*<sup>155</sup>, en él se especifica que éste es un sistema en extremo sofisticado que usa una fuerte encriptación para protegerse a si mismo de las herramientas tradicionales de seguridad, además de contar con un monitoreo externo contaste y dispone de un mecanismo de auto destrucción. Los investigadores de Lookout determinaron que el spyware se aprovecha de tres vulnerabilidades “*zero-day*” (nombradas *Trident*) para adentrarse y apropiarse de la información contenida en los dispositivos con el sistema operativo iOS de Apple. Las vulnerabilidades detectadas son:

-*CVE 2016-4657: Memory Corruption in WebKit*: vulnerabilidad en el navegador web Safari que le permite al atacante comprometer el dispositivo cuando el usuario entra en un link específico.

-*CVE-2016-4655: Kernel Information Leak*: esta debilidad en el mecanismo admite que información del teléfono se filtre al atacante con lo cual éste puede localizar la memoria *kernel* y acceder a las distintas aplicaciones del dispositivo.

-*CVE-2016-4656: Kernel Memory corruption leads to Jailbreak*: las vulnerabilidades en el nivel *kerner* en celulares con iOS de 32 y 64 bits permiten que el atacante rompa<sup>156</sup> los candados digitales de seguridad del dispositivo y con ello, tenga libertad de instalar el software de vigilancia “silenciosamente” (sin que el usuario se percate).

Los ataques de infección suceden en este orden: primero se envía un SMS engañoso personalizado con un enlace URL falso, este mensaje tiene como finalidad hacer que el

---

<sup>155</sup> Bazaliy, M, Flossman, M. Blaich, A. et al, “*Technical Analysis of Pegasus Spyware*”, Lookout Security Inc, S/F, disponible en: <https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf>, consultado el 4 de julio de 2019

<sup>156</sup> “*Jailbreak*” en el original.

usuario blanco del ataque abra el enlace adjunto. Los mensajes se valen de estrategias diversas para llamar la atención de la persona y provocar que ella acceda al link sin dudar.

Si la persona hace click en el link malicioso se abre el navegador de internet para acceder a un sitio web (*Anonymizer*) que manda una solicitud al servidor de quien opera el ataque, *Pegasus Installation Server*, ahí se encuentra alojado el malware. Es en ese servidor donde se examina si existen debilidades en el equipo (en este caso, la cadena *Trident*), si las hay se instala el software, en caso contrario se redirige a un sitio web autentico para evitar sospechas. Una vez instalado el software este opera recolectando y enviando la información a una estación de trabajo fija, *Pegasus Working Station*.<sup>157</sup>

Lo único que el usuario observa, si la infección fue exitosa, es que el navegador Safari se abre para después cerrarse inmediatamente.

### 3.2. Cómo Pegasus llegó a México

#### 3.2.1 Relatoría de hechos.

Las investigación “*PGR compró Pegasus a prestanombres*”, publicada por Mexicanos contra la corrupción y la impunidad A.C. el 28 de julio de 2017, es la reconstrucción de hechos más cercana y exacta de la que disponemos para rastrear la llegada del software *Pegasus* a México<sup>158</sup>, en dicha investigación se relatan los medios de los cuales se valieron funcionarios de la extinta Procuraduría General de la Republica (PGR) para conseguir el software de espionaje mencionado. A continuación se presenta un re elaboración cronológica de los hechos tomando como base los contenidos de la investigación recién mencionada, al igual que datos provenientes de los reportes “*El estado de vigilancia. Fuera de control*”<sup>159</sup> y “*Gobierno Espía*”<sup>160</sup>, documentos de indagación provenientes de la sociedad civil

---

<sup>157</sup> Marczak, Bill y Scott-Railton, John, “*The Million Dollar Dissident. NSO Group’s Iphone Zero-Days used against a UAE Human Rights Defender*”, Citizen Lab, Universidad de Toronto, 24 de agosto de 2016, disponible en: <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>, consultado el 24 de febrero de 2019

<sup>158</sup> Olmos, Raul; Durán, Valeria y Lizárraga Daniel, “*PGR compró Pegasus a prestanombres*”, Mexicanos Contra la Corrupción y la Impunidad A. C., México, D.F., 28 de Julio de 2017, disponible en: <https://contralacorrupcion.mx/web/pgrcompropegasus/index.html>, consultado el 12 de mayo de 2019.

<sup>159</sup> R3D, “*El estado de vigilancia...*” op. cit. Pp. 97 - 100

<sup>160</sup> R3D, Artículo 19 y Social TIC, “*Gobierno Espía. Vigilancia sistemática a periodistas y defensores derechos humanos en México*”, Ciudad de México, junio de 2017, disponible en: <https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf>, consultado el 12 de marzo de 2019. Pp 63-66

organizada sobre el espionaje tecnológico ilegal en México. Junto a estos tres informes se agregan las acotaciones o agregados pertinentes provenientes de fuentes complementarias.

Para facilitar la lectura se ha decidido hacer una narración de tipo lineal, es decir, se siguen los hechos en una sucesión temporal continua, siempre teniendo como eje central la negociación para la adquisición de *Pegasus* por parte de las autoridades mexicanas. De igual manera, para hacer más ágil la identificación y comprensión de individuos y relación de hechos dentro del relato, se incluye en el apartado inmediato un dibujo de los perfiles de los actores más importantes en la transacción por *Pegasus*.

### 3.2.1.1 Perfiles.

-**Tomas Zerón de Lucio**, ex director de la Agencia de Investigación Criminal de la Procuraduría General de la República (PGR), nombrado en tal puesto en 2013 por el entonces procurador General de la República, Jesús Murillo Karam. Su carrera como servidor público incluyen los puestos de Jefe de Sección en la Policía Federal Preventiva, Comisionario Jefe en la Secretaría de Seguridad Pública Federal, titular de la Dirección General de Inteligencia<sup>161</sup>. Posterior a su cargo en la PGR, fue Secretario Técnico del Consejo Nacional de Seguridad durante el mandato de Enrique Peña Nieto (EPN). De acuerdo con su perfil en el Portal Oficial de internet del Gobierno de México, entre sus actividades como Secretario Técnico estaban “propone[r] al consejo las políticas, lineamientos y acciones en materia de Seguridad Nacional y el contenido del Programa para la Seguridad Nacional, [también] realiza[r] estudios especializados en materias relacionadas con la Seguridad Nacional, el inventario de la infraestructura estratégica del país y el requerimiento de información necesaria a las dependencias federales para la Seguridad Nacional”<sup>162</sup>

Zerón de Lucio ha sido objeto de escrutinio público porque él fue el encargado de la investigación de la desaparición de los 43 normalistas de Ayotzinapa el 26 y 27 de septiembre de 2014, en Iguala, Guerrero (situación que se entrelazará con nuestro análisis

---

<sup>161</sup> El Universal, “*Perfil. Tomás Zerón de Lucio*”, México, D.F., 14 de septiembre de 2016, Disponible en: <https://www.eluniversal.com.mx/articulo/nacion/2016/09/14/perfil-tomas-zeron-de-lucio>, Consultado el 17 de mayo de 2019.

<sup>162</sup> Gobierno de México. “*Directorio Tomas Zerón de Lucio*”, Portal del Gobierno de México, Directorio. Disponible en: <https://www.gob.mx/epn/estructuras/tomas-zeron-de-lucio>, Consultado el 17 de mayo de 2019

eventualmente). En la *Recomendación 15VG/2018*, hecha por la Comisión Nacional de los Derechos Humanos por el caso de los 43, se pedía una investigación a Zerón de Lucio por irregularidades en su accionar durante la investigación<sup>163</sup>.

**-Asaf Zanzuri**, de origen israelí, es el creador de Balam Seguridad Privada. De acuerdo con la descripción en su página de internet, él es ingeniero electrónico, con más de 12 años de experiencia laboral en los sectores de seguridad, tecnología, cibernética e inteligencia, en diversos países de Europa, “después de realizar 8 años este tipo de trabajo, decidió abrirse y crear su propia empresa. Desde entonces se desempeña como director ejecutivo de la misma”<sup>164</sup>

En su perfil de *crunchbase* se lee que entre sus clientes se encuentran los gobiernos de Israel, Colombia y Chile, “en (sic.) los cuales la compañía suministra sistemas de inteligencia y salas de control cibernéticos. Otros clientes incluyen el ejército y la marina mexicana, la policía nacional de Chile y la policía nacional de Perú. (...) Asaf y su compañía están ahí para proveerlos con equipos militares, sistemas de seguridad y aeronaves civiles de primer nivel”<sup>165</sup>

**-Rodrigo Ruiz de Teresa Treviño**, socio de Balam Seguridad. Tiene dentro de sus familiares a Guillermo Ruiz de Teresa, su tío, quien fuera dirigente del sector popular del PRI y coordinador de Puertos y Marina Mercante de la SCT. En el perfil que se encuentra en *crunchbase* se describe a Rodrigo como “un joven emprendedor que se ha desempeñado como socio minoritario en varios restaurantes y clubes nocturnos”<sup>166</sup>. En el resumen biográfico que se encuentra en su página blog se menciona que “además de ser un prominente empresario en el sector restaurantero y participar con varias hoteleras, desde el 2014 Rodrigo se ha iniciado en la Industria de la Tecnología de la Seguridad Privada fundando la empresa

---

<sup>163</sup> Carrasco Araizaga, J., “Tomas Zerón se dice dispuesto a que lo investiguen la Comisión para Ayotzinapa”, Proceso, CDMX, 16 de enero, 2019, disponible en: <https://www.proceso.com.mx/567916/tomas-zeron-se-dice-dispuesto-a-que-lo-investigue-la-comision-para-ayotzinapa>, consultado el 13 de julio de 2019.

<sup>164</sup> Wordpress, Home, Asaf Anzuri, disponible en: <https://asafzanzuri.wordpress.com/>, consultado el 19 de mayo de 2019.

<sup>165</sup> Crunchbase, Person: Asaf Anzuri, disponible en: <https://www.crunchbase.com/person/asaf-zanzuri#section-overview>, consultado el 19 de mayo de 2019.

<sup>166</sup> Crunchbase, Person: Rodrigo Ruiz De Teresa Treviño, disponible en: <https://www.crunchbase.com/person/rodrigo-ruiz-de-teresa-trevino#section-overview>, consultado el 21 de mayo de 2019.

Balam Seguridad Privada, la cual provee sistemas de seguridad de la más alta gama a diferentes países como México, Colombia, Nigeria, entre otros.”<sup>167</sup>

-**Carlos Cayetano Miguel**, de 26 años en el 2017, fungía como dueño y administrador único de Tech Bull cuando se llevó acabo la venta de *Pegasus* a la PGR en el 2014. Se licenció como contador público en el Instituto Politécnico Nacional, por la tesis “Conversión de estados financieros a moneda extranjera en el sector alimentos”, obteniendo su cédula en el 2014<sup>168</sup>.

-**Jorge de Jesús Sánchez**, de 29 años de edad en el 2017, es técnico en informática egresado del Conalep, aparece como socio de Tech Bull<sup>169</sup>. No se tienen más registros sobre otras actividades empresariales, académicas o laborales

-**Luis Armando Pérez Herero**, procedente de Hidalgo, es el apoderado general en Tech Bull. Su formación es como licenciado en Ingeniería en sistemas computacionales por el Instituto de Estudios Superiores del Valle de Orizaba, Veracruz. Tenía 34 años de edad en el 2017<sup>170</sup>.

-**NSO Group**: es una firma israelí de ciber-seguridad fundada en el 2009 por Niv Carmi, Ormi Lavie y Shalev Hulio. El antiguo presidente de la junta de directivos en NSO es el general retirado Avigdor Ben-Gal, quien fuera cabecera de “*Israel Aerospace Industries*” en los 90’s<sup>171</sup>. En el sitio web de la compañía<sup>172</sup> se indica que ellos desarrollan tecnología que permite a los servicios de inteligencia de los gobiernos prevenir e investigar el terrorismo y el crimen. Más adelante se remarca que los “Productos de NSO son usados exclusivamente

---

<sup>167</sup> RodrigoRuizTeresaBlog, Home, disponible en: <https://rodrigoruzdeteresa.mx/index.html>, consultado el 21 de mayo de 2019.

<sup>168</sup> El Universal, “*Perfil, Carlos Cayetano*”, México, D.F., 29 de julio de 2017. Disponible en: <https://www.eluniversal.com.mx/articulo/nacion/seguridad/2017/07/29/perfil-carlos-cayetano>, consultado el 19 de mayo de 2019.

<sup>169</sup> Olmos, Raul, Mexicanos Contra la Corrupción y la Impunidad, “*Funcionario Federal era uno de los socios del grupo empresarial que vendió Pegasus*”, Animal Político, México, D.F. 20 de febrero de 2018, disponible en: <https://www.animalpolitico.com/2018/02/funcionario-federal-empresa-pegasus-pgr/>, consultado el 20 de mayo de 2019.

<sup>170</sup> Olmos, Raul; Durán et al, “*PGR compró Pegasus*”, *op. cit.*

<sup>171</sup> Hirschauge, Ory y Orpaz, Inbal; “*U.S. Fun to Buy NSO and Its Smartphone-snooping Software*” Haaretz, Israel News, 17 de febrero de 2014, disponible en: <https://www.haaretz.com/israel-news/business/u-s-fund-to-buy-snooping-software-1.5323394>, consultado el 24 de mayo de 2019.

<sup>172</sup> NSO Group, About US, NSO Grup web page, disponible en: <https://www.nsogroup.com/about-us/>, consultado el 4 de agosto de 2019.

por agencias gubernamentales de inteligencia y de seguridad para combatir el crimen y el terror”. Destacan que sus equipos han sido empleados en escenarios que involucran la prevención del terrorismo, (tirotesos, coches bomba y ataques suicidas) así como en casos de desmantelación de grupos de pedofilia, tráfico de drogas y lavado de dinero.

**-Hacking Team:** compañía italiana, con sede en Milán, exclusivamente dedicada a la seguridad ofensiva, fue fundada en el 2003 por David Vincenzetti y Valeriano Bedeschi. La empresa vende servicios de vigilancia e intrusión tecnológica a dependencias gubernamentales y corporaciones<sup>173</sup>. En el 2015 fueron objeto de una filtración masiva de datos privados (cerca de 400 GB de información) que fue puesta a disposición pública.<sup>174</sup> Después de dicha filtración la compañía sufrió un gran revés en sus negocios y mantuvo un bajo perfil durante algunos meses, sin embargo reportes posteriores indicaron que seguía en activo (2018) y que había sufrido cambios en la estructura de sus accionistas, siendo ahora *Tabled Limited* la propietaria principal, con un 20% de las acciones. *Tabled Ltd.* Tiene su base oficialmente en Chipre. Investigaciones recientes la han relacionado con personajes cercanos al gobierno de Arabia Saudita.<sup>175</sup>

### 3.2.1.2 Negociaciones y compra de *Pegasus*.

Del 2010 al 2012 la Secretaria de la Defensa Nacional (SEDENA) realizó al menos 18 contratos para obtener equipos y servicios de inteligencia. 8 de estos contratos se realizaron con la empresa Security Tracking, SA de CV<sup>176</sup>. La finalidad de estas adquisiciones fue la de mejorar e incrementar las capacidades de espionaje y procesamiento de la información de la SEDENA. La compra de la “Primera Fase del Sistema de Inteligencia Regional para Incrementar las Capacidades de la Sección Segunda del Estado Mayor de la Defensa Nacional” se realizó el 10 de septiembre de 2010. La segunda y tercera fase, ambas del 2012,

---

<sup>173</sup> Batey, Angus, “*The spies behind your screen*”, The Telegraph U.K., 24 de noviembre de 2011, disponible en: <https://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html>, consultado el 1 de junio de 2019.

<sup>174</sup> Wikileaks, Hacking Team leak, 8 de julio de 2005, disponible en: <https://wikileaks.org/hackingteam/emails/>, consultado el 10 de julio de 2019

<sup>175</sup> Kafka, Filip, “*Nuevas señales de que Hacking Team está activo*”, welvesecurity by eset, 13 de marzo de 2018, disponible en: <https://www.welvesecurity.com/la-es/2018/03/13/nuevas-senales-de-que-hacking-team-esta-activo/>, consultado el 4 de junio de 2019.

<sup>176</sup> Camacho, Z. “*Sedena, bajo escrutinio por ocho contratos de 5.6 mil MDP*”. Contralínea, México, D.F., 22 de julio de 2012, disponible en: [https://www.contralinea.com.mx/archivo-  
revista/index.php/2012/07/22/sedena-bajo-escrutinio-por-ocho-c](https://www.contralinea.com.mx/archivo-revista/index.php/2012/07/22/sedena-bajo-escrutinio-por-ocho-c), consultado el 3 de junio, de 2019

sirvieron para la instalación del “Módulo Central de la Plataforma NSO *Pegasus* de Monitoreo de smartphones”.

La empresa Balam Seguridad es fundada el 15 de mayo del 2012 por el ingeniero electrónico israelí Asaf Zanzuri<sup>177</sup>; el 23 de enero de 2013, el empresario mexicano Rodrigo Ruiz Treviño se vuelve socio de la compañía.

10 de octubre de 2013 se crea legalmente la firma Grupo Tech Bull en la Ciudad de México, ante la presencia del notario Alfredo Ayala Herrera. De acuerdo con su acta constitutiva, Carlos Cayetano Miguel es socio y administrador único. Jorge de Jesús también figura como socio. Su capital inicial es de 50 mil pesos.<sup>178</sup>

El 15 de enero de 2014, un ingeniero de Hacking Team (HT), Sergio Rodríguez-Solis, escribe un mail acerca de una visita al Centro de Investigación y Seguridad Nacional de México, (CISEN), menciona que miembros de esa institución habían probado un sistema de infección para teléfonos móviles que funcionaba en el 80% de los dispositivos, (Android, BlackBerry, iOS y Symbian); los empleados del CISEN se quejaron porque HT no contaba con ese tipo de infecciones , “como las de NSO”<sup>179</sup> En el mismo correo electrónico se hace manifiesto el encuentro con personal de la SEDENA, quienes dicen contar y estar encantados con el programa NSO para celulares. Comentan que el precio de NSO inicia en 18 millones. Sergio Rodríguez acota que deben explicar las diferencias de precio por los productos de su empresa y los de NSO Group.

En otro correo electrónico, esta vez del 29 de enero del mismo año, un vendedor de HT, llamado Alex Velasco, escribe que la SEDENA anda en busca de un contrato con 600 agentes. De acuerdo con el mail, “ellos también compraron NSO hace dos años y actualmente

---

<sup>177</sup> Aristegui Noticias, Redacción, “*Revelan vínculos entre proveedor de equipo de espionaje y EPN*”, Aristegui Noticias, México D.F. 25 de junio de 2017, disponible en: <https://aristeguinoticias.com/2506/mexico/revelan-vinculos-entre-proveedor-de-equipo-de-espionaje-y-epn/>, consultado el 2 de julio de 2019.

<sup>178</sup> Olmos, Raul; Durán et al, “*PGR compró Pegasus*”, *op. cit*

<sup>179</sup> Rodríguez Solis, S. E-mail filtrado, Wikileaks, 19 de enero, 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/5275>, consultado el 10 de julio de 2019.

no está funcionando. Fueron engañados por el revendedor de NSO y quieren estar seguros que nosotros no somos solo otra mentira”<sup>180</sup>.

El 26 de agosto del 2014, Alex Velasco envía un correo más a otros miembros de HT, esta vez para informarles que después de hablar con Gilberto<sup>181</sup>, éste le dijo que una persona llamada Ori, estaba apoyando a NSO Group. Ori parece haberse convertido en un buen amigo del hijo del jefe de compras y ofreció NSO por 15 millones. Alex cree que hay algunos “buenos pagos” involucrados en esas transacciones<sup>182</sup>

16 de octubre de 2014, ingresa al Registro Público de Comercio de la Ciudad de México un acta en la que Luis Armando Pérez es designado como el encargado de cobranzas de Tech Bull y nuevo representante ante futuros litigios de Carlos Cayetano, dueño de TB.<sup>183</sup>

La PGR, compra el malware *Pegasus* al Grupo Tech Bull (filial de Balam Seguridad) por 32 millones de pesos, para ser usado en 500 infecciones, el 29 de octubre del 2014. Firman Zerón de Lucio por parte de la PGR y Luis Armando Pérez en representación de Tech Bull<sup>184</sup>

Carlos Cayetano sale oficialmente de Tech Bull el 10 de noviembre de 2014. No conserva relaciones de tipo comercial o personales con otros miembros del equipo.<sup>185</sup>

Con fecha del 28 de noviembre de 2014, Armando Pérez, de Tech Bull, envía un mensaje a Hacking Team mediante correo electrónico, dentro dice que el director de su compañía es Rodrigo Ruiz, quien habló antes por teléfono con alguien de HT llamado Simoneta. Posteriormente pasa a hacer un resumen de su compañía y qué hacen, esto con el fin de entablar una relación comercial. En el cuerpo del escrito, se lee:

---

<sup>180</sup> Velasco, Alex, E-mail filtrado, Wikileaks, 29 de enero de 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/8964>, enlace roto, consultado el 10 de julio de 2019. Ver: R3D, Artículo 19 et al “*Gobierno Espía...*”, op. cit. P. 64

<sup>181</sup> De acuerdo con R3D, se refiere a Gilberto Enríquez, vinculado a la empresa Neolinx quienes vendieron equipos de vigilancia de Hacking Team al estado de Guerrero, el Edo. de México y al CISEN; ver en: R3D, “*El estado de vigilancia...*” op. cit. P. 100, nota al pie, 120.

<sup>182</sup> Velasco, Alex, E-mail filtrado, Wikileaks, 26 de agosto de 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/6584>, consultado el 11 de julio de 2019.

<sup>183</sup> Olmos, Raul; Durán et al, “*PGR compró Pegasus*”, op. cit.

<sup>184</sup> Ídem.

<sup>185</sup> Ídem.

“Nosotros somos una compañía que vende inteligencia y seguridad al gobierno mexicano. Somos subsidiarios de la compañía principal que es Balam Seguridad que es una de las más importantes compañías de seguridad en el país y #1 en la PGR y la Marina. Nuestros mejores clientes, son los marines mexicanos, PGR, CISEN, policía federal, y un montón de procuradurías [...], Nosotros acabamos de vender a la PGR (contrato ya firmado y ellos ya enviaron el dinero) el sistema NSO Pegasus”<sup>186</sup>

Inmediatamente, pasa a relatar que una vez que NSO Group se enteró que ellos habían firmado el contrato decidieron incrementar el precio en un 50%, por lo que Tech Bull canceló con ellos y ahora están buscando hacer trato con el software de HT para cumplir lo pactado con la PGR, sin embargo, el problema es que “Tomas Zeron, quien está a cargo de esta nueva área, trabajó en la PGJ del Edo de México (él compro [ahí] el sistema a ustedes) y les está diciendo a todos que el sistema que ustedes instalaron no sirve y que él no lo quiere en la PGR. Nuestro trabajo es convencerlos de que tu sistema trabaja de manera similar [al de NSO]”<sup>187</sup>

Un día después (29 / nov / 2014), Eric Banoun, un intermediario israelí, indica que Ruiz Treviño era el principal negociador con la PGR y “uno de los mayores jugadores hoy en el campo de las soluciones de inteligencia en México”<sup>188</sup>

En noviembre de 2015, consta en acta administrativa que la PGR recibió el software *Pegasus* para ser usado en contra de 500 objetivos. Noé Ramírez aparece como el administrador y operador de dicho programa. La empresa Tech Bull fue la vendedora quienes ofrecen, además, la capacitación a 25 operadores. Aparecen como testigos firmantes Christian González Lozano, director general adjunto de Sistematización y Seguridad de la Información de la CENAPI; Eduardo Mendoza Juárez, subdirector de Integración de la Información y Apoyo de la misma entidad; además de dos funcionarios de la oficina de la procuradora: Joel

---

<sup>186</sup> Pérez, Armando, E-mail filtrado, Wikileaks, 28 de noviembre, 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/5391>, Consultado el 15 de julio de 2019. La traducción y edición del texto en minúsculas (mayúsculas en el original) es propia.

<sup>187</sup> Ídem.

<sup>188</sup> Proceso, Redacción “Rechaza Balam Seguridad Privada vender el software Pegasus”, Proceso, México D.F. 27 de junio de 2017, disponible en: <https://www.proceso.com.mx/492612/rechaza-balam-seguridad-privada-vender-software-pegasus>, consultado el 9 de julio de 2019

David Torres Ortega, director de área, y Marco Antonio Pérez Guzmán, supervisor operativo.<sup>189</sup>

La cronología de eventos queda de la siguiente manera:

- 10 / 09 / 2010 – La SEDENA compra a Security Tracking, SA de CV la “Primera Fase del Sistema de Inteligencia Regional para Incrementar las Capacidades de la Sección Segunda del Estado Mayor de la Defensa Nacional”

- ¿? / ¿? / 2012 – Se adquieren la Segunda y Tercera Fase del Sistema de Inteligencia Regional para Incrementar las Capacidades de la Sección Segunda del Estado Mayor de la Defensa Nacional”; dichas fases tenían como finalidad la instauración y consolidación del “Módulo Central de la Plataforma NSO Pegasus de Monitoreo de smartphones”

- 15 / 05 / 2012: Se crea la compañía Balam Seguridad Privada. Su fundador es Asaf Sanzuri.

- 23 / 01 / 2013: Rodrigo Ruiz de Teresa Treviño se hace socio de Balam Seguridad Privada

- 10 / 10 / 2013: Grupo Tech Bull se constituye en la Ciudad de México, con la presencia del notario Alfredo Ayala Herrera. Su capital inicial es de 50 mil pesos. Carlos Cayetano aparece en el acta constitutiva como socio y administrador único. Jorge de Jesús aparece como socio también. Tech Bull posteriormente se convierte en filial de Balam Seguridad.

- 10 / 01 / 2014 Se registran acercamientos de la firma italiana Hacking Team con personal del CISEN y la SEDENA para la venta de servicios de espionaje. Durante el transcurso de ese año se menciona una pugna, entre HT y NSO Group, por asegurar contratos con la PGR

- ¿? / ¿? / 2014: Carlos Cayetano obtiene su cédula profesional como contador público.

- 16 / 10 / 2014: Entra al Registro Público de Comercio de la Ciudad de México un acta en donde Carlos Cayetano nombra a Luis Armando Pérez como encargado de cobranzas en Tech Bull así como su representante ante litigios futuros.

---

<sup>189</sup> Milenio Digital, “PGR recibió Pegasus en 2015”, Milenio, México D.F. 28 de junio de 2017, disponible en: <https://www.milenio.com/politica/pgr-recibio-pegasus-en-2015>, consultado el 24 de mayo de 2019.

- 29 / 10 / 2014: Tech Bull vende a la PGR el software espía *Pegasus* por 32 millones de dólares. El contrato se realiza por el servicio de 500 infecciones a equipos celulares mediante ese malware. *Pegasus* fue desarrollado por NSO Group, una empresa con sede en Israel. Las firmas que aparecen en el documento son las de Tomás Zerón por parte de la PGR y Luis Armando Pérez en representación de Tech Bull.

- 07 / 11 / 2014. Se retira Carlos Cayetano de la administración de Tech Bull.

- 28 / 11 / 2014 Luis Armando Pérez negocia con Hacking Team la compra de un software similar a *Pegasus* para cumplir lo acordado con la PGR, después de que NSO Group aumentará el precio estipulado en su contrato.

- 12 / 01 / 2015: *Sucede el primer intento de infección (documentado) por el software Pegasus*<sup>190</sup>

- 12 / 11 / 2015: La PGR recibe / renueva *Pegasus* de parte de la vendedora Tech Bull. La transacción fue por 500 infecciones y la capacitación a 25 operadores.

- 12 / 11 / 2017- Luis Armando Pérez Herrero obtiene su cédula profesional como licenciado en Ingeniería en sistemas computacionales

- 19 / 07 / 2017: *Se divulga públicamente, en el New York Times el uso ilegal del software Pegasus por parte de autoridades mexicanas*<sup>191</sup>

Del contenido de los correos filtrados se observa una intencionalidad por parte de diversas instituciones del Estado Mexicano por adquirir un software de espionaje para teléfonos celulares, específicamente el programa de infección *Pegasus*. En la puja por proveer el servicio de espionaje se encuentran al menos dos compañías internacionales de ciberseguridad: Hacking Team y NSO Group, sin embargo, el objetivo principal, sobre todo por parte de Zerón de Lucio, era obtener el malware desarrollado por NSO Group debido a que ese ya tenía probada su “efectividad”. De igual forma, se dejan entrever que algunas de estas negociaciones, como lo muestran los mails de Alex Velasco y Eric Banoun, son influenciadas

---

<sup>190</sup> R3D, Artículo 19 et al “*Gobierno Espía...*”, op. cit. P. 19

<sup>191</sup> Ahmed, A. y Perlroth, N. “*Using texts as lures...*” op. cit.

por injerencias de tipo personal, que buscan beneficios económicos privados para personas concretas a través de los contratos.

Por la narración de los hechos también es posible percatarnos que existen irregularidades e inconsistencias a lo largo de los mismos, dos específicamente: la primera es la incongruencia entre los perfiles requeridos para realizar transacciones de seguridad nacional, sistemas electrónicos sofisticados y las personas que las realizan. Llama la atención que dos de los principales actores por parte de Tech Bull (Carlos Cayetano y Armando Pérez) hayan conseguido sus cédulas profesionales hasta después de haber sellado un contrato multimillonario con la PGR. Igualmente, los dos socios fundadores de dicha empresa (C. C. y Jorge de Jesús) no disponían de referencias o experiencia previas en el campo de la seguridad e inteligencia cibernética, ni habían realizado alguna actividad empresarial previa. Pasaron en un año de fundar una compañía de seguridad sin ventas anteriores a cerrar un contrato de 32 millones de dólares con una de las dependencias principales del país.

El otro aspecto es el manejo de tiempos y espacios por parte de Tech Bull. Al prestar atención a sus movimientos de personal, se advierten 2 cambios abruptos, pero que guardan relación con eventos importantes próximos. El primero de ellos es el ingreso de Armando Pérez a Tech Bull como encargado de cobranzas representante ante litigios futuros el 16 de octubre del 2014, trece días después, el 29 de ese mes, se cierra el contrato con la Procuraduría General de la República; en el documento oficial aparecen las firmas de Armando Pérez y Tomás Zerón, representantes de sus respectivos grupos. 9 días después, es decir, el 9 de noviembre de 2014, Carlos Cayetano sale de la dirección de Tech Bull. En correo electrónico con fecha de 28 de noviembre del mismo año, se ve a Armando Pérez haciendo las negociaciones con Hacking Team.

Con respecto a los espacios, en la citada investigación de Mexicanos Unidos Contra la Corrupción y la Impunidad, se indica que las instalaciones de Tech Bull se ubicaban, en un inicio, en Homero 538, interior 303, Polanco, en la hoy CDMX. En dicha dirección se alza un edificio que alberga “oficinas virtuales”, entre las cuales se hallaban dos empresas fantasmas ligadas al exgobernador de Veracruz, Javier Duarte. Compartiendo espacio y domicilio fiscal con la agencia de Tech Bull, se encontraba “Zamtria SA de CV”, empresa veracruzana ligada a Patricia Ríos Triana, quien fungía como accionista en dicha entidad

empresarial y en otras 12 extras, una de ellas siendo “Desarrolladores Mercalim”, parte de la red fantasma orquestada por el gobernador Duarte.<sup>192</sup>

### 3.3. Descripción del uso ilegal de Pegasus en contra de activistas, defensores de derechos humanos y periodistas, 2015 – 2017

El caso más antiguo conocido de uso de Pegasus para espiar actores sociales destacados (mas no el primero en ser registrado) es un mensaje engañoso enviado al celular de la periodista Carmen Aristegui, el 12 de enero de 2015. Hasta el momento, se ha registrado ataques a 25 personas distintas<sup>193</sup>, los primeros 76 intentos de infección fueron detallados en el reporte “*Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México*”, realizado por las organizaciones R3D Red en Defensa de los Derechos Digitales, Artículo 19 y Social TIC. Dicho documento reviste de una importancia fundamental en la divulgación y esclarecimiento de los procedimientos, operación y tipología de los mecanismos utilizados por autoridades mexicanas para espiar objetivos civiles de manera arbitraria, injustificada y fuera de la ley. El apartado que ahora compete versa sobre la descripción de dichas acciones y para ello se retomará la información contenida en el reporte aludido. Debido a la extensión, variedad de mensajes y objetivos, así como los entrecruzamientos y descripciones contextuales por caso específico, sería muy complicado reproducirlo en su totalidad, por lo tanto se eludirá hacer una transcripción literal, y en cambio, a favor de una lectura más ágil y concreta, se opta por un narración visual concentrada en 4 gráficas principales, cada una retomando la agrupación en casos temáticos que el propio informe ya contemplaba en su estructura.

Al llegar a estas líneas, ya se ha explicado a grandes rasgos qué es *Pegasus*, cómo funciona y la forma en la que lo obtuvieron algunas dependencias del Estado Mexicano, sin embargo, previo a exponer su uso indiscriminado en el país, considero pertinente mencionar cómo es que la sociedad civil se percató que el malware ya estaba siendo utilizado, para ello, es

---

<sup>192</sup> Olmos, Raul; Durán et al, “*PGR compró Pegasus...*”, *op. cit.*

<sup>193</sup> R3D: Red en Defensa de los Derechos Digitales, “*A dos años de Gobierno Espía: Una cronología de la Impunidad*”, 19 de Junio de 2019, disponible en: [https://r3d.mx/2019/06/19/gobierno-espia-cronologia/?fbclid=IwAR2o\\_nbj9ytDTGY7vXHbw0KwVcFRyPI5FhCfP2ZkI3zgMQDdYrFPDTo9RvE](https://r3d.mx/2019/06/19/gobierno-espia-cronologia/?fbclid=IwAR2o_nbj9ytDTGY7vXHbw0KwVcFRyPI5FhCfP2ZkI3zgMQDdYrFPDTo9RvE), consultado el 20 de julio de 2019.

necesario rastrear el primer caso mundial relacionado al programa de espionaje de NSO Group.

### 3.3.1 *El paciente cero y el descubrimiento de los primeros casos en México.*

Podemos identificar a Ahmed Mansoor como el “paciente cero” respecto a los intentos de infección con *Pegasus*. Esta persona es un defensor de los derechos humanos residente en los Emiratos Árabes Unidos (EAU). El 10 y 11 de agosto de 2016, Mansoor recibió mensajes de texto (SMS) a su iPhone que prometían interesantes “secretos nuevos”, sobre detenidos torturados en las cárceles de los Emiratos Árabes, si es que entraba en el link adjunto. Mansoor decidió no acceder a dicho link y en su lugar mandó los mensajes a los investigadores de Citizen Lab (CL), ubicados en Toronto, Canadá. Ahí se identificaron los enlaces como pertenecientes a una infraestructura de engaño<sup>194</sup> conectada a la compañía de “guerra cibernética”, NSO Group. En un trabajo en conjunto entre personal de Citizen Lab y Lookout Security (compañía ya mencionada al inicio de este capítulo), se llegó a establecer la forma en la que funcionaba el ecosistema de *Pegasus*. En agosto de 2016, se publica el reporte con esta investigación y la descripción del caso de Ahmed Mansoor: “*The Million Dollar Dissident*”<sup>195</sup>. En ese escrito se indica que los EAU y México, son los países a los que NSO Group dedicaba la mayor parte de su infraestructura de dominios falsos, los cuales tenían como fin suplantar sitios web relacionados a cadenas de noticias, redes sociales, entretenimiento, etc. Reproduzco a continuación la gráfica que elaboró Citizen Lab y Lookout Security para señalar este aspecto.

### **Gráfico 3.1**

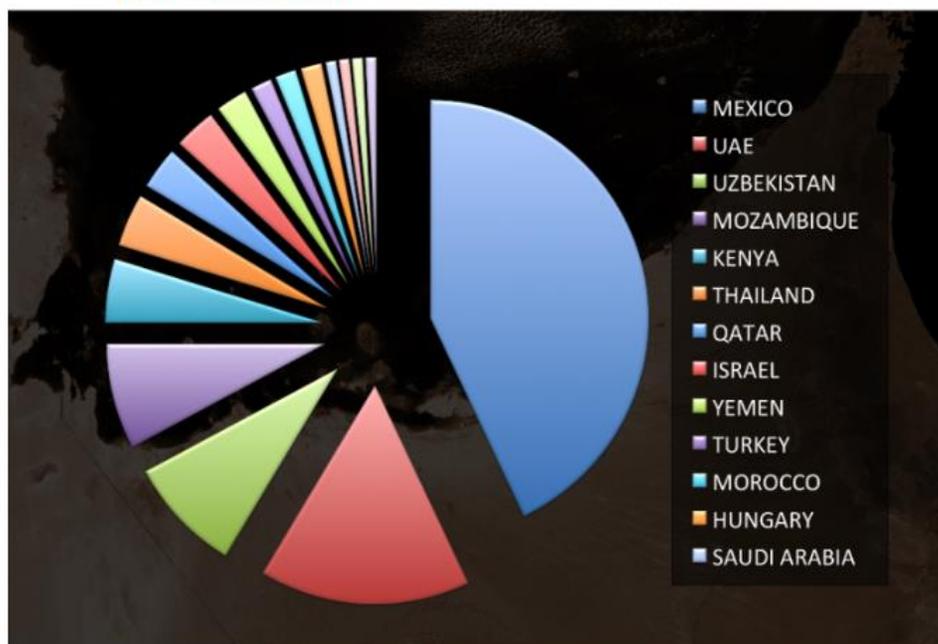
#### **Países con mayores dominios relacionados a la infraestructura de engaño**

---

<sup>194</sup> “*exploit*” en el original, hace referencia a una herramienta de software que se aprovecha de una falla en un sistema computacional, normalmente para propósitos maliciosos, en este caso instalar malware.

<sup>195</sup> Marczak, Bill y Scott-Railton, John, “*The Million Dollar Dissident...*” op. cit.

## COUNTRY THEMES IN EXPLOIT INFRASTRUCTURE NAMES



From: Marczak & Scott-Railton  
The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

CITIZEN LAB 2016

Figure 14: Country theme based on domain name.

**Fuente:** Marczak, Bill y Scott-Railton, John, "The Million Dollar Dissident. NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", Citizen Lab, Universidad de Toronto, 24 de agosto de 2016, disponible en: <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>

Salta a la vista la enorme diferencia que guarda la infraestructura específica para México de la del resto de los países. Es de notar también la particularidad geográfica que el gráfico expone, la mayoría de estos países se encuentran en zonas próximas a medio oriente, históricamente lugar de conflictos y violaciones flagrantes a los derechos humanos<sup>196</sup>, siendo México el único país americano en aparecer en el reporte del uso del software espía.

En el informe de CL se dan ejemplos de los nombres de dominios con los cuales *Pegasus* se hacía pasar por portales y páginas web legítimas. Retomo el cuadro que ellos presentan, editado para mostrar aquellos que atañen a México.

<sup>196</sup> Amnistía Internacional, "Oriente Medio y Norte de África: indiferencia mundial que aumenta la impunidad hacia las violaciones de derechos humanos cometidas", Amnistía Internacional España, 26 de febrero de 2019, disponible en: <https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/oriente-medio-y-el-norte-de-africa-indiferencia-mundial-que-aumenta-la-impunidad-hacia-las-violacio/>, consultado el 15 de julio de 2019.

### Gráfico 3.2.

#### Ejemplos de nombres de dominios falsos utilizados en la infraestructura de Pegasus

Type	Example	Impersonating
<b>News Media</b>	aljazeera.co	Aljazeera
	bbc-africa.com	BBC
	cnn-africa.co	CNN
	unonoticias.net	Las Ultimas Noticias
	univision.click	Univision
<b>Shipment Tracking</b>	track-your-fedex-package.org	FedEx
<b>ISP / Telco</b>	mz-vodacom.info	Vodacom (Mozambique)
	iusacell-movil.com.mx	Iusacell (Mexico)
	sabafon.info	Sabafon (Yemen)
	newtarrifs.net	Generic
<b>Popular Online Platforms</b>	y0utube.com.mx	YouTube
	fb-accounts.com	Facebook
	googleplay-store.com	Google
	whatsapp-app.com	WhatsApp

**Fuente:** Marczak, Bill y Scott-Railton, John, “The Million Dollar Dissident. NSO Group’s Iphone Zero-Days used against a UAE Human Rights Defender”, Citizen Lab, Universidad de Toronto, 24 de agosto de 2016, disponible en: <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>

En la primera columna se encuentra el tipo de plataforma que se intentaba emular, en orden: Medios de Noticias, Rastreo de paquetería, Empresas/servicios de telecomunicaciones, sitios populares en línea; en la segunda columna está un ejemplo del nombre falso, y al final la compañía real a la cual se imitaba. En la sección de medios de comunicación se puede encontrar dos tocantes a México, la cadena de televisión latina (con sede en los Estados Unidos de Norteamérica) Univisión<sup>197</sup> y el servicio de noticias por mensajería SMS, “Unonoticias”<sup>198</sup>. Con respecto a empresas de telecomunicaciones se encuentra una que pretendía duplicar a la compañía de telefonía celular “Iusacell” (ahora parte de AT&T<sup>199</sup>) y por último están cuatro copias apócrifas de populares plataformas / servicios de internet: Youtube, Facebook, Google y Whatsapp. De acuerdo a los datos de *top ranking web*, en

<sup>197</sup> Ver: Univisión Media. [https://corporate.univision.com/?\\_ga=2.239144131.1141334171.1567794224-1636358028.1567794221#gs.lzbv8l](https://corporate.univision.com/?_ga=2.239144131.1141334171.1567794224-1636358028.1567794221#gs.lzbv8l), consultado el 14 de julio de 2019

<sup>198</sup> Ver: AMX Contenido SA de CV. <https://www.unotv.com/inicio/#>, consultado el 14 de julio de 2019.

<sup>199</sup> Roberto Arteaga, José, “Nextel y Iusacell concluirán fusión con AT&T en 2016”, Forbes México, 24 de agosto de 2015, disponible en: <https://www.forbes.com.mx/nextel-y-iusacell-concluiran-fusion-con-att-en-2016/>, consultado el 16 de julio de 2019.

México, durante el 2018, el sitio más visitado es precisamente el buscador Google, con un estimado de 525 millones de visitas al mes, con un promedio de 13 minutos y 17 segundos; la segunda es el sitio de videos Youtube con 404 millones 800 mil visitas, cuyo promedio es de 36 minutos con 56 segundos; Facebook ocupa el tercer lugar con 3223 millones 200 de visualizaciones con un promedio de 20 minutos y 27 segundos. Whatsapp se colocaría en el octavo lugar de esta lista<sup>200</sup>.

Es notable que en los nombres falsos que la plataforma *Pegasus* usa, se busca mantener cierta similitud con la empresa o el servicio real, este parecido buscaría confundir a la persona objetivo del mensaje, llevándola a tomar el enlace por legítimo y a acceder al contenido que promete. La variedad de mensajes, nombres falsos y técnicas de engaño podrán observarse más adelante.

Posterior a la publicación de *“The Million Dollar Dissident”*, las organizaciones mexicanas R3D: Red en Defensa de los Derechos Digitales y Social TIC se pusieron en comunicación con los investigadores de Citizen Lab y miembros de Amnistía Internacional, porque tenían indicios de que *Pegasus* había sido utilizado en territorio nacional en contra de los activistas Alejandro Calvillo y Luis Encarnación; y del científico Simón Barquera, todos ellos habían sido portavoces en el movimiento por aplicar un impuesto especial a todas las bebidas azucaradas que se vendieran en México. La organización Access Now, enfocada en la defensa de los derechos humanos y promotores de un internet abierto y libre, fue el puente de enlace entre las asociaciones nacionales y las extranjeras<sup>201</sup>. Del fruto de esta colaboración surgieron los reportes *“Bitter Sweet: Supporters of Mexico’s Soda Tax Targeted with NSO Exploit Links”*<sup>202</sup> y *“Destapa la vigilancia: promotores del impuesto al refresco, espías*

---

<sup>200</sup> Merca2.0, Mesa Editorial, *“Sitios Web más visitados por mexicanos”*, Revista Merca2.0., disponible en: <https://www.merca20.com/sitios-web-mas-visitados-por-los-mexicanos/>, consultado el 14 de julio de 2019.

<sup>201</sup> R3D, Artículo 19 et al *“Gobierno Espía...”*, op. cit. P. 7

<sup>202</sup> Scott-Railton, J.; Marczak, B.; Guarnieri, B. et al, *“Supporters of Mexico’s Tax Soda Targeted With NSO Exploit Links”*, Citizen Lab, Universidad de Toronto, 11 de febrero de 2017, disponible en: <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>, consultado el 10 de junio de 2019.

con *malware gubernamental*”<sup>203</sup>, así como un artículo en el New York Times<sup>204</sup>. Todos estos escritos se publicaron el 11 de febrero de 2017 y constituyen las primeras documentaciones del uso de software *Pegasus* en territorio americano.

### 3.3.2. Uso sistemático del software espía *Pegasus* en México, 2015 - 2017

De acuerdo con los datos provenientes de “*Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México*”<sup>205</sup> podemos organizar los intentos de infección con *Pegasus* en contra de activistas, defensores de derechos humanos y periodistas de la siguiente manera:

#### **Mensajes dirigidos a Aristegui Noticias; Enero, 2015 – Julio, 2016**

Carmen Aristegui (CA): periodista, titular de Aristegui Noticias y del programa de radio *Primera Edición*. Fue miembro de la Unidad de Investigaciones Especiales de MVS Noticias Primera Edición (UNI MVS). Junto a Rafael Cabrera, Irving Huerta, Daniel Lizárraga, Sebastián Barragán y Gustavo Varguez publicó el reportaje “La casa blanca de Enrique Peña Nieto” a través del portal *Aristegui Noticias*.

Emilio Aristegui (EA): Hijo de la periodista Carmen Aristegui. Era aún menor de edad cuando fue objeto de infiltración por parte de *Pegasus*.

Rafael Cabrera (RC) y Sebastián Barragán (SB) : Periodistas, participaron en la investigación de “La casa blanca”. Formaban parte tanto de Aristegui Noticias como del equipo de la UNI MVS.

Fecha	Persona objetivo	Mensaje	Nombre del dominio NSO	Eventos socio-político relevantes
12/01/2015	Carmen Aristegui	El siguiente mensaje no ha sido enviado [link]	hxxp://smscentro[.com (vía bit.ly)	-24/10/14 Cobertura

<sup>203</sup> R3D: Red en Defensa de los Derechos Digitales, “*Destapa la vigilancia: promotores del impuesto al refresco, espíados con malware gubernamental*”, R3D, 11 de febrero de 2017, disponible en: <https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espíados-con-malware-gubernamental/>, consultado el 10 de junio de 2019.

<sup>204</sup> Perlroth, Nicole, “*Spyware’ Odd Tarjets: Backers of mexico’s Soda Tax*”, The New York Times, Nueva York, 11 de febrero de 2017, disponible en: [https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?\\_r=0](https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?_r=0), consultado el 10 de junio de 2019.

<sup>205</sup> R3D, Artículo 19 et al “*Gobierno Espía...*”, op. cit pp. 8 – 51 y 82 - 88

12/04/2015	Carmen Aristegui	Notificación de compra con tarjeta **** monto \$3,500.00 M.N, ver detalles en [link]	hxxp://smsmensaje[.]mx	profunda sobre el caso Ayotzinapa.
08/05/2015	Carmen Aristegui	Aviso de vencimiento de pago asociado a tu servicio con cargo a tu tarjeta ****, ver mas detalles: [link]	hxxp://smsmensaje[.]mx	-09/11/14 Se publica en el portal Aristegui Noticias el reportaje “La casa blanca de Enrique Peña Nieto”
08/05/2015	Carmen Aristegui	Haz realizado un Retiro/Compra en Tarjeta **** M.N. monto \$3,500.00 verifica detalles de operación: [link]	hxxp://smsmensaje[.]mx	
11/05/2015	Carmen Aristegui	Estimado cliente informamos que presentas un problema de pago asociado a tu servicio, ver detalles... [link]	hxxp://smsmensaje[.]mx	-03/02/15 Se nombra a Virgilio Andrade como titular de la Secretaria de la Función Pública. Se le encargó investigar si el presidente Peña, su esposa o el secretario Videgaray habían incurrido en conflicto de interés en la compra de “la casa blanca”
13/05/2015	Carmen Aristegui	UNONOTICIAS. [contenido no disponible] [link]	hxxp://unonoticias[.]net	
26/07/2015	Carmen Aristegui	UNOTV.COM/ ANONYMUS ANUNCIA QUE ATACARÁ PAGINA DE ARISTEGUI VER DETALLES: [link]	hxxp://smsmensaje[.]mx	
26/07/2015	Carmen Aristegui	Haz realizado un Retiro /Compra en Tarjeta **** M.N monto \$3,500 verifica detalles de la operación [link]	hxxp://unonoticias[.]net	
20/08/2015	Carmen Aristegui	IUSACELL/ Estimado cliente su factura esta lista, agradeceremos pago puntual por \$17401.25	hxxp://Iusacell-movil[.]com.mx	
20/08/2015	Carmen Aristegui	USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	-11/03/15 La compañía MVS despide a CA y su equipo (entre ellos RC y SB)
22/08/2015	Carmen Aristegui	IUSACELL.COM/EL SIGUIENTE MENSAJE ESTA MARCADO COMO URGENTE REVISALO DESDE NUESTRO PORTAL VER [link]	hxxp://Iusacell-movil[.]com.mx	-19/04/15 Publicación en Aristegui Noticias (AN), Univisión y Proceso del reportaje “Fueron los federales”.
24/08/2015	Carmen Aristegui	ALERTA AMBER DF/ COOPERACION PARA LOCALIZAR AL NINO DE 9 ANOS, DESAPARECIDO EN LA COLONIA [contenido omitido]. DETALLES [link]	hxxp://mymensaje-sms[.]com (vía bit.ly)	
30/08/2015	Emilio Aristegui	UNOTV.COM/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRIA ENCARCELAR REPORTEROS MIENTRAS INVESTIGA VER NOMBRES: [link]	hxxp://unonoticias[.]net (vía bit.ly)	-27/07/15 AN publica “Directores de Pemex y CFE involucrados en nuevas grabaciones de OHL”
30/08/2015	Emilio Aristegui	UNOTV.COM / PRESIDENCIA DEMANDARÁ POR DIFAMACIÓN A QUIENES PUBLICARON REPORTAJE DE LA CASA BLANCA. NOTA: [link]	hxxp://unonoticias[.]net	
30/08/2015	Emilio Aristegui	UNOTV.COM/ DETIENEN A PRESUNTO LIDER DE CARTEL DE SINALOA EN [contenido omitido] VER: [link]	hxxps://unonoticias[.]net (vía bit.ly)	-21/08/15 En el informe de la Secretaria de la Función Pública se exonera a EPN
30/08/2015	Rafael Cabrera	UNOTV.COM/ PRESIDENCIA DEMANDARA POR DIFAMACION A QUIENES PUBLICARON	hxxp://fb-accounts[.]com (vía bit.ly)	

		REPORTAJE DE LA CASA BLANCA. NOTA: [link]		por la casa blanca.
30/08/2015	Rafael Cabrera	UNOTV.COM/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRÍA ENCARCELAR REPRTEROS MEINTRAS INVESTIGA VER NOMBRES: [link]	hxxp://unonoticias[.]net (vía bit.ly)	-01/10/15 CA publica el librp “La casa blanca de Enrique Peña Nieto”.
25/10/2015	Carmen Aristegui	Hola te envio invitación electrónica con detalles por motivo de mi fiesta de disfraces espero contar contigo alonso: [link]	hxxp://smsmensaje[.]mx (vía tinyurl.com)	-06/02/16 En AN aparece el reportaje “El expediente secreto de la Boda Peña Nieto-Rivera”
09/02/2016	Carmen Aristegui	Carmen hace 5 días que no aparece mi hija te agradecer mucho que compartas su foto, estamos desesperados: [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	
10/02/2016	Carmen Aristegui	Querida Carmen fallecio mi hermano en un accidente, estoy devastada, envio datos del velorio, espero asistas: [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	
24/02/2016	Carmen Aristegui	UNOTV.COM/LANZA TELEVISA DESPLEGADOS EN TODOS SUS MEDIOS; CRITICA POSTURA DE ORGANIZACIÓN ARTICULO 19. VER: [link]	hxxps://unonoticias[.]net (vía bit.ly)	03/04/16 Sale a luz la investigación sobre los Papeles de Panamá.
18/03/2016	Emilio Aristegui	UNOTV.COM/ EN ENTREVISTA PARA DIARIO DE EU; MIEGUEL ANGEL MANCERA ACEPTA SU HOMOSEXUALIDAD. DETALLES: [link]	hxxp://unonoticias[.]net	-09/05/16 Se publica el reportaje de SB “Licitaciones a modo benefician a empresarios cercanos a Peña Nieto”
01/04/2016	Emilio Aristegui	ARISTEGUI NOTICIAS ESTRENA SERVICIO DE SMS, SUSCRIBASE Y RECIBIRA RESUMEN DE LAS NOTICIAS MAS IMPORTANTES: [link]	hxxp://unonoticias[.]net	
06/04/2016	Emilio Aristegui	ARISTEGUINOTICIASONLINE.MX ESTRENA SERVICIO DE SMS, SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: [link]	hxxps://smsmensaje[.]mx	-13/05/16 Se divulga la nota DE SB Y RC: “Video revela tortura a detenido en la Procuraduría del Edomex”
11/05/2016	Emilio Aristegui	UNOTV.COM/ CONFIRMA PGR QUE HIJO MAYOR DE AMLO LLEVA 48 HRS DESAPARECIDO. DETALLES: [link]	hxxp://unonoticias[.]net (vía bir.ly)	
12/05/2016	Sebastián Barragán	Tengo pruebas clave y fidedignas en contra de servidores públicos, ayúdame tiene que ver con este asunto [link]	hxxps://secure-access10[.]mx (vía bit.ly)	-03/06/16 CA y Javier Sicilia presentan el libro del Movimiento por la Paz con Justicia y dignidad.
16/05/2016	Emilio Aristegui	UNOTV.COM/ ASESINAN AL CITY MANAGER ARNE DEN RUHEN. DETALLES: [link]	hxxps://unonoticias[.]net	
18/05/2016	Rafael Cabrera	TELCEL.COM/ EL SIGUIENTE MENSAJE SE HA AMRCADO COMO URGENTE Y NO SE RECIBIO COMPLETAMENTE RECUPERELO EN [link]	hxxps://smsmensaje[.]mx (vía bit.ly)	-19/06/16 Enfrentamiento entre policías y pobladores de Asunción
18/05/2016	Emilio Aristegui	UNOTV.COM/ FILTRAN VIDEO DONDE LORET DE MOLA MANTIENE RELACIONES	hxxp://unonoticias[.]net	

		SEXUALES CON PAOLA ROJAS VER VIDEO [link]		Nochixtlán, Oaxaca. AN cubre ampliamente el caso.  -21/07/16 CA hace pública la demanda presentada en contra del Libro “La Casa Blanca de EPN” por parte de MVS
19/05/2016	Rafael Cabrera	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE \$8,854.90 M/N VERIFIQUE DETALLES [link]	hxxps://ideas- telcel[.]mx	
19/05/2016	Emilio Aristegui	UNOTV.COM/ POSIBLE CORRUPCION REVELA AUDIO TELEFONICO ENTRE EPN Y PRESIDENTE DE OHL AUDIO EN: [link]	hxxps://unonotici as[.]net	
20/05/2016	Rafael Cabrera	Facebook reporta intentos de acceso a la cuenta: Rafa Cabrera. Evita bloqueo de cuenta, verifique en: [link]	hxxps://fb- accounts[.]com	
20/05/2016	Emilio Aristegui	TELCEL.COM/ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE \$10,854.90 M/N VERIFIQUE DETALLES [link]	hxxps://ideas- telcel[.]com.mx	
23/05/2016	Rafael Cabrera	UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. DETALLES: [link]	hxxps://unonotici as[.]net	
23/05/2016	Emilio Aristegui	UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. DETALLES: [link]	hxxps://unonotici as[.]net	
24/05/2016	Rafael Cabrera	No tienes los huevos de ver como me fajo a tu pareja. Mira nada mas como cojemos bn rico y en tu cama: [link]	hxxps://smsmensa je[.]mx (vía bit.ly)	
26/05/2016	Emilio Aristegui	UNOTV.COM/ HAYAN DECAPITADO A PERIODISTA EN VERACRUZ Y DEJAN NARCOMENSAJE AMENAZADOR. FOTOS Y DETALLES: [link]	hxxps://unonotici as[.]net	
27/05/2016	Emilio Aristegui	UNOTV.COM/ DECOMISAN CARGAMENTO DEL CIDA/ OBAMA BIN LADEN NO HA MUERTO/ DETIENEN A LUPITA DALESIO [link]	hxxps://unonotici as[.]net (vía bit.ly)	
30/05/2016	Emilio Aristegui	UNOTV.COM/ EJECUTAN PERIODISTA Y DEJAN NARCOMENSAJE/ CONTINUA DOBLE NO CIRCULA/ NOVIA ENLOQUECE DE CELOS [link]	hxxps://smsmensa je[.]mx (vía bit.ly)	
01/06/2016	Emilio Aristegui	UNOTV.COM/ CARMEN ARISTEGUI SE DESTAPA COMO CANDIDATA AL GOBIERNO DE LA CDMX PARA EL 2018. DETALLES: [link]	hxxps://unonotici as[.]net	
03/06/2016	Carmen Aristegui	Carmen la pagina esta intermitente, esta apareciendo este error al intentar ingresar: [link]	hxxp://smsmensaj e[.]mx	

<b>03/06/2016</b>	Emilio Aristegui	USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA VER DETALLES: [link]	hxxps://smsmensaje[.]mx (vía bit.ly)
<b>13/06/2016</b>	Carmen Aristegui	Hace 3 días que no aparece mi hija, estamos desesperados, te agradeceré que me ayudes a compartir su foto: [link]	hxxps://smsmensaje[.]mx (vía bit.ly)
<b>15/06/2016</b>	Carmen Aristegui	Buenas tardes Carmen, únicamente paso a saludarte y enviarte esta nota de Proceso que es importante retomar: {link}	hxxps://smsmensaje[.]mx (vía bit.ly)
<b>22/06/2017</b>	Emilio Aristegui	UNOTV.COM/ REVELAN VIDEO DONDE CRISTIANO RONALDO SE ENFADA Y AVIENTA MICROFONO DE REPORTERO. VIDEO EN: [link]	hxxps://unonoticias[.]net
<b>28/06/2016</b>	Carmen Aristegui	UNOTV.COM/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/ SECUESTRAN REPORTERO DE TELEVISIA/ FALLECE CHACHITA [link]	hxxps://smsmensaje[.]mx (vía bit.ly)
<b>28/06/2016</b>	Emilio Aristegui	UNOTV.COM/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/ SECUESTRAN REPORTERO DE TELEVISIA/ FALLECE CHACHITA [link]	hxxps://smsmensaje[.]mx (vía bit.ly)
<b>04/07/2016</b>	Carmen Aristegui	UNOTV.COM/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON [link]	hxxps://unonoticias[.]net (vía bit.ly)
<b>04/07/2016</b>	Emilio Aristegui	UNOTV.COM/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON [link]	hxxps://unonoticias[.]net (vía bit.ly)
<b>12/07/2016</b>	Emilio Aristegui	UNOTV.COM/FILMAN A REPORTERO Y PERIODISTA CUANDO SON LEVANTADOS POR COMANDO ARMADO EN TAMAULIPAS. VIDEO: [link]	hxxps://unonoticias[.]net
<b>15/07/2016</b>	Carmen Aristegui	[Contenido no disponible] [link]	hxxps://smsmensaje[.]mx (vía bit.ly)
<b>18/07/2016</b>	Emilio Aristegui	Hola oye abriste nuevo facebook? Me llego una solicitud de un face con tus fotos pero con otro nombre mira: [link]	hxxp://fb-accounts[.]com
<b>19/07/2016</b>	Carmen Aristegui	Hola buen martes. Oye que pedo con el puto Lopez Doriga? Mira lo que escribió sobre ti hoy urge desmentirlo: [link]	hxxps://smsmensaje[.]mx (vía bit.ly)
<b>23/07/2016</b>	Emilio Aristegui	Amigo, hay una pseudo cuenta de fb y twitter identica a la tuya checala para que la denuncies mira checala: [link]	hxxp://fb-accounts[.]com

<b>25/07/2016</b>	Carmen Aristegui	Bienvenido Club [contenido omitido], se ha aplicado un cargo de \$875.85 a su línea, si desea cancelar ingrese a: [link]	hxxps://smsgmensaje[.]mx (vía bit.ly)	
<b>28/07/2016</b>	Emilio Aristegui	UNOTV.COM/ VIRAL EL VIDEO DE FUERTE GOLPE QUE RECIBE EN LA CARA OSORIO CHONG PROPINADO POR MAESTRO. VIDEO: [link]	hxxps://unonoticias[.]net	

Se contabilizaron un total de 56 intentos de infección en contra de personas relacionadas al medio Aristegui Noticias. La distribución de los mensajes es la siguiente: 24 dirigidos a Carmen Aristegui, 24 a Emilio Aristegui, 7 para Rafael Cabrera y 1 en contra de Sebastián Barragán.

El contenido del mensaje del 15 de julio de 2016 fue omitido por el equipo de R3D, Artículo 19 y Social TIC debido a que contenía fuertes alusiones sexuales. Los mensajes enviados a CA del 12 de abril; 8 y 11 de mayo; 26 de julio y 7 comprendidos del 20 al 30 de agosto del 2015 se enviaron del mismo número telefónico: 55\*\*\*\*\*066. De igual forma, el 9, 10 y 24 de febrero del 2016 se recibieron mensajes provenientes del número 55\*\*\*\*\*427. El texto que contenían los SMS variaba en su contenido.

**Mensajes dirigidos al periodista Carlos Loret de Mola;** Agosto – septiembre, 2015 y marzo – abril, 2016

Carlos Loret de Mola (CL): periodista, titular del noticiero matutino en el canal 2 de la compañía de medios, Televisa. Además es columnista en el periódico El Universal, así como productor y locutor de Radio. Ganó el premio nacional de periodismo en el 2005 y 2007.

<b>Fecha</b>	<b>Persona objetivo</b>	<b>Mensaje</b>	<b>Nombre del dominio NSO</b>	<b>Eventos socio-político relevantes</b>
<b>20/08/2015</b>	Carlos Loret de Mola	USEMBASSY.GOV/DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: [link]	hxxp://smsgmensaje[.]mx (vía bit.ly)	--/08/15 Durante el mes de agosto, CL realizó múltiples cuestionamientos públicos (mediante su columna en El Universal y su cuenta de personal de Twitter) en contra del ejército mexicano por supuestas ejecuciones
<b>29/08/2015</b>	Carlos Loret de Mola	estas personas vinieron preguntando por usted vienen en camioneta sin placas tome foto los reconoce? [link]	hxxp://fb-accounts[.]com (vía bit.ly)	
<b>01/09/2015</b>	Carlos Loret de Mola	TELCEL.COM/ Estimado cliente su factura esta próxima a vencer, agradeceremos su pago por \$19750.26 Detalles: [link]	hxxp://ideas-telcel[.]com	

<b>03/09/2015</b>	Carlos Loret de Mola	Carlos, buen día. Otra vez estan sacando chismes tuyos, supuestamente te tomaron fotos en UNIVISION mira [link]	hxxp://twitter-com[.]mx (vía bit.ly)	extrajudiciales en el municipio de Tanhuato, Michoacán
<b>05/09/2015</b>	Carlos Loret de Mola	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE TIENE UN SALDO PENDIENTE DE \$4280.00 M/N VERIFICA DETALLES DEL CARGO: [link]	hxxp://ideas-telcel.com[.]mx (vía bit.ly)	03/03/16 CL publica en su columna que personal de la Subprocuraduría Especializada en Investigación y delincuencia Organizada, así como de las Secretarías de Gobernación y Marina habían interrogado “informalmente” al narcotraficante, Joaquín “El Chapo” Guzmán. .
<b>06/09/2015</b>	Carlos Loret de Mola	ALERTAAMBER.COM/SOLICITAMOS SU COOPERACION PARA LOCALIZAR A ESTUDIANTE DE LA FACULTAD DE FILOSOFIA DE LA UNAM VER FOTO [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	
<b>05/03/2016</b>	Carlos Loret de Mola	Loret fallecio mi padre estamos devastados envio datos del velorio espero contar contigo mau [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	
<b>20/04/2016</b>	Carlos Loret de Mola	Querido Loret, fíjate que tvnotas tiene fotos tuyas donde estas con una chica cenando. Dales una checada [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	

Los dos primeros mensajes provinieron del mismo número 55\*\*\*\*\*974

**Mensajes dirigidos al Instituto Mexicano para la Competitividad (IMCO);** diciembre, 2015 y mayo, 2016

Juan Pardinás (JP): Director General del IMCO.

Alexandra Zapata (AZ): Directora de Educación e Innovación Cívica del IMCO

<b>Fecha</b>	<b>Persona objetivo</b>	<b>Mensaje</b>	<b>Nombre del dominio NSO</b>	<b>Eventos socio-político relevantes</b>
<b>21/12/2015</b>	Juan Pardinás	en la madrugada fallecio mi padre, estamos devastados, te envio los datos del velatorio, espero puedas venir [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	01/12/15 IMCO presenta el índice de Información Presupuestal Estatal 2015, resaltan la opacidad de las finanzas públicas
<b>08/01/2016</b>	Juan Pardinás	oiga afuera de su casa anda una camioneta con 2 vatos armados, les tome fotos véalos y cuidese: [link]	hxxp://smsmensaje[.]mx (vía bit.ly)	02/12/15 Convenio del Senado con el IMCO para elaborar leyes anticorrupción.
<b>17/05/2016</b>	Alexandra Zapata	UNOTV.COM/ REPORTAJE: LA HISTORIA DE CORRUPCION DETRÁS DEL INTITUTO MEXICANO PARA LA COMPETITIVIDAD. VER: [link]	hxxps://unonoticias[.]net	--/04/16 Durante el mes de abril se discute en el Senado el dictamen y aprobación de la ley anticorrupción, la cual incluye la Ley 3
<b>18/05/2016</b>	Alexandra Zapata	UNOTV.COM/ [contenido no disponible] [link]	hxxps://unonoticias[.]net	

				de 3. Se aprueba una versión reducida.
--	--	--	--	--

Los dos mensajes recibidos Juan Pardini tenían como remitente el número: 55\*\*\*\*\*720

El texto del SMS enviado a Alexandra Zapata, con fecha del 18 de mayo, mencionaba la existencia de un video íntimo que involucraba a personal de IMCO.

**Mensajes dirigidos al Centro de Derechos Humanos Miguel Agustín Pro Juárez (PRODH); Abril – Junio, 2016**

Mario Patrón (MP): Director del Centro PRODH. Fungió como uno de los principales intermediarios con el gobierno federal para que el Grupo Interdisciplinario de Expertos Independientes (GIEI) pudiera colaborar en la investigación de los 43 estudiantes desaparecidos de Ayotzinapa.

Stephanie Brewer (SB): Coordinadora del área internacional del Centro PRODH. Interlocutora del caso Atenco ante la Comisión Interamericana de Derechos Humanos. Parte de un grupo de organizaciones que impulsaban la aprobación de la Ley General de Tortura.

Santiago Aguirre (SA): Subdirector del Centro PRODH. Él manejó y tuvo acceso a material e información legal y victimal sobre los casos de Ayotzinapa y Tlatlaya; así mismo fue interlocutor ante el GIE. También se desempeña como profesor universitario.

Fecha	Persona objetivo	Mensaje	Nombre del dominio NSO	Eventos socio-político relevantes
20/04/2016	Mario Patrón	EL GOBIERNO DE MEXICO MADRUGA AL GIEI [link]	hxxps://secure-access10[.]mx (vía bit.ly)	24/04/16 El GIE presenta su último informe sobre Ayotzinapa
11/05/2016	Stephanie Brewer	y según ustedes que hacen Derechos Humanos ante esto, y la dignidad de ellos que... [link]	hxxps://secure-access10[.]mx (vía bit.ly)	04/05/ 10° aniversario del caso Atenco.
20/05/2016	Santiago Aguirre	SrJorge soy Juan Magarino ayuda con mi hermano Heriberto se lo llevo la policía por ser maestro es un delito [link]	hxxps://network190[.]com (vía bit.ly)	-08/06/16 La PGR presenta su reporte sobre los 43 de Ayotzinapa. SA ofreció varias entrevistas criticando el informe.
08/06/2016	Santiago Aguirre	Mtro. tuve un incidente, le envió nuevamente mi tesis, basada en su tesina para que me de sus comentarios [link]	hxxps://network190[.]com (vía bit.ly)	-27/06/16 GIE presenta sus resultados ante el Comité y Grupo de Trabajo contra la
28/06/2016	Santiago Aguirre	Buen día Mtro. trabajo en mi tesis, tome como base su tesina, me interesa	hxxps://network190[.]com (vía bit.ly)	

		su opinión, le mando los adelantos [link]		Desaparición Forzada de la ONU
--	--	---	--	--------------------------------

El 3 de abril, días previos al intento de infección con *Pegasus*, la línea telefónica de Santiago Aguirre fue intervenida ilegalmente cuando conversaba con uno de los padres de los jóvenes desaparecidos.

### Mensajes dirigidos a Mexicanos Contra la Corrupción y la Impunidad (MCCI); mayo 2016

Salvador Camarena (SC): Director general de investigación periodística en MCCI, unidad creada el primero de marzo de 2016. Fue editor en el periódico Reforma, director de la revista Chilango, corresponsal del Universal y columnista en el Financiero.

Daniel Lizárraga (DN): encargado de la jefatura de información en la unidad de investigación periodística de MCCI. Anteriormente fue el subdirector de Animal Político y de la unidad de investigaciones especiales de MVS Radio Primera Emisión. Es coautor en la investigación sobre el caso de la “casa blanca” relacionada con el presidente Enrique Peña Nieto.

Fecha	Persona objetivo	Mensaje	Nombre del dominio NSO	Eventos socio-político relevantes
18/05/2016	Daniel Lizárraga	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE RPRESENTA UN ADEUDO DE \$8,854.90 M/N VERIFIQUE DETALLES: [link]	hxxp://ideas-telcel[.]com.mx	3/04/16 – DN participó en el reportaje” El constructor de la casa blanca de EPN ocultó una fortuna en paraísos fiscales”
24/05/2016	Salvador Camarena	No tienes los huevos de ver como me fajo a tu pareja. Mira nada mas como cojemos bn rico y en tu cama [link]	hxxps://smsgmensaje[.]mx (vía bit.ly)	24/05/16 SC publica “Javier Duarte
25/05/2016	Salvador Camarena	Afuera de tu casa esta una camioneta sospechosa y estan tomando videos de la casa. Les tome foto mira [link]	hxxp://smsgmensaje[.]mx (vía bit.ly)	Millones por explicar” 25/05/16 Se hace pública la existencia de MCCI

Los mensajes dirigidos a Salvador Camarena provinieron del mismo número a pesar de contener mensajes distintos

## CAPITULO IV: DISCURSOS

### 4.1 Ataques basados en ingeniería social.

Los distintos mensajes enviados a los objetivos civiles tenían la intención de captar la atención del individuo y que este ingresara al link malicioso adjunto para así instalar el software espía. Los mensajes buscaban despertar la curiosidad o el interés de la persona mediante mensajes falsos, los cuales, en varias ocasiones, apelaban a situaciones o temas significativos muy específicos para cada objetivo. Esta estrategia es conocida como ingeniería social y es definida por el Departamento de Seguridad Informática de la Universidad de Lujan como “un método basado en el engaño y la persuasión que puede llevarse a cabo a través de canales tecnológicos o bien en persona, y que se utiliza para obtener información significativa o lograr que la víctima realice un determinado acto”<sup>206</sup>. La ingeniería social intenta acceder a información reservada o confidencial a través de acciones físicas, tecnológicas y sobre todo psicológicas<sup>207</sup>.

El proceso general que implican los actos de ingeniería social sigue cuatro pasos: 1) se realiza la recolección de información sobre la persona objetivo; 2) se establece una relación con el blanco; 3) se aprovecha la información disponible y se realiza el ataque; 4) se alcanza el objetivo y se sale sin dejar rastros.<sup>208</sup> La ingeniería social también se vale de la creación de escenarios inventados, pero convincentes de acuerdo al contexto o interés de la víctima, que buscan orillar a la misma a revelar información privada o a actuar de una forma inoportuna o poco común en circunstancias normales<sup>209</sup>

---

<sup>206</sup> Universidad Nacional de Lujan, “*Ingeniería Social*”, Departamento de Seguridad de la Universidad Nacional de Lujan, Buenos Aires, s/f, disponible en: <http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/11>, consultado el 28 de agosto de 2019.

<sup>207</sup> Hertwig, Ralph, “Efficient Social Engineering and Realistic Cognitive Modeling: A Psychologist’s Thoughts”, en *Economics and Psychology*, MIT Press, Cambridge, 2007, pp. 247 – 251, disponible en: [http://library.mpib-berlin.mpg.de/ft/rh/RH\\_Efficient\\_2007.pdf](http://library.mpib-berlin.mpg.de/ft/rh/RH_Efficient_2007.pdf), consultado el 9 de septiembre de 2019

<sup>208</sup> Segovia, L.; Torres, F.; Rosillo, M.; Tapia, E.; Albarado, F, et al; “Social engineering as an attack vector for ransomware”, en *Proceedings of the Conference on Electrical Engineering and Information Communication Technology*, Pucó, Chile, Octubre de 2017, pp 1 – 6.

<sup>209</sup> Salahdine, Fatima y Kaabouch, Naima; “Social Engineering Attacks: A survey”, en *Future Internet*, Universidad de Dakota del Norte, Grand Forks, EUA, 2 de abril de 2009, p. 5, disponible en: [https://res.mdpi.com/d\\_attachment/futureinternet/futureinternet-11-00089/article\\_deploy/futureinternet-11-00089.pdf](https://res.mdpi.com/d_attachment/futureinternet/futureinternet-11-00089/article_deploy/futureinternet-11-00089.pdf), consultado el 1 de septiembre de 2019.

Se observa en múltiples SMS un conocimiento previo sobre el trabajo público desempeñado por la persona a la cual van dirigidos los mensajes o sus intereses personales potenciales. En mensaje del 8 y 28 de junio del 2016, enviados a Santiago Aguirre del Centro ProDH, se le pide que acceda a los enlaces maliciosos bajo una falsa solicitud para revisar una tesis. Santiago Aguirre además de colaborar en el Centro ProDH también se desempeñaba como profesor universitario. En un mensaje previo, del 20 de abril del mismo año, dirigido al director del Centro Prodh, Mario Patrón, se le incita a acceder al enlace mediante un mensaje provocativo “EL GOBIERNO MEXICANO MADRUGA AL GIEI: [enlace]”, Mario Patrón fue uno de los intermediadores principales para que el Grupo Interdisciplinario de Expertos Independientes (GIEI) pudiera colaborar junto con las autoridades mexicanas en la investigación de los 43 estudiantes desaparecidos de Ayotzinapa.

La contextualización geográfica específica también es señal de una investigación previa. En el mensaje recibido el 24 de agosto de 2015 en el celular de Carmen Aristegui, se pide la ayuda, mediante una alerta ámbar falsa, para encontrar a un menor desaparecido en la colonia donde vive la periodista. Días después, el 30 de agosto, se envió mensaje a Emilio Aristegui, hijo de Carmen, en donde se anunciaba la presunta detención de un líder del Cartel de Sinaloa en la misma colonia donde residía el menor de edad.

Mitnick, retomando el trabajo sobre la persuasión del doctor en psicología social, Brad Sagarin, enlista los principios psicológicos sobre los cuales se sustentan las tácticas de la ingeniería social<sup>210</sup>, se observan elementos en común con los mensajes empleados para intentar implantar el software *Pegasus*:

**-Los rasgos de un rol:** el atacante toma un rol, mostrando abiertamente rasgos específicos de su papel para que la víctima infiera el resto y con ello actué en consonancia. En la mayoría de las ocasiones se desea que el blanco desempeñe el rol del colaborador. En los mensajes de la infraestructura *Pegasus*, el papel desempeñado por el agresor toma en ocasiones la forma de una organización, por ejemplo, en los SMS mandados a Carmen Aristegui y Carlos Loret de Mola el 20 de agosto de 2015; y el 3 de junio de 2016 a Emilio Aristegui, se finge un anuncio de la Embajada de los Estados Unidos anunciando un problema con la visa,

---

<sup>210</sup> Mitnick, Kevin y Simon, William, “*El arte de la intrusión*”, AlfaOmega, Madrid, abril 2007, pp. 335 – 343.

solicitando la participación del blanco para solucionar el problema mediante acceso al enlace adjunto<sup>211</sup>.

**-Credibilidad:** todo ataque de ingeniería social aspira a ser lo más legítimo y fidedigno a la realidad posible. Al establecer una credibilidad en su estructura y fondo, los ataques se hacen pasar por legítimos y con ello intentan no levantar ninguna sospecha por parte de la víctima. Las direcciones adjuntas en los mensajes de la infraestructura *Pegasus* siguen esta lógica, el link del mensaje del 22 de agosto de 2015 en contra de Carmen Aristegui, emula uno real por parte de la compañía de telefonía móvil Iusacell (hxxp://Iusacell-movil[.]com.mx); de manera similar, en mensajes recibidos por Rafael Cabrera (19/05/16), Emilio Aristegui (20/05/16), Carlos Loret de Mola (05/09/15) y Daniel Lizarra (18/05/16) se simula un enlace proveniente de Telcel, otra popular compañía de telefonía (hxxps://ideas-telcel[.]com). El intento por aparentar ser mensajes reales y seguros se observa igual en el cuerpo de los mismos. Para comparar, un SMS auténtico de la empresa Telcel, recibido personalmente el 4 de diciembre de 2018, dice: “TELCEL. Estimado cliente, su línea presenta un saldo vencido por \*cantidad\* [...]. Puede pagar con tarjeta en [link]”; mientras que la estructura general de los mensajes ficticios para instalar el malware es la siguiente: “TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE \*cantidad\* M/N VERIFIQUE DETALLES: [link]”. Al observar ambos mensajes se puede identificar una similitud en su estructura, lenguaje y sentido: inician con el nombre de la compañía, posteriormente refieren la presencia de un adeudo y finalizan con un link para que ingrese el usuario.

Los intentos de infección con mensajes simulando ser el servicio de noticias por SMS UNOTV siguen una disposición parecida. Por ejemplo, en un mensaje legítimo recibido personalmente el 30 de agosto de 2019 se lee: “UNOTV.COM ALERTAN POR ESTOS TRATAMIENTOS PODRIAN CAUSAR CANCER unotv.mx/0WI”, por el otro lado, un mensaje simulado por la estructura *Pegasus*, enviado el 23 de agosto del 2016 a Rafael Cabrera y a Emilio Aristegui muestra lo siguiente: UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. DETALLES:

---

<sup>211</sup> USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: [link] Supra. p. 76, 79 y 80

unonoticias[.]net”. La semejanza en los casos de “UNOTV”, entre los mensajes auténticos y los falsos, es mucho mayor. Ambos inician con el título del servicio más la terminación .com, solo que los engañosos llevan una diagonal al final. El texto del mensaje todo en mayúsculas es compartida por ambos, al igual que un enlace al final. Incluso la forma en la que está escrito el link guarda semejanzas: unotv.mx en el genuino y unonoticias[.]net para el artificial.

Los ataques del tipo UNOTV presentan un nivel de personalización y sofisticación destacable en cuanto al contenido de los mismos y su relevancia para las víctimas. En el ejemplo planteado arriba se hace mención a la posible candidatura de Carmen Aristegui para las próximas elecciones presidenciales. Los blancos de este mensaje guardaban una relación muy estrecha con esa periodista, siendo Emilio hijo de la misma y Rafael Cabrera colaborador cercano en el equipo de noticias de Aristegui. En otro mensaje, este del 17/05/16, enviado a Alejandra Zapata, una de las directivas del Instituto Mexicano para la Competitividad, se lee: “UNOTV.COM/ REPORTAJE: LA HISTORIA DE CORRUPCIÓN DEL INSTITUTO MEXICANO PARA LA COMPETITIVIDAD. VER: unonoticias[.]net” Al analizar esta combinación entre un mensaje con formato muy parecido al servicio verdadero y por lo tanto creíble a primera vista, junto a un contenido que invoca intereses directos para la persona objetivo se infiere un trabajo previo de investigación y planeación que tiene como fin persuadir a una persona para que ésta acceda al enlace contenido en el SMS, sin que medie duda alguna.

**-Desviar la atención del pensamiento sistemático.** El procesamiento sistemático de la información es caracterizado por ser racional, ordenado y evaluativo, este tipo de procesamiento es factible cuando las personas, además de tener las cualidades cognitivas necesarias, están motivadas para analizar detenidamente un conjunto de información y emitir una evaluación sobre la misma.<sup>212</sup> Al contrario, el procesamiento heurístico surge cuando no hay una motivación suficiente y /o la capacidad del sujeto para procesar la información es baja, ello debido a múltiples factores, a saber: a) existe poco tiempo disponible para pensar; b) existe una sobrecarga de información o bien ésta es escasa; c) hay fácil accesibilidad a un

---

<sup>212</sup> Tesser, Abraham y Shaffer, David, “Attitude and Attitude Change”, Anual Review of Psychology, Vol. 41, Febrero de 1990, pp. 479 - 523

heurístico (atajo en el pensamiento) y d) existe la presencia de una emoción intensa.<sup>213</sup>. En un SMS sin remitente para Carmen Aristegui (15/06/2016) se menciona una supuesta nota de la revista Proceso que reviste una importancia periodística, pero sin mencionar el tema o dar más datos que pudieran contextualizar su relevancia, solo se deja el link para consultar la información completa. B. Stephanie Brewer, colaboradora en el Centro ProDH, recibió el 11 de mayo del 2016 un mensaje escueto que decía “y según ustedes que hacen derechos humanos ante esto, y la dignidad de ellos que... [enlace]”, la ambigüedad del mensaje y la falta de información quieren despertar la curiosidad del receptor del mensaje, depositando en el link malicioso la única vía para satisfacer la necesidad por saber más. Este tipo de estrategia también busca que la víctima reaccione rápido y visceralmente, suspendiendo momentáneamente su capacidad evaluativa y con ello no repare en la peligrosidad del mensaje. Una muestra de cómo se deseaba conseguir una respuesta rápida, casi inmediata, a través de un estímulo emocional urgente, puede encontrarse en los mensajes enviados a dos objetivos distintos (Salvador Camarena del IMCCO y Rafael Cabrera de Aristegui Noticias) el día 24 de mayo de 2016. En los SMS mencionados se encontraba un texto que aludía a encuentros sexuales con las respectivas parejas de los periodistas además de supuestas fotos sobre el acto que se podían ver si el blanco entraba en el link señalado.

Dos mensajes más, uno del 8 de mayo del 2016, dirigido a Alexandra Zapata del IMCO y el otro, del 15 de julio del mismo año, con Carmen Aristegui como destinataria, hacen uso de imaginación sexual en un escenario laboral controversial como medio para generar una reacción emocional intensa que minimice el pensamiento sistemático y con ello el usuario entré al link, el cual promete información adicional, sin reparar en su contexto fraudulento.

**-El deseo de ayudar.** La sensación de bienestar, poder o alivio<sup>214</sup>, entre otras, que nos produce el prestar ayuda a los otros, es aprovechada por las tácticas de ingeniería social para conducir a una persona a que realice una acción o provea información sin detenerse en las posibles consecuencias que acarrea ese acto. Este tipo particular de engaño se manifiesta de dos formas en la infraestructura de *Pegasus*, en la primera, un SMS haciéndose pasar por la

---

<sup>213</sup> Pratkanis, Anthony y Aronson, Elliot, “*La era de la Propaganda. Uso y abuso de la persuasión*”, Paidós, Barcelona, 1994, pp 52 – 56.

<sup>214</sup> Rivera, Alba Nydia, “*Factores que determinan la atribución de altruismo*”, Revista Latinoamericana de psicología, vol. 12, núm. 1, Bogotá, 1980, pp 63 - 77

Alerta Amber solicita ayuda para localizar a una persona desaparecida, ofreciendo los datos completos en el link malicioso al final del mensaje. Como ya se mencionó párrafos arriba, Carmen Aristegui fue víctima de este tipo particular de engaño el 24 de agosto de 2015. De manera similar, el 6 de septiembre del mismo año, Carlos Loret de Mola recibió un mensaje aparentando ser de la Alerta Amber solicitando su cooperación para localizar a una estudiante de la Facultad de Filosofía de la UNAM. Para ver la foto de la presunta desaparecida había que acceder al enlace corrupto.

La otra manera en la que se presentaron ilegítimas solicitudes de ayuda fue mediante mensajes de tipo personal. En el intento de infección del 9 de febrero de 2016, el texto del SMS, dirigido a Carmen Aristegui decía: “Carmen, hace 5 días que no aparece mi hija te agradecer (sic.) mucho que compartas su foto, estamos desesperados: [link]”, meses después, el 13 de junio, Aristegui recibió un mensaje muy similar al anterior, modificando a 3, los días desaparecidos de la presunta persona extraviada. El 20 de mayo de 2016 llega al celular de Santiago Aguirre, subdirector del Centro ProDH, un SMS con el siguiente contenido: “Sr.Jorge soy Juan Margarino ayuda con mi hermano Heriberto se lo llevo la policía por ser maestro es un delito [link]”. Este mensaje presenta la localización de intereses y personalización de contenido, señalado ya en ataques anteriores, cuyo diseño responde a un perfil bien definido, previa investigación. Aguirre fue una de las personas del Centro ProDH que colaboraron en la investigación de los hechos de la desaparición de los 43 estudiantes normalistas de Ayotzinapa, por lo cual el tema de la desaparición forzada de personas relacionadas con la exigencia de derechos educativos le resultaba relevante.

**-Atribución de funciones / características.** Complemento de la atribución de un rol, se pone en primer plano las características de la víctima para que ésta cumpla una o varias funciones específicas. En el caso del ataque del malware *Pegasus* a Sebastián Barragán<sup>215</sup>, se intentó invocar su interés investigativo y la función periodística que desempeña para hacerlo caer en la trampa electrónica. La atribución de funciones puede ser sutil y recurrir a elementos emocionales. En mensaje a Juan Pardinás, director general del IMCO, del 21 de diciembre de 2015, se lee: “en la madrugada falleció mi padre, estamos devastados, te envío los datos

---

<sup>215</sup> Mensaje del 12 de mayo de 2016: “Tengo pruebas clave y fidedignas en contra de servidores públicos, ayúdame tiene que ver con este asunto: [link]”, supra p. 77

del velatorio, espero puedas asistir [enlace]”, la intención de este mensaje era apelar al aparato sentimental de la persona para que la misma abriera el enlace adjunto después de considerar brindar un soporte emocional al remitente, o bien, creyera necesario cumplir con el protocolo social correspondiente. Un mensaje similar llegó al teléfono celular de Carmen Aristegui el 16 de febrero del 2016.

**-Miedo.** La capacidad que tiene el miedo de influir en la conducta de las personas ha sido objeto de múltiples estudios desde la psicología social,<sup>216</sup> las técnicas utilizadas por la infraestructura Pegasus hacen uso expansivo de este aspecto de la constitución humana, basándose particularmente en el principio de que un mensaje que apela al miedo es mucho más eficaz si dentro del mismo se proporcionan instrucciones de cómo evitar esas amenazas<sup>217</sup>. Los ataques que se valen de esta estrategia siguen un modelo base, aunque difieran en su contenido o forma: envían la notificación de que algo peligroso está por suceder, pero esa situación puede evitarse (o disponer de más datos para prevenirla), si uno accede a la dirección electrónica colocada al final del SMS.

El 29 de agosto de 2015, Carlos Loret de Mola recibió un mensaje advirtiéndole sobre la presencia de personas extrañas: “estas personas vinieron preguntando por usted vienen en camioneta sin placas tome foto los reconoce? [enlace]”. Un mensaje similar en el tono, pero de mayor intensidad fue enviado a Juan Pardinas, director del IMCO: “oiga, afuera de su casa anda una camioneta con 2 vatos armados, les tome fotos véalos y cuídese: [enlace]. Una variable de los mensajes anteriores puede encontrarse en el intento de infección a Salvador Camarena (25/05/2016), director general del área de investigación periodística en Mexicanos Contra la Corrupción y la Impunidad: “Afuera de tu casa esta una camioneta sospechosa y estan tomando videos de la casa. Les tome foto mira [enlace]”

En el caso de las personas relacionadas al medio Aristegui Noticias puede observarse una progresión en la gravedad de las amenazas planteadas en los mensajes de Pegasus. Los SMS siguen la estructura ya analizada del modelo UNOTV, iniciando con un mensaje del 26 de

---

<sup>216</sup> Ver: León, J.L. “*Persuasión de Masas. Psicología y efectos de las comunicaciones sociopolíticas y comerciales*”, Deusto, Bilbao, 1989; y Leventhal, H. “*Findings and Theory in the Study of Fear Communications*”, *Advances in Experimental Social Psychology*. Vol. 5, 1970, pp. 119 – 186.

<sup>217</sup> Briñol, Pablo; De la Corte, Luis y Becerra, Alberto, “*Qué es la persuasión*”, Biblioteca Nueva, Madrid, 2001, p. 80

julio del 2015 a Carmen Aristegui, en donde se anuncia que el grupo de ciberactivistas Anonymus atacaría la página web de Aristegui Noticias. Días después, el 30 de agosto del mismo año, Emilio Aristegui y Rafael Cabrera reciben el mismo mensaje: “UNOTV/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRÍA ENCACELAR REPORTEROS MIENTRAS INVESTIGA VER NOMBRES: [enlace]”. El siguiente mensaje de este tipo se enviaría al hijo de Aristegui el 26 de mayo del 2016, en el texto se indica: “UNOTV.COM/ HAYAN DECAPITADO A PERIODISTA EN VERACRUZ Y DEJAN NARCOMENSAJE AMENAZADOR. FOTOS Y DETALLES: [enlace]”, 4 días más tarde, Emilio recibe un mensaje semejante informando sobre la ejecución de un periodista y un mensaje del narco acompañándolo. El último mensaje utilizando el miedo como vehículo para propiciar una reacción en personas cercanas a Carmen Aristegui fue mandado, una vez más, a Emilio el 12 de julio del 2016. La nota falsa informaba que un reportero y un periodista habían sido filmados mientras eran “levantados” por un comando armado. Si deseaba ver el video, tenía que ingresar en el enlace marcado.

La estrategia de utilizar el miedo, la desconfianza y la intimidación en contra de periodistas y activistas resulta particularmente significativa cuando analizamos estos mensajes a la luz del contexto en el cual sucedieron. De acuerdo a datos de la Comisión Nacional de los Derechos Humanos<sup>218</sup>, en el marco del Programa de Agravios a Periodistas y Defensores Civiles de Derechos Humanos, en el periodo de 2000 al 20 de diciembre de 2018, se han registrado un total de 141 homicidios de periodistas, de los cuales 15 casos fueron mujeres, es decir un 10.6% del total. Respecto al caso de activistas y defensores de los DDHH se registraron un total de 40 homicidios entre el año 2006 al 20 de diciembre de 2018, en 15 de esos casos, las víctimas fueron mujeres. Relativo a las solicitudes de medidas precautorias para la protección de periodistas y personas defensoras, la CNDH advierte un incremento importante en la frecuencia y gravedad de las agresiones cometidas contra esos dos grupos de población durante los años 2014 y 2016. Al cierre de 2014, se solicitaron 11 medidas cautelares para periodistas y 4 para defensores de DDHH. Para el 2015 el número incremento a 15 solicitudes para periodistas y 12 en favor de activistas. Ese número volvió a crecer en el

---

<sup>218</sup> Comisión Nacional de los Derechos Humanos, “Análisis situacional de los Derechos Humanos de Periodistas y Personas Defensoras”, Ciudad de México, 2018. Disponible en: <http://informe.cndh.org.mx/menu.aspx?id=40063>, consultado el 19 de septiembre de 2019.

2016, año en el que se registraron 27 medidas cautelares para periodistas y 28 para defensores.

Por su parte, la organización Artículo 19, en su reporte del 2016 sobre la situación de los periodistas en México<sup>219</sup>, indica que en 2015 se documentaron 397 casos de agresión a periodistas, cifra que aumentó un 7% en el 2016, registrándose 426 ataques en contra de la prensa. Se contabilizaron 11 asesinatos de periodistas durante el 2015, dando un total de 30 hasta la fecha de publicación del reporte. En cuanto al tipo de agresiones, éstas fueron: ataques físicos (81), intimidaciones (79), amenazas (76), privación ilegal de la libertad (58) y actos de hostigamiento o acoso (58).

En el escenario descrito, el uso del miedo y la intimidación como herramienta para provocar una reacción súbita y de descuido en la persona revela que los objetivos fueron bien definidos, desarrollándose un perfil complejo sobre los mismos que tomó en cuenta la situación social en la cual se desenvolvían, utilizando ese contexto como factor de vulnerabilidad.

**-Reactancia.** La teoría de la reactancia psicológica, propuesta por el psicólogo Jack Brehm,<sup>220</sup> señala la reacción negativa que experimentan las personas cuando perciben que sus libertades, o capacidad de elección, se les han arrebatado o está siendo amenazadas. Para Doile “cada vez que un comportamiento accesible a un individuo sea retirado, por una u otra razón, de su campo de posibilidades (o amenazado de ser retirado), este individuo experimentará una restricción de su libertad, lo que despertará en él un estado de reactancia psicológica, estado emocional orientado hacia una recuperación de su libertad.”<sup>221</sup>

En el SMS del 18 de julio de 2016 para Emilio Aristegui, se encuentra un mensaje con tratamiento familiar, avisando al menor de edad sobre la existencia de un supuesto perfil falso de Facebook que hace uso de sus fotos personales,<sup>222</sup> cinco días después, 23 del mismo mes, Emilio recibe otro mensaje en tono similar, esta vez destacando el robo de identidad en el

---

<sup>219</sup> Article 19, “Informe 2016: Libertades en resistencia”, Ciudad de México, 6 de abril de 2017, disponible en: [https://articulo19.org/wp-content/uploads/2017/04/Libertades-en-Resistencia\\_Informe-2016-A19.pdf](https://articulo19.org/wp-content/uploads/2017/04/Libertades-en-Resistencia_Informe-2016-A19.pdf), consultado el 25 de septiembre de 2019

<sup>220</sup> Brehm, J.W., “A theory of psychological reactance”, Academic Press, Oxford, 1966.

<sup>221</sup> Doise, W. “Psicología Social Experimental”, Editorial Hispano: Europa, 1980, p. 309

<sup>222</sup> Mensaje del 18 de julio de 2016: “Hola oye abriste nuevo Facebook? Me llego una solicitud de un face con tus fotos pero con otro nombre mira: [enlace]” supra p. 79

que incurre la cuenta falsa: “Amigo, hay una pseudo cuenta de fb y twitter idéntica a la tuya checala para que la denuncies mira checala: hxxp://fb-accounts[.]com”. Ambos mensajes tienen por meta que la respuesta del objetivo, al ver en riesgo su privacidad y su capacidad de mantener imágenes e información personal alejada de personas indeseadas, sea la de solucionar inmediatamente el fingido problema, sin reparar en que se trata de un ataque electrónico a su privacidad.

El mismo esquema, pero en una situación artificial distinta, subyace en dos mensajes enviados a Carlos Loret de Mola. En el primero de ellos, del 3 de septiembre de 2015 se alude a la existencia de unas fotos íntimas del periodista en manos de la cadena de televisión Univision. Posteriormente, se retoma aquella idea pero ahora con un escenario más específico: “Querido Loret, fíjate que tvnotas tiene fotos tuyas donde estas con una chica cenando. Dales una checada [link]”, mensaje del 20 / 04/ 2016. La recuperación de la capacidad de mantener la vida íntima fuera del escrutinio público ante una amenaza externa es el sustento psicológico bajo el cual los intentos de infección descritos buscan romper la cadena de seguridad en el dispositivo del objetivo y con ello instalar el programa de espionaje electrónico.

La clasificación enunciada en las páginas anteriores persigue un fin didáctico – analítico para sistematizar las estrategias psicológicas usadas por la infraestructura *Pegasus*. Por lo tanto, mensajes que se encuentran en una categoría no los excluye de presentar características de alguna otra, de hecho, el cruce de elementos provenientes de diversas estrategias puede observarse en varios SMS. El ya citado mensaje a Alexandra Zapata del IMCO, en el que se hace mención a la existencia de un video con contenido sexual que involucra personal de dicha organización, se enlazan principios provenientes de las categorías de reactancia, miedo y desviación del pensamiento sistémico. En otro ejemplo, esta vez un texto enviado a Carmen Aristegui el 19 de julio de 2017: “Hola buen martes. Oye que pedo con el puto Lopez Doriga? Mira lo que escribió sobre ti hoy urge desmentirlo: [link]”, se observan herramientas propias de la atribución de características (rectitud), la desviación del pensamiento sistémico (información escasa / ambigua), y la reactancia (recuperar la credibilidad perdida).

## 4.2 Declaraciones públicas de autoridades.

### 4.2.1 Enrique Peña Nieto

#### 4.2.1.1 Parque Industrial Lagos de Moreno

El 22 de junio de 2019, 3 días después de la publicación de la investigación del New York Times sobre los intentos de infección con *Pegasus* por parte de autoridades mexicanas, el entonces presidente de la República, el Lic. Enrique Peña Nieto, se refirió por primera vez al tema en su discurso de inauguración del Parque Industrial en Lagos de Moreno, Jalisco.<sup>223</sup> Reproduzco a continuación la parte del discurso dedicado al espionaje tecnológico<sup>224</sup>:

“Quiero referirme a un tema que está en el debate público y que yo creo que no escapa, a casi ninguno de los que están aquí presentes, y es este, es este señalamiento muy reciente de haberse afirmado que el Gobierno mexicano se involucraba, espiaba la actividad privada de activistas, de defensores de derechos humanos, de periodistas. Y aquí hoy quiero afirmar de manera muy categórica: éste es un gobierno democrático, éste es un gobierno que respeta y tolera las voces críticas, y también así ha quedado acreditado, nadie puede señalar o advertir que este gobierno no haya tolerado, haya sido condescendiente, haya aceptado y haya reconocido que la crítica enriquece el actuar del gobierno, por eso somos un gobierno que condenamos de manera categórica cualquier intervención que se tenga en la vida privada de quienes son activistas y de cualquier persona, no cabe, intervenir de manera ilegal la vida privada de ningún [inaudible] eso no cabe en una democracia como en la que vivimos en nuestro país. Y este es un gobierno que actúa por convicción. He dado indicaciones a la Procuraduría General de la República para que haga la investigación correspondiente a partir de las denuncias que se ha presentado, para que, con celeridad y prontitud pueda deslindar responsabilidades; primero determinar si tienen sustento dichas afirmaciones, segundo para determinar cuál es el origen y la fuente de dichas afirmaciones, de dichos señalamientos; déjenme decirles que este gobierno rechaza categóricamente cualquier tipo de intervención en la vida privada de cualquier ciudadano. Todo el equipamiento, toda la tecnología que efectivamente tiene el gobierno y que ha adquirido es para mantener la seguridad interna del país, es para combatir al crimen organizado, es para generar condiciones de seguridad para

---

<sup>223</sup> Animal Político, Redacción, “Gobierno espía: Peña Nieto amenaza, luego se retracta y después niega responsabilidad”, Animal Político, 23 de junio de 2017. Disponible en: <https://www.animalpolitico.com/2017/06/gobierno-espia-pena-nieto/>, consultado el 3 de octubre de 2019.

<sup>224</sup> Presidencia Enrique Peña Nieto, “Inauguración del Parque Industrial en Lagos de Moreno”, Video almacenado en la plataforma Youtube, 22 de junio de 2017, disponible en: <https://www.youtube.com/watch?v=EqoKGVEdmPw>, transcripción a partir del min. 53:32 al 57:46. Consultado el 4 de octubre de 2019.

los mexicanos, esa es la utilidad y ese es el empleo de la tecnología que tienen efectivamente distintas instituciones encargadas de la seguridad de nuestro país. Resulta muy fácil señalar y apuntar, resulta muy fácil convocar para que se señale al gobierno como alguien que espía, o como una entidad que espía, nada más falso que eso, porque ninguno de las personas que se sienta agraviada puede afirmar o mostrar o evidenciar siquiera que su vida se ha visto afectada, lastimada por esas supuestas intervenciones y por esos, por ese supuesto espionaje. Somos os una sociedad que las más de las veces nos sentimos espíados, yo mismo, como presidente de la república, a veces recibo mensajes cuya fuente u origen desconozco, pero procuro en todo caso ser cuidadoso en lo que hablo telefónicamente, no faltará quien, alguien o que alguna vez exhiban alguna conversación mía, ya ha ocurrido, ya ha pasado, pero nada más falso y nada más fácil que señalar a un gobierno que se dedique a esta actividad. El uso de inteligencia que tiene el gobierno es para mantener condiciones de seguridad para la sociedad mexicana, espero que la Procuraduría General de la República, con celeridad, pueda deslindar responsabilidades y espero, al amparo de la ley, pueda aplicarse contra ellos que han levantado esos falsos señalamientos contra el gobierno.”

Para realizar el análisis del discurso del presidente Peña y sus implicaciones en el caso *Pegasus*, habría que iniciar situándolo en un lugar del orden social. Comúnmente, el discurso, así como otras interacciones hechas por actores sociales, se suelen colocar dentro del nivel <<micro>> del análisis, mientras que las instituciones, los grupos y sus relaciones (poder social) se catalogan como parte del nivel <<macro>>,<sup>225</sup> sin embargo, habría que entender que esta división es artificial, un constructo sociológico<sup>226</sup> que en la realidad social, en la cotidianidad, forman un conjunto unificado, por lo tanto, cuando una persona, inserta en todo momento en comunidades humanas, hace uso del lenguaje, lo hace como individuo y, a la vez, como miembro de distintos grupos sociales.<sup>227</sup> Peña Nieto, al emitir sus declaraciones públicas, lo hace a título personal, en tanto individuo, pero al mismo tiempo habla como miembro de un partido político, de una institución y/o de un conjunto de autoridades que él encarna como figura presidencial. Podría realizarse el ejercicio inverso, de macro a micro, y decir que la autoridad, una parte específica de la misma, u otros grupos sociales hablan

---

<sup>225</sup> Van Dijk, Teun, “*El análisis crítico...*” op. cit. P. 25

<sup>226</sup> Alexander, J.C., Giesen, B., Munch, R. y Smelser, N.J., “*The micro - macro link*”, University of California Press, Berkeley, 1987.

<sup>227</sup> Van Dijk, Teun, “*El análisis crítico...*” op. cit. P. 25

mediante él. Para efectos de este escrito, se considerará solo un grupo de pertenecía social: Peña como miembro y vocero de la autoridad política mexicana.

En tanto miembro de un grupo de la elite política, debe considerarse su capacidad moldeadora de grupos sociales,<sup>228</sup> Para Teun Van Dijk, existe una íntima relación entre el discurso y el poder, específicamente el poder que pueden ejercer los grupos poderosos (los políticos, los de *mass media*, los científicos, etc.) sobre el resto de la población; en sus palabras:

“los grupos poderosos tienen acceso preferente al discurso público y lo controlan, y a través del discurso controlan las mentes del público, en el sentido amplio [...]. Esto no sólo significa que mucha gente interpretará el mundo del modo que los poderosos o las élites se lo presentan, sino también que actuará (más) en consonancia con los deseos y los intereses de los poderosos”<sup>229</sup>

Conviene precisar que cuando se habla de controlar las mentes en sentido amplio, se hace referencia, más que a una forma directa e infalible para dictar pensamientos y conductas, a las formas mediante las cuales el discurso puede influir en las ideas de una persona (por ejemplo en sus conocimientos o sus opiniones) para así dirigir indirectamente algunas de sus acciones y estas se inclinan más hacia un tipo de comportamiento específico.<sup>230</sup>

En el mismo nivel de relevancia que tiene el acceso privilegiado al discurso público que ostentan los grupos poderosos, se encuentra su capacidad para decidir quién controla los temas a discutirse y los cambios en los mismos<sup>231</sup>, al igual que los medios elegidos para tal fin, los tiempos, espacios, y demás circunstancias que pueden englobarse como control del contexto y control del texto y habla.<sup>232</sup> Esto se hace notable en la decisión del presidente Peña de tocar el tema del espionaje electrónico y las acusaciones al Gobierno no mediante un comunicado de prensa oficial o en un mensaje de difusión nacional transmitido por los medios masivos de comunicación, sino dedicándole los 4 minutos finales, en un discurso de una hora de duración, mientras inauguraba un corredor industrial. El contexto en el cual se trasmite el mensaje también reviste de importancia. Van Dijk reflexiona que el uso del

---

<sup>228</sup> Beyme, Klaus von, “*Teorías políticas contemporáneas*”, IEP, Madrid, 1977, p. 351.

<sup>229</sup> Van Dijk, Teun, “*El análisis crítico...*” op. cit. P. 32

<sup>230</sup> *Ibidem*. P. 26.

<sup>231</sup> *Ibidem*. P. 28

<sup>232</sup> *Ibidem*, pp. 27 y 28.

lenguaje (de manera general) y la producción / comprensión del discurso (específicamente), dependen e influyen a la par en las propiedades significativas de la situación comunicativa cuando son interpretadas por las personas. Esas “definiciones de situación” de índole subjetiva (contexto), adquieren representaciones situacionales (modelos) específicos en la memoria de tipo episódica para formar los llamados “modelos de contexto”.<sup>233</sup> “Los modelos de contexto controlan muchos aspectos del proceso de discurso y aseguran que un discurso sea socialmente apropiado”.<sup>234</sup>

Encontrándose en un ambiente celebratorio y con invitados seleccionados (autoridades estatales, empresarios y gente de la comunidad de Lagos de Moreno), la posibilidad de encontrar oposición o crítica alguna hacia EPN era mínima. Era un ambiente controlado que permitía la exposición de la situación, pero sin la repercusión masiva que podría significar una comunicado oficial por los canales masivos de divulgación a los que tiene acceso la autoridad federal. El grupo poderoso puede controlar el nivel de divulgación que desee para exponer su discurso y evitar la confrontación o la crítica directa.

La parte del discurso del presidente Peña que trata sobre las acusaciones de espionaje tecnológico inicia con la declaración tácita de que los pronunciamiento en contra del gobierno han llegado al mismo y que este tiene conocimiento de los mismos. Se reconoce también que este tema ya es de dominio público y por lo tanto forma parte de la discusión social, del “debate público”. Se identifica además a los supuestos grupos de población que son víctimas y denunciantes del espionaje ilegal: activistas, defensores de derechos humanos y periodistas.

Hecha la introducción y el reconocimiento tanto de hechos como de actores involucrados, EPN pasa a enunciar su argumento principal para desestimar las denuncias referidas: el Estado mexicano es un gobierno democrático que respeta y tolera las voces críticas; al usar el pronombre demostrativo “este”, contextualiza el abstracto “Gobierno Mexicano” para delimitarlo en el tiempo: habla concretamente de *su* periodo de gobierno. Para reforzar su argumento, afirma que se ha acreditado el respeto y apertura del gobierno debido a que

---

<sup>233</sup> Van Dijk, Teun, “Context models in discourse processing”, en Van Oostendorp, Herre & Goldman, Susan R. (coords.), *The construction of mental representations during reading*, Lawrence Erlbaum Associates. Mahwah NJ, 1999, pp. 123 - 148

<sup>234</sup> Van Dijk, Teun, “*Ideología y análisis del discurso*”, Utopía y Praxis Latinoamericana, año 10, núm. 29 Universidad del Zulia, Maracaibo- Venezuela, Abril - Mayo de 2005, p. 16.

**“nadie puede señalar o advertir que este gobierno no haya tolerado, haya sido condescendiente, haya aceptado y haya reconocido que la crítica enriquece el actuar del gobierno”**. Se observa una doble figura en su argumentación, un doble discurso<sup>235</sup>, que se repetirá lo largo de su exposición, en la que por un lado afirma y destaca cualidades positivas del gobierno, pero por el otro, minimiza, desvalora o incluso llega a realizar amenazas sobre las acciones de los “otros.” La afirmación de Peña sobre la imposibilidad de que alguien pueda señalar un actuar incorrecto en su gobierno con respecto a las voces disidentes lo conduce a señalar que, con toda autoridad, el gobierno puede condenar todo tipo de intervención a la vida privada ya no solo de activistas, sino de cualquier ciudadano de este país.

La expresión de rechazo y desaprobación por parte de la autoridad a todo acto de intervención es seguida por un llamado a la justicia. El presidente dice haber dado la indicación para que las investigaciones necesarias para deslindar responsabilidades sean realizadas por la PGR, sin embargo, la carga de responsabilidad no la pone sobre las autoridades acusadas, sino en las personas que realizaron las denuncias: **“primero determinar si tienen sustento dichas afirmaciones, segundo para determinar cuál es el origen y la fuente de dichas afirmaciones, de dichos señalamientos”**, es decir, la investigación girará sobre las personas y no sobre el acto. En el siguiente enunciado, EPN vuelve a recalcar que su Gobierno rechaza todo tipo de intervención a la vida privada. Invierte el orden del doble discurso, ahora acusa primero y después resalta la autoridad moral del gobierno. Posterior a esta sentencia, Peña hace el segundo reconocimiento del discurso, acepta que “efectivamente” el Gobierno ha adquirido y dispone de tecnología para, de manera general, mantener la seguridad interna del país, y específicamente, combatir al crimen organizado. La evocación al concepto e idea de tecnología se hace desde lo abstracto, nunca se detalla qué tipo de tecnología es la que se dispone ni cómo se utiliza para lograr el fin indicado. Cierra esa aceptación insistiendo en que varias instituciones encargadas de la seguridad tienen acceso a “tecnología”.

En el minuto 56:14 del discurso, prácticamente al tercer minuto de iniciado el tema del espionaje tecnológico, EPN expresa: “Resulta muy **fácil señalar y apuntar, resulta muy**

---

<sup>235</sup> Ver: Lischinsky, Alon, “*Un caso de doble discurso en política: contraargumentos del gobierno español al racismo discursivo de la oposición parlamentaria*”, *Discurso & Sociedad*, Vol. I, núm. 1, Barcelona, 2007, pp. 3 - 65

**fácil convocar para que se señale al gobierno** como alguien que espía” para inmediatamente negar que esa sea la verdad. Como elemento de prueba vuelve a esgrimir la idea de que **“ninguno de las personas que se sienta agraviada puede afirmar o mostrar o evidenciar siquiera que su vida se ha visto afectada, lastimada por esas supuestas intervenciones”**. La “carga de la prueba” y la responsabilidad de demostrar que hubo una violación al derecho a la privacidad otra vez la vuelca sobre los denunciados, exculpando a las autoridades. Incluso se observa una minimización de las hipotéticas afectaciones que hubieran tenido las víctimas cuando utiliza la palabra “siquiera”, es decir, el afectado no es lo es tanto, en cuanto que nada grave le paso a su vida, por lo tanto no hay daño de ningún tipo. Esta declaración podría constituir un caso de revictimización, concepto bajo el cual, una persona que ha sido víctima de una afectación directa por un delito, vuelve a serlo cuando se enfrenta a una mala o inadecuada atención al entrar en contacto con las instituciones sociales que le brindan servicios.<sup>236</sup> La revictimización comprende todas las consecuencias psicológicas, sociales, jurídicas, económicas o de otro tipo originadas por las relaciones entre la víctima y la realidad institucional.<sup>237</sup> Al hacer uso del espacio público y de sus recursos como miembro de un grupo de poder, EPN contribuye a la reproducción<sup>238</sup> y consolidación de un discurso de desigualdad y desvalorización a las víctimas de violaciones a sus DDHH.

Antes de cerrar su discurso, el presidente Peña expone su sentir sobre el ambiente de espionaje que él percibe: **“Somos una sociedad que las más de las veces nos sentimos espiados”** e inmediatamente, agrega **“yo mismo, como Presidente de la república, a veces recibo mensajes cuya fuente u origen desconozco, pero procuro en todo caso ser cuidadoso en lo que hablo telefónicamente”**. La primera aseveración “cotidianiza” las intervenciones privadas, colocándolas en el campo de lo esperado, situación que fortalece cuando él mismo se coloca como sujeto y objeto del mismo escenario. Esta enunciación juega tanto con la estandarización de la práctica como con el intercambio de roles. Por un lado indica que si incluso él, figura de autoridad máxima en el país, sufre ataques de espionaje, entonces los otros no tienen motivos para quejarse; y, complementario a ello, invierte los papeles, pasando

---

<sup>236</sup> Albertin, P. “Psicología de la victimización criminal”, en Soria, M. y Saíz, D. (coords.) *Psicología Criminal*, Pearson Educación, España, 2006, pp. 245 – 276.

<sup>237</sup> Gutiérrez de Pineres Botero, C.; Coronel, E. y Andres Pérez, C. “Revisión teórica del concepto de victimización secundaria”, *Liberalit*, vol. 15, núm. 1, 2009, pp 49 – 58.

<sup>238</sup> Van Dijk, Teun, “*El análisis crítico...*” op. cit. P 32.

a ocupar el papel de víctima y ya no el de agresor. Sin embargo, su papel como víctima no es pasivo, al contrario, él es “cuidadoso” y por lo tanto protege su privacidad activamente, juiciosamente, señalando indirectamente que los otros, los denunciantes, no actuaron adecuadamente. Otra vez, coloca a los denunciantes como individuos incapaces e insidiosos. En múltiples estudios del análisis crítico del discurso se ha observado<sup>239</sup> una estratégica prácticamente generalizada de autoproclamación positiva por parte del grupo dominante (o hablante) y de una hetero-presentación negativa del grupo contrario y/o dominado. Esa polarización absoluta entre el grupo percibido como nosotros y los otros o ellos, presente en las representaciones sociales compartidas y sus ideologías subyacentes, es expresada y reproducida en todos los planos del texto y del habla.<sup>240</sup> Cierra esta parte del discurso haciendo referencia velada a las investigaciones periodísticas que expusieron diversos casos de corrupción vinculadas a su figura<sup>241</sup> sin dejar de mencionar que la salida fácil es culpar al gobierno.

La formación ideológica de un *ellos contra nosotros* cobra especial relevancia cuando analizamos el enunciado final del discurso: “espero que la Procuraduría General de la República, con celeridad, pueda deslindar responsabilidades y, espero al amparo **de la ley, pueda aplicarse contra ellos que han levantado esos falsos señalamientos contra el Gobierno.**” Peña, como representante de la autoridad y del poder político, directamente alude a un grupo contrario, identificándolo como “ellos”, los que señalan falsos en contra del Gobierno; y, en cuanto antónimos del “Gobierno Democrático”, debe aplicárseles todo el peso de la ley, misma que ostenta el grupo de poder representado por el Presidente. Esa frase final encauza los argumentos esgrimidos a lo largo del discurso y llama a la acción para terminar con la injusticia. El objetivo ha sido desvalorar los señalamientos y, por el contrario, revertir el escenario, transformando al Gobierno de EPN como la víctima auténtica. Al respecto, Van Dijk señala: “cuando los miembros de un grupo explican, motivan o legitiman

---

<sup>239</sup> Ver: Van Dijk, Teun, “*Elite discourse and racism*”, Sage Publications Inc, Newbury Park, CA, 1993; y Van Dijk, Teun, “*Ideology: A multidisciplinary study*”, Sage, Londres, 1998.

<sup>240</sup> Van Dijk, Teun, “*El análisis crítico...*”. op. cit. P. 28

<sup>241</sup> Aristegui Noticias, Redacción, “*La casa blanca de Enrique Peña Nieto (investigación especial)*”, Aristegui Noticias, México D.F., 9 de noviembre de 2014. Disponible en: <https://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/>, consultado el 21 de julio de 2019.

sus acciones (grupales), lo hacen típicamente en términos de discurso ideológico”,<sup>242</sup> entendiendo a las ideologías como un cúmulo de creencias fundamentales que subyacen en la gran mayoría de las representaciones sociales que comparten tipos específicos de grupos sociales.<sup>243</sup>

#### 4.2.1.2 Obra Línea 3, Guadalajara, Zapopan, Tlaquepaque

El mismo 22 de junio, durante la Supervisión de Obra de la Línea 3 del Tren Ligero de Guadalajara, Zapopan y Tlaquepaque, diversos medios de comunicación inquirieron al presidente sobre sus declaraciones previas. Retomo una parte de la versión estenográfica realizada por el medio “Animal Político” sobre dicha entrevista:

“Presidente EPN: [...] Lo que estoy queriendo afirmar, primero, que el gobierno no tiene ninguna participación en ningún tipo de espionaje contra ninguna persona. Y creo que no hay sustento, el más mínimo sustento, a una afirmación de este tipo. Segundo. Que es muy fácil señalar al Gobierno. Y. tercero. Que es muy fácil que, en esa ola de señalamientos al Gobierno, muchos se quieran subir a esa ola, y a esta ola que va en contra del Gobierno.

A veces lo más fácil en este mundo es apuntar y señalar siempre como culpable al Gobierno. El Gobierno no tiene nada que ver en espionaje alguno. Sí, tiene equipamiento. Sí hace uso de tecnología para realizar trabajos de inteligencia, que nos permite mantener un clima de seguridad en el país y, sobre todo, para combatir el crimen organizado, que cada vez, lo hemos señalado, tiene capacidades mucho más sofisticadas y tenemos que estar al nivel, a la altura de poder atacarlas o combatir las, realmente, con elementos tecnológicos suficientes.

No supongan que en la aprehensión de muchos de los blancos buscados, de las personas más buscadas fue por obra de la casualidad. Hubo un gran trabajo de investigación y de inteligencia para poder dar con muchas de estas personas que eran buscadas por la ley, precisamente siendo parte del crimen organizado.

[...]

Al final de cuentas, lo que el Gobierno está condenando es la intervención en la vida privada, a través del uso de alguna tecnología, a través de intervenir celulares, o involucrarse en la vida de las personas, a través del uso de alguna tecnología

[...]

---

<sup>242</sup> Van Dijk, Teun, “*Ideología y análisis...*” op. cit. P. 15

<sup>243</sup> Ídem.

Entonces, yo sí, simplemente afirmo categóricamente que el Gobierno no tiene nada que ver en este tipo de señalamientos que ha habido, y por eso he dado indicaciones a la Procuraduría General de la República para que haga las investigaciones que correspondan y si hay responsables, como se señala, si los hay, se puedan deslindar responsabilidades.

Pero este tipo de afirmaciones no viene más que de una especulación a partir de equipo que el Gobierno adquirió y que el Gobierno no ha rechazado haber adquirido. El Gobierno se ha hecho de tecnologías, precisamente, con un solo propósito: combatir al crimen organizado, hacer labor de inteligencia para preservar condiciones de seguridad que deben de prevalecer en nuestro país”.<sup>244</sup>

Lo primero a señalarse es el cambio de contexto entre estas declaraciones y la proferida horas antes en el Discurso de Inauguración del Parque Industrial Lagos de Moreno. Esta fue en un ambiente controlado, propicio a la intervención del Presidente y en el cual no iba a existir contrarréplica por parte de los asistentes. En la “supervisión de obra”, EPN se encontraba a nivel de piso, rodeado por un grupo de periodistas que constantemente preguntaban, replicaban y exigían mayores detalles sobre el discurso de esa misma mañana. Debido a este formato, el discurso es más entrecortado y menos elaborado, sin embargo se observan otros cambios más allá de su estructura. Ante pregunta de reportero requiriendo un esclarecimiento sobre el sentido de su mensaje en Lagos de Moreno, el Presidente responde con una síntesis de tres puntos: -1) El gobierno no ha participado en espionaje contra nadie y no existente sustento para alegar lo contrario; 2) Es fácil señalar a las autoridades y 3) Que en esos señalamientos, gente se una a los mismos con fines de mera crítica política.

Refuerza el reconocimiento de que el gobierno tiene tecnología y que esta es utilizada para garantizar la seguridad en el país, sin embargo, esta ocasión pone mayor hincapié en que la tecnología es usada “**para combatir el crimen organizado**”, destacando que este se ha vuelto más sofisticado y para enfrentarlo adecuadamente, el Gobierno requiere de mejores herramientas. Remarca este aspecto al decir que las capturas de importantes delincuentes han sido gracias a ese “**gran trabajo de investigación y de inteligencia**”. Para cerrara esa

---

<sup>244</sup> Animal Político, Redacción, “*Gobierno espía: Peña Nieto amenaza...*” op. cit. Versión estenográfica de la entrevista almacenada en issuu: [https://issuu.com/pajaropolitico/docs/22062017.epn.guadalajara\\_\\_jal./4](https://issuu.com/pajaropolitico/docs/22062017.epn.guadalajara__jal./4), consultado el 3 de octubre de 2019.

pregunta subraya que los detenidos eran parte del crimen organizado y por ello la ley debe aplicarse a ellos.

Respondiendo a otro cuestionamiento, el Presidente reitera la condena por parte del Gobierno a la intervención a la privacidad y, a la vez, coloca al frente el tema de la tecnología y cómo esta es usada, mencionando por primera vez la **intervención de celulares**, *modus operandi* ya analizado de la infraestructura *Pegasus*.

Ante otra pregunta, Enrique Peña Nieto retoma su declaración sobre las indicaciones que dio a la PGR para investigar el tema, solo que esta vez no pone la mira sobre los denunciados, al contrario, concede que “si hay responsables, como se señala, si los hay” se tomen las medidas necesarias. Al no limitar a un grupo específico como blanco de las investigaciones, otorga la posibilidad de que autoridades estén implicadas en las acusaciones.

Finaliza esa contestación con un contrapeso a la licencia recién hecha “Pero este tipo de afirmaciones **no viene más que de una especulación**”, inmediatamente, regresa al tema de la tecnología de la que dispone el gobierno y para qué la usa: “**El Gobierno se ha hecho de tecnologías**, precisamente, con un **solo propósito: combatir al crimen organizado**, hacer labor de inteligencia”.

El cambio más relevante entre ambos discursos es la conceptualización y posterior señalamiento del grupo percibido como contrario, como los “otros”. En el primer discurso las personas que levantaron falsas acusaciones contra el gobierno (periodistas, activistas y defensores de DDHH) eran quienes deberían ser investigados y recibir el tratamiento punitivo de la ley. Horas después, el Presidente Peña indica que el crimen organizado era el grupo perseguido por la ley. De hecho, sobre este grupo enemigo cae la justificación de que el gobierno haya adquirido, en primer lugar, los aparatos de espionaje tecnológico.

Evidentemente, los dos grupos vistos como antónimos a los intereses del gobierno no guardan relación temática de ningún tipo, tampoco comparten un escenario espacial y temporal que unifique la necesidad de que sean investigados. Es el texto, el contexto y las palabras las que definen su conceptualización ideológica<sup>245</sup> como “enemigos”. Las palabras, las frases y los

---

<sup>245</sup> <sup>245</sup> Van Dijk, Teun, “*Ideología y análisis...*” op. cit. P. 23

temas no son ideológicamente prejuiciados *per se*, es su uso específico en situaciones comunicativas particulares las que los hacen tales.<sup>246</sup>

El escenario, las personas, sus requerimientos y la forma del dialogo en su conjunto, es decir el contexto es lo que marcó la intencionalidad en las declaraciones del ex presidente y del grupo social que él representaba.

A pesar del cambio en los discursos expresados, en ambos el énfasis está en las persona (los otros, las autoridades, Peña), no en la tecnología, esta se encuentra en segundo plano, es ya una herramienta, para contener - investigar; o bien el acto que destapa el accionar de las personas, pero no el eje rector de la discusión. Para determinar el rol de las TIC en el discurso público, conviene ascender un nivel más en su estudio macro social.

#### 4.3 De la Sociedad de la Información a la Sociedad del Conocimiento

Al hablar del control de la mente, Van Dijk aclara que:

“<<control de la mente>> es poco más que una cómoda apelación. La psicología cognitiva y las investigaciones sobre la comunicación de masas han mostrado que influenciar la mente no es un proceso tan directo como las ideas simplificadoras sobre el control a veces sugieren (Briton y Graesser, 1996; Glasser y Salmon, 1995; Klapper, 1960; Van Dijk y Kintsch 1983). Los receptores pueden ser bastante autónomos y variables en su interpretación y uso del texto y del habla, que son también una función de la clase, del género o de la cultura (Liebes y Katz, 1990).”<sup>247</sup>

Esa idea puede extenderse al cómo entendemos culturalmente la relación humano – tecnología en nuestras comunidades contemporáneas, específicamente con las TIC. En la década de los 70's del siglo pasado comenzó un proceso de *informatización de la sociedad*<sup>248</sup> global, dicho evento fue posible por la convergencia de múltiples factores económicos, sociales, políticos y tecnológicos. Consistió en un auge inusitado de la combinación de las

---

<sup>246</sup> Ídem

<sup>247</sup> Van Dijk, Teun, “*El análisis crítico...*”. op. cit. Pp. 28 y 29.

<sup>248</sup> Nora, Simon y Alan Minc, “*Informatización de la sociedad*”, Fondo de Cultura Económica, México D.F. 1980.

telecomunicaciones y el procesamiento automático de datos<sup>249</sup>. Las nuevas tecnologías de la información, quienes sustentaban dicha combinación, ganaron una preeminencia expansiva en varias esferas de la actividad humana global. Este proceso de informatización llevaría a la formulación de un concepto socio-histórico conocido como “Sociedad de la Información”. Entender esta idea es comprender el momento temporal en cual nos encontramos y en el que se circunscriben todas las temáticas de esta tesis.

En un pronunciamiento de la CEPAL al respecto se dice que:

“El concepto de la sociedad de la información hace referencia a un paradigma que está produciendo profundos cambios en nuestro mundo al comienzo de este nuevo milenio. Esta transformación está impulsada principalmente por los nuevos medios disponibles para crear y divulgar información mediante tecnologías digitales. Los flujos de información, las comunicaciones y los mecanismos de coordinación se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de nuevas formas de organización social y productiva. Esta “actividad digital”, que se va convirtiendo poco a poco en un fenómeno global, tiene su origen fundamental en las sociedades industrializadas más maduras. De hecho, la adopción de este paradigma, basado en la tecnología, está íntimamente relacionado con el grado de desarrollo de la sociedad. Sin embargo, la tecnología no es sólo un fruto del desarrollo (por ser consecuencia de éste), sino también, y en gran medida, uno de sus motores (por ser una herramienta de desarrollo).”<sup>250</sup>

Delia Crovi Druetta, en *Sociedad de la Información y el Conocimiento. Entre el optimismo y la desesperanza* dice:

“De manera general entiendo por sociedad de la información, SÍ, a una sociedad caracterizada por un modo de ser comunicacional que atraviesa todas las actividades (industria, entretenimiento, educación, organización, servicios, comercio, etcétera).

En este tipo de organización social la información ocupa un lugar sustantivo y se

---

<sup>249</sup> Mine Main, “La informatización de la sociedad”, en *Policy implications of Data Network Developments in the OECD*, Organización para la Cooperación y el Desarrollo Económico, Paris, 1980, Traducción de: Mario R. dos Santos. Disponible en: <http://biblioteca.clacso.edu.ar/ar/libros/critica/nro7/minc.pdf>, consultado el 20 de abril, 2019.

<sup>250</sup> CEPAL, “*Los caminos hacia una sociedad...*” op. cit. P ix.

convierte en fuente de riqueza (Miége, 1998). Se produce un crecimiento rápido de las tecnologías de información y comunicación, TIC, las que repercuten en todos los sectores sociales. En efecto, a pesar de haber grandes diferencias en el acceso a estas nuevas tecnologías entre las naciones y entre los individuos, todos los países tienen al menos una franja de su sociedad que las ha integrado a sus actividades. La mayoría de esos desarrollos tecnológicos (tanto su parte dura, *hardware*, como su parte blanda o lógica, *software*) se producen en los países de primer mundo.”<sup>251</sup>

De la lectura de ambas aproximaciones es posible notar que se habla de una honda y radical transformación en nuestra sociedad, comandada por los aparatos tecnológicos digitales. La transformación a la que se hace referencia consiste en una novedosa forma en la cual nos comunicamos e interrelacionamos, tanto entre nosotros, como con los contenidos multimedia; y a la vez, en un cambio en la manera en la que procesamos todo el flujo inmenso de información que transita constantemente entre herramientas y personas. En cierta medida, y retomando una de las características de las TIC aludidas en el primer capítulo, esta evolución radical en las colectividades es causa y efecto de la posibilidad que tienen los aparatos digitales para modificar la forma en la manejamos, ordenamos e interpretamos los códigos lingüísticos. Esta nueva manera de concebir los códigos lleva a buscar otras formas de dotar significado. Hasta este momento se ha referido a las TIC y su relación con las personas en términos casi individualistas, o a la sumo como una colectividad de individuos organizados, sin embargo, las definiciones de la Sociedad de la Información colocan, indirectamente, a dos actores más en nuestro escenario: El estado (con sus instituciones), y el Mercado (con sus empresas multinacionales).

En otro texto de la CEPAL, *Report of the Round Table on Telecommunications and the Knowledge Society*, se profundiza en esta relación social con la tecnología y se agrega un concepto nuevo: “La sociedad del conocimiento”; para distinguirla de la sociedad de la información, se dilucida de la siguiente manera:

---

<sup>251</sup> Covi Druetta, Delia, “Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza”, Revista Mexicana de Ciencias Políticas y Sociales, año XLV, no. 185, México, mayo – agosto de 2002, p.16. Disponible en: <https://www.redalyc.org/pdf/421/42118502.pdf>, consultado el 4 de junio de 2019.

“En la diferenciación entre una Sociedad del Conocimiento y una Sociedad de la Información, el Dr. Kim Mallalieu postulaba que la sociedad del conocimiento era aquella que valoraba el conocimiento como un medio para lograr el bienestar económico y social. Se reconocía que en dicha sociedad, los ciudadanos tienen una capacidad de elección y oportunidad más grande, una integración social más profunda y una expectativa de vida más larga. La indagación, la investigación, la creatividad, el uso de la tecnología moderna y el liderazgo emprendedor se muestran como elementos de gran importancia. Como resultado, las habilidades críticas que deberían cultivarse incluyen el conocimiento práctico, la colaboración, la innovación, la comunicación, la diversidad y la flexibilidad. En contraste, en una sociedad de la información, las innovaciones basadas en la información, se presentan como simples herramientas para la producción y el entretenimiento, con poco o ningún interés por la asimilación, la integración o la aplicación del entendimiento a dichas invenciones.”<sup>252</sup>

En *Terra Incógnita*, Lefranc Weegan sintetiza la discusión de la siguiente manera: “No hay que equivocarse, la crítica no es a la evolución de la tecnología, ni tampoco frente sus posibilidades ni frente a sus usos. La crítica se dirige a la concepción epistemológica del discurso, en el entendido de que esta concepción se puede articular entendiendo al sujeto como receptos de dicho discurso”<sup>253</sup>. Mientras que en la Sociedad de la Información (SI) las TIC son vistas como meros utensilios a favor de la producción y el ocio, en la Sociedad de la Comunicación (SC), éstas son intermediarios importantes en la construcción de una sociedad más justa y equitativa, tanto en lo económico como en lo socio-cultural. Ambos conceptos ocultan un modelo de ciudadano, una idea preconcebida sobre lo que significa ser persona y cómo debe comportarse en el mundo dicho individuo, en esencia, sostienen un sujeto epistemológico<sup>254</sup> ideal. En la SI dicho sujeto es pasivo, apenas un espectador de las

---

<sup>252</sup> Comisión Económica para América Latina y el Caribe (CEPAL), “*Report of the Round Table on Telecommunications and Knowledge Society*”; Naciones Unidas, mayo 2006, p. 3 Disponible en: [https://repositorio.cepal.org/bitstream/handle/11362/38908/LCCARL96\\_en.pdf?sequence=1&isAllowed=y](https://repositorio.cepal.org/bitstream/handle/11362/38908/LCCARL96_en.pdf?sequence=1&isAllowed=y), consultado el 2 de junio de 2019.

<sup>253</sup> Lefranc Weegan, Federico, “*Terra Incógnita: Bases para una política criminal pro persona en la Sociedad Digital*”, Infotec, Centro de Investigaciones e Innovación en Tecnologías de la Información y Comunicación., México D.F., 2015, p. 44

<sup>254</sup> Lefranc Weegan, “*Sujetos...*”, op. cit. Pp.36-37

fuerzas socio-económicas dominantes: el Estado y el Mercado, cuyo único papel es el de consumidor. Por el otro lado, la SC nos propone un ser crítico y reflexivo, interesado en la participación activa (con ayuda de las TIC) para la construcción de una *sociedad del bienestar común*, en constante dialogo con las instituciones del Estado y sin estar sometido a los designios arbitrarios de las autoridades que representan a este último o a los intereses meramente económicos de los grandes conglomerados capitalistas.

## CONCLUSIONES

Para obtener acceso a conversaciones, datos e información privada de diversa índole de un número aún por determinar de activistas, defensores de derechos humanos y periodistas (ADyP) en el territorio nacional, de 2015 a 2017, diversas instituciones federales de seguridad mexicanas se valieron de un programa especializado en espionaje cibernético, *Pegasus*, que aprovechaba los errores de programación e infraestructura en teléfonos móviles para intervenir dichos aparatos y silenciosamente recopilar su contenido multimedia.

La convergencia de medios y capacidades para almacenar diversos tipos de contenido (audio, imágenes, posicionamiento geográfico en tiempo real, etc.) dentro de un solo aparato, así como el intercambio continuo de información privada en el ecosistema de los Smartphones, hacían de estas herramientas un objetivo notable para recabar información sobre objetivos relevantes para las autoridades.

El fin último del espionaje tecnológico, o el tratamiento que se hizo de los datos obtenidos es desconocido por el momento, sin embargo, al observar las fechas de los intentos de infección y compararlas con las actividades de los sujetos blancos del ataque, se identifica una confluencia entre ambas durante coyunturas críticas en el trabajo de los objetivos civiles. Todas tienen en común al Gobierno Federal como actor principal en dichos momentos clave. De manera general pueden agruparse de la siguiente forma; Aristegui Noticias y su investigación sobre la Casa Blanca; Carlos Loret de Mola con sus artículos sobre las ejecuciones extrajudiciales en Tlaxcala, Michoacán; el Centro PRODH y sus vínculos con el caso de la desaparición forzada de los 43 estudiantes de Ayotzinapa; el impulso del IMCCO para la aprobación de la Ley 3 de 3; y la Alianza por la Salud Alimentaria con su apoyo al incremento al impuesto de bebidas azucaradas. Las personas atacadas compartían una relevancia social por su postura inquisitoria y crítica ante hechos concretos de la administración del presidente Enrique Peña Nieto.

Tanto por investigaciones periodísticas como por declaraciones de las autoridades, se tiene certeza de que el gobierno mexicano dispone de tecnologías invasivas, hipotéticamente adquiridas para prevenir e investigar delitos, en concordancia con los principios y regulaciones legales nacionales e internacionales. Sin embargo, su uso en los casos documentados en contra ADyP fue de carácter ilegal, criminal y violatorio de los derechos

humanos de las personas afectadas. En ninguno de los intentos de infección con la plataforma *Peagaus* se respetó el principio de legalidad, fin legítimo, ni tampoco el espionaje constituía una medida necesaria ni proporcional. Al contrario, al actuar de esa manera las autoridades cometieron violaciones graves a los derechos de privacidad y protección de los datos personales de las víctimas.

Es deber de las autoridades realizar las indagaciones necesarias y dar cuenta a la sociedad sobre los hechos acontecidos. Debido a la gravedad de las acciones y sus repercusiones en el ejercicio de los derechos aludidos, las investigaciones deberán ser serias, exhaustivas, transparentes y sobre todo imparciales, en tanto que una de las instituciones involucradas es la misma que lleva la investigación, la antes llamada, Procuraduría General de la República.

Si bien existe una regulación en el derecho interno que contempla la intervención de las comunicaciones privadas y/o limitantes en el derecho a la protección de los datos personales, son necesarios controles más específicos cuando se traten herramientas con un potencial altamente intrusivo como *Pegasus*, a la vez que es indispensable una supervisión elaborada y competente cuando su uso sea necesario y completamente acorde a los parámetros legales y de derechos humanos.

Las TIC, y el uso de tecnologías en general, fueron medios para conseguir fines. Los grupos involucrados, especialmente los grupos de poder (desarrolladores y autoridades), se valieron por igual de sus fallos en diseño, programación y ejecución, así como de su penetración en la cotidianeidad de las sociedades humanas a finales de esta década para acceder a datos significativos a estos grupos. No obstante que el objetivo de las autoridades era infiltrarse en dichos aparatos, su valor no radicaba en ellos mismos, sino en su cualidad como contenedores y generados de datos provenientes de una persona. Es decir, los teléfonos móviles solo tenían valor en cuanto eran propiedad de una *persona específica* y, por lo tanto, ahí se resguardaba información privada de la misma.

Las herramientas de ingeniería social desplegadas por la plataforma *Pegasus* confirman el papel central del individuo en este escenario. La variedad de mensajes y la especificidad de los mismos dan cuenta de un escudriñamiento previo de los blancos, esta investigación retomaba elementos públicos y privados sobre los cuales se formuló un perfil psico-social bien definido que sirvió de base para plantear la estrategia de mensajes engañosos. Las

estructuras y tipologías de los SMS falsos también demuestran un conocimiento profundo de la composición psíquica humana que moldea nuestras respuestas cognitivas, emocionales y conductuales.

Durante las declaraciones iniciales del ex – presidente Peña Nieto respecto al tema, se observa también que el papel de las TIC está supeditado al de las personas. Las herramientas tecnológicas son utilizadas como medios preventivos o reactivos dependiendo del accionar del grupo percibido como contrario. La particularidad del discurso de EPN radica en que, cuando se habla del Gobierno, este rehúye la capacidad infractora del uso de la tecnología, negándolo categóricamente, pero es capaz de colocarse como la víctima, argumentando que él también ha sido objeto de intervenciones a su privacidad. La carga ideológica de fondo resalta las cualidades positivas de la autoridad e intenta minimizar las acusaciones de espionaje, dibujando una representación social negativa de los denunciantes. Al hacerlo, Enrique Peña Nieto ejecuta un *revictimización pública* de las víctimas de espionaje arbitrario gubernamental.

Del análisis de los diversos elementos que componen los intentos de invasión a la privacidad de ADyP con el software *Pegasus*, es posible afirmar que el papel ejercido por las TIC es relevante pero no definitorio. Las TIC no definen el derecho a la privacidad, sobre ellas, en efecto, puede materializarse y concretarse, pero no lo determina. El individuo, la persona, es el eje rector sobre el cual las herramientas tecnológicas se aglutinan para ofrecerle posibilidades de comunicación e intervención, pero no pueden garantizar el ejercicio adecuado de los mismos.

La ciencia y la tecnología han provisto a la humanidad de un cúmulo importante de conocimientos y utensilios para facilitar su estadía en el mundo, sin embargo, por sí solas no pueden regular y regir todos los campos de la existencia humana. Existe un discurso, una manera de concebir al mundo que entiende a las personas como mecanismos pasivos y receptores acrílicos de estímulos. Para esta visión de la realidad, los seres humanos son entes que deben ser guiados y tratados como mercancías o valores de uso. Coloca a las personas en el mismo nivel que las herramientas, pasos para un fin. En este modelo, la privacidad, y la dignidad en su conjunto, tienen poco o nulo valor. Claramente este no es el modelo de los derechos humanos. Estos pugnan por un modelo de humano pleno y digno, que desarrolle

todas sus cualidades en un ambiente de armonía, respeto y equidad. Al igual que la ciencia y la tecnología, los DDHH fueron una creación que respondió a necesidades de nuestra especie, y en sintonía con ellas aspira al crecimiento humano, por lo tanto, estas invenciones, estas ficciones humanas, no deberían ir por caminos separados, al contrario, se debe apelar a un trabajo en conjunto, con el cual, estaremos en mejores condiciones de garantizar una sociedad justa y plena para todas las personas, en todos los rincones de este mundo.

## **BIBLIOGRAFÍA:**

20 MINUTOS ESPAÑA y agencia EFE “*Cronología del caso Snowden, el joven que reveló el espionaje masivo de los Estados Unidos*”, 7 de julio de 2013, disponible en: <https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/>

ACKOFF L., Russel, “*Rediseñando el futuro*”, Limusa, México D.F., 2012

ADFAST, “*¿Qué es un malware?*”, Advast Software, s.r.o., s/f, disponible en: <https://www.avast.com/es-es/c-malware>

AGAZZI, Evandro, “*El bien, el mal y la ciencia*”, Tecnos, Madrid, 1996

AHMED, A. y Perlroth, N. “*Using texts as lures, Government psyware targets mexican journalists and their families*”, New York Times, Nueva York, 19 de junio de 2017, disponible en: <https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html>

ALEMANY Verdaguer, Salvador, *Curso de derechos humanos*, 1a. ed., Bosch, Casa Editorial, S.A., España, 1984

ALBERTIN, P. “*Psicología de la victimización criminal*”, en Soria, M. y Saíz, D. (coords.) *Psicología Criminal*, Pearson Educación, España, 2006

ALEXANDER, J.C., Giesen, B., Munch, R. y Smelser, N.J., “*The micro - macro link*”, University of California Press, Berkeley, 1987

AMNISTÍA INTERNACIONAL, “*Oriente Medio y Norte de África: indiferencia mundial que aumenta la impunidad hacia las violaciones de derechos humanos cometidas*”, Amnistía Internacional España, 26 de febrero de 2019, disponible en: <https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/oriente-medio-y-el-norte-de-africa-indiferencia-mundial-que-aumenta-la-impunidad-hacia-las-violacio/>

AMX Contenido SA de CV. <https://www.unotv.com/inicio/#>

ANIMAL POLÍTICO, Redacción, “*Gobierno espía: Peña Nieto amenaza, luego se retracta y después niega responsabilidad*”, Animal Político, 23 de junio de 2017. Disponible en: <https://www.animalpolitico.com/2017/06/gobierno-espia-pena-nieto/>

ARISTEGUI NOTICIAS, Redacción, “*La casa blanca de Enrique Peña Nieto (investigación especial)*”, Aristegui Noticias, México D.F., 9 de noviembre de 2014. Disponible en: <https://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/>

\_\_\_\_\_, Redacción, “*Revelan vínculos entre proveedor de equipo de espionaje y EPN*”, Aristegui Noticias, México D.F. 25 de junio de 2017, disponible en: <https://aristeguinoticias.com/2506/mexico/revelan-vinculos-entre-proveedor-de-equipo-de-espionaje-y-epn/>

ARTICLE 19, “*Informe 2016: Libertades en resistencia*”, Ciudad de México, 6 de abril de 2017, disponible en: [https://articulo19.org/wp-content/uploads/2017/04/Libertades-en-Resistencia\\_Informe-2016-A19.pdf](https://articulo19.org/wp-content/uploads/2017/04/Libertades-en-Resistencia_Informe-2016-A19.pdf)

ASAMBLEA DE LAS NACIONES UNIDAS, “*El derecho a la privacidad en la era digital*”, ONU, 31 de octubre de 2016. Disponible en: <http://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf>

BALLINAS Valdés, Christopher, “*Participación política y las nuevas tecnologías de la información y la comunicación*”, Tribunal Electoral del Poder Judicial de la Federación, México, 2011

BAUTISTA López, Angélica, “Comunicación social”, en Arciga Bernal, S.; Juárez Romero, J.; Mendoza García J. (Coords.) *Introducción a la psicología social*, Universidad Autónoma Metropolitana, México 2013

BATEY, Angus, “*The spies behind your screen*”, The Telegraph U.K., 24 de noviembre de 2011, disponible en: <https://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html>

BAZALIY, M, Flossman, M. Blaiçh, A. et al, “*Technical Analysis of Pegasus Spyware*”, Lookout Security Inc, S/F, disponible en: <https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf>

BEYME, Klaus von, “*Teorías políticas contemporáneas*”, IEP, Madrid, 1977

BIDART Campos, Germán J., “*Teoría general de los derechos humanos*”, 2ª reimpresión, Instituto de Investigaciones Jurídicas de la UNAM, México, 1993

Bobbio, Norberto, “*El tiempo de los derechos*”, Editorial Sistema, Madrid, 1996

\_\_\_\_\_ “Su fundamento dei diritti dell uomo”, *II Problema della guerra e le vie della pace*, Bologna, II, Mulino, 1979

BRINOL, Pablo; De la Corte, Luis y Becerra, Alberto, “*Qué es la persuasión*”, Biblioteca Nueva, Madrid, 2001

BREHM, J.W., “*A theory of psychological reactance*”, Academic Press, Oxford, 1966

BUNGE, Mario, “*La ciencia. Su método y su filosofía*”, Nueva Imagen, Segunda Edición, México, 2012

BYUNG-CHAN, Han, “*La sociedad del cansancio*”, Herder, Barcelona, 2012

CABERO, Julio, “*Las nuevas tecnologías en la sociedad de la Información*”, Universidad de Sevilla, 2006.. Disponible en: [https://www.researchgate.net/publication/238672345\\_Las\\_nuevas\\_tecnologias\\_en\\_la\\_Sociedad\\_de\\_la\\_Informacion](https://www.researchgate.net/publication/238672345_Las_nuevas_tecnologias_en_la_Sociedad_de_la_Informacion)

CAMACHO, Z. “*Sedena, bajo escrutinio por ocho contratos de 5.6 mil MDP*”. Contralínea, México, D.F., 22 de julio de 2012, disponible en: <https://www.contralinea.com.mx/archivo-revista/index.php/2012/07/22/sedena-bajo-escrutinio-por-ocho-c>

CARRASCO Araizaga, J., “*Tomas Zerón se dice dispuesto a que lo investiguen la Comisión para Ayotzinapa*”, Proceso, CDMX, 16 de enero, 2019, disponible en: <https://www.proceso.com.mx/567916/tomas-zeron-se-dice-dispuesto-a-que-lo-investigue-la-comision-para-ayotzinapa>

CASTELLS, Manuel, “*La era de la información. Economía, sociedad y cultura*” Vol. 1, Siglo XXI, México, 1996, Disponible en: <http://www.economia.unam.mx/lecturas/inae3/castellsm.pdf>

CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES, Artículo 291, primer párrafo. Estados Unidos Mexicanos

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE (CEPAL), “*Los caminos hacia una sociedad de la información en América Latina y el Caribe*”, Naciones

Unidas, Julio de 2003, p2. Disponible en:  
[https://repositorio.cepal.org/bitstream/handle/11362/1836/S0015K19\\_es.pdf](https://repositorio.cepal.org/bitstream/handle/11362/1836/S0015K19_es.pdf)

\_\_\_\_\_, “*Report of the Round Table on Telecommunications and Knowledge Society*”;  
Naciones Unidas, mayo 2006, p. 3 Disponible en:  
[https://repositorio.cepal.org/bitstream/handle/11362/38908/LCCARL96\\_en.pdf?sequence=1&isAllowed=y](https://repositorio.cepal.org/bitstream/handle/11362/38908/LCCARL96_en.pdf?sequence=1&isAllowed=y)

COMISIÓN DE LOS DERECHOS HUMANOS DEL DISTRITO FEDERAL, “*Defensor, El uso de las nuevas tecnologías y los derechos humanos*”, Ciudad de México, Junio de 2016, disponible en: [https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor\\_06\\_2016.pdf](https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf)

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, “*Situación de Derechos Humanos en México*”, Organización de los Estados Americanos, 31 de diciembre de 2015, disponible en: <http://www.oas.org/es/cidh/informes/pdfs/mexico2016-es.pdf>

COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS, “*Análisis situacional de los Derechos Humanos de Periodistas y Personas Defensoras*”, Ciudad de México, 2018. Disponible en: <http://informe.cndh.org.mx/menu.aspx?id=40063>

CONSANTE, Alberto, “La memoria perdida de las cosas (crítica a la modernidad)”, en *Claves del pensamiento*, Vol. 1, No. 1, Scielo, México, 2007, Disponible en: [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S1870-879X2007000100005](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-879X2007000100005)

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Art. 16, Párrafo segundo

CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS. ORGANIZACIÓN DE LAS ESTADOS AMERICANOS, 1969

CONVENCIÓN DE LOS DERECHOS DEL NIÑO. Art.16. Asamblea de las Naciones Unidas, 1989.

CONVENIO EUROPEO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES. Art. 8. Consejo de Europa, 1950

CORTE IDH, La Colegiación de Periodistas (Arts. 13 y 29 Convención Americana Sobre Derechos Humanos). Opinión Consultiva OC-5/85, Serie A núm. 5 13 de noviembre de 1985

CORTE IDH, *Caso Herrera Ulloa vs. Costa Rica*. Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C. núm. 107, Sentencia de 2 de julio de 2004

CORTE IDH, *Caso Palamara Iribarne vs. Chile*, Fondo, Reparaciones y Costas. Serie C, núm. 155, Sentencia de 22 de noviembre de 2005

CORTE IDH, *Caso Claude Reyes y otros vs. Chile*. Fondo, Reparaciones y Costas, Serie C, núm. 151, Sentencia de 19 de septiembre de 2006

CORTE IDH, *Caso Chaparro Álvarez y Lapo Íñiguez vs. Ecuador*. Excepciones preliminares, Fondo, Reparaciones y Costas, Serie C, núm. 170. Sentencia de 21 de noviembre de 2007

CORTE IDH, *Caso Kimel vs. Argentina*. Fondo, reparaciones y costas, Serie C. Núm. 177, Sentencia de 2 de mayo de 2008

CORTE IDH, *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, Fondo, Reparaciones y Costas, Serie C. núm. 193, Sentencia de 9 de enero de 2009

CORTE IDH, *Caso Escher vs. Brasil*. Excepciones preliminares, Fondo, Reparaciones y Costas, Serie C. núm. 200, Sentencia de 6 de julio de 2009

CROVI DRUETTA, Delia, “*Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza*”, Revista Mexicana de Ciencias Políticas y Sociales, año XLV, no. 185, México, mayo – agosto de 2002, p.16. Disponible en: <https://www.redalyc.org/pdf/421/42118502.pdf>

CRUNCHBASE, Person: Asaf Anzuri, disponible en: <https://www.crunchbase.com/person/asaf-zanzuri#section-overview>

\_\_\_\_\_ Person: Rodrigo Ruiz De Teresa Treviño, disponible en: <https://www.crunchbase.com/person/rodrigo-ruiz-de-teresa-trevino#section-overview>

CRUZ Parcero, Juan A., “Crisis de la Fundamentación de los Derechos Humanos en el siglo XIX”, en Margarita Moreno-Bonnett y María del refugio (Coords.), *La Génesis de los*

*derechos humanos en México*, Universidad Nacional Autónoma de México, México, D.F., 2006.

DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS. Art. 12. Asamblea General de las Naciones Unidas, 1948

DOISE, W. “*Psicología Social Experimental*”, Editorial Hispano: Europa, 1980

EL UNIVERSAL, “*Perfil, Carlos Cayetano*”, México, D.F., 29 de julio de 2017. Disponible en: <https://www.eluniversal.com.mx/articulo/nacion/seguridad/2017/07/29/perfil-carlos-cayetano>

\_\_\_\_\_, “*Perfil. Tomás Zerón de Lucio*”, México, D.F., 14 de septiembre de 2016, Disponible en: <https://www.eluniversal.com.mx/articulo/nacion/2016/09/14/perfil-tomas-zeron-de-lucio>

ESTÉVEZ López, Ariadna, “*Los derechos humanos*”, disponible en: [http://www.academia.edu/25038679/Derechos\\_humanos](http://www.academia.edu/25038679/Derechos_humanos)

FOX-BREWSTER, Thomas, “*NSO Group: Los espías israelíes que hackean iPhones con un solo SMS*”, Forbes México, 18 de abril de 2017, disponible en: <https://www.forbes.com.mx/nso-group-los-espias-israelies-que-hackean-iphones-con-un-solo-sms/>

FREUD, Sigmund, “*El malestar en la cultura*”, Alianza Editorial, tercera edición, Madrid, 2013

GALIMBERTI, Umberto, “*Los mitos de nuestro tiempo*”, Debate, Barcelona, 2013

GELLMAN, B., Blake, A. y Miller G., “*Edward Snowden comes forward as source of NSA leaks*”, The Washington Post, 9 de junio de 2013, disponible en: [https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459\\_story.html?utm\\_term=.84a966e21cf2](https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.84a966e21cf2)

GOBIERNO DE MÉXICO. “*Directorio Tomas Zerón de Lucio*”, Portal del Gobierno de México, Directorio. Disponible en: <https://www.gob.mx/ejn/estructuras/tomas-zeron-de-lucio>

GROSS Espiell, Héctor “Nuevas tendencias del constitucionalismo en América Latina”, en *Tendencias del constitucionalismo en Iberoamérica*, Universidad Nacional Autónoma de México, México, 2009

GUEVARA Rosas, Erika, “*Enrique Peña Nieto. El recuento de los daños*”, Amnistía Internacional Américas, 30 de noviembre de 2018, disponible en: <https://www.amnesty.org/es/latest/news/2018/11/enrique-pena-nieto-el-recuento-de-los-danos/>

GUTIÉRREZ de Pineres Botero, C.; Coronel, E. y Andres Pérez, C. “*Revisión teórica del concepto de victimización secundaria*”, *Liberalit*, vol. 15, núm. 1, 2009

HARRIS, Marvin, “*Antropología Cultural*”, Alianza Editorial, Tercera edición, Madrid, 2011

HERTWIG, Ralph, “Efficient Social Engineering and Realistic Cognitive Modeling: A Psychologist’s Thoughts”, en *Economics and Psychology*, MIT Press, Cambridge, 2007, pp. 247 – 251, disponible en: [http://library.mpib-berlin.mpg.de/ft/rh/RH\\_Efficient\\_2007.pdf](http://library.mpib-berlin.mpg.de/ft/rh/RH_Efficient_2007.pdf)

HIRSCHAUGE, Ory y Orpaz ,Inbal; “*U.S. Fun to Buy NSO and Its Smartphone-snooping Software*” Haaretz, Israel News, 17 de febrero de 2014, disponible en: <https://www.haaretz.com/israel-news/business/u-s-fund-to-buy-snooping-software-1.5323394>

HUBER, Florian, “*Tecnologías de Información y Comunicación (TIC), protección de datos y derechos humanos en la jurisprudencia del Tribunal Europeo de Derechos Humanos*”, Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, México 2016, p. 82. Disponible en: <https://archivos.juridicas.unam.mx/www/bjv/libros/9/4065/8.pdf>

JIMÉNEZ Cano, Rosa, “*Así espía la CIA en Internet, según Wikileaks*”, El País, Madrid, 7 de marzo del 2018, disponible en: [https://elpais.com/internacional/2017/03/07/estados\\_unidos/1488902840\\_337837.html](https://elpais.com/internacional/2017/03/07/estados_unidos/1488902840_337837.html)

KAFKA, Filip, “*Nuevas señales de que Hacking Team está activo*”, welivesecurity by eset, 13 de marzo de 2018, disponible en: <https://www.welivesecurity.com/la-es/2018/03/13/nuevas-senales-de-que-hacking-team-esta-activo/>

LABRADA Rubio, Valle, “*Introducción a la teoría de los derechos humanos: fundamento, historia, Declaración Universal*” de 10.XII.1948, 1a. edición, Civitas, S.A., España, 1998

LAMPERT, Ernâni, “*Posmodernidad y universidad: ¿una reflexión necesaria?*”, Perfiles educativos, vol. 30, México, Enero 2008, pp. 79-93, Disponible en: [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0185-26982008000200005](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-26982008000200005)

LEFRANC Weegan, Federico, “*Los límites de la interpretación de la dignidad humana. La presencia Kantiana en su concepción jurídica actual*”, Tesis Doctoral, Universitat Atonoma de Barcelona, Diciembre de 2009

\_\_\_\_\_ “*Terra Incógnita: Bases para una política criminal pro persona en la Sociedad Digital*”, Infotec, Centro de Investigaciones e Innovación en Tecnologías de la Información y Comunicación., México D.F., 2015

\_\_\_\_\_ “*Los sujetos de la SIC*”, en *Derecho y TIC. Vertientes actuales*, UNAM, Instituto de Investigaciones Jurídicas, México, 2016, p. 36. Disponible en: <https://biblio.juridicas.unam.mx/bjv/detalle-libro/4065-derecho-y-tic-vertientes-actuales>

LEÓN, J.L. “*Persuasión de Masas. Psicología y efectos de las comunicaciones sociopolíticas y comerciales*”, Deusto, Bilbao, 1989

LEVENTHAL, H. “*Findings and Theory in the Study of Fear Communications*”, *Advances in Experimental Social Psychology*. Vol. 5, 1970

LEY DE LA POLICÍA FEDERAL, artículo 48. Estados Unidos Mexicanos

LEY DE SEGURIDAD NACIONAL, artículo 5, numeral I. Estados Unidos Mexicanos

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS Obligados. Art. 3º, 18, 19, 22, 80 y 81

LISCHINSKY, Alon, “*Un caso de doble discurso en política: contraargumentos del gobierno español al racismo discursivo de la oposición parlamentaria*”, *Discurso & Sociedad*, Vol. I, núm. 1, Barcelona, 2007

LOCKE, John, “*Ensayo sobre el gobierno civil*”, Ediciones Nuevo Mar, México D.F., 1984

MAC-GREGOR Poisot, Eduardo F; Caballero Ochoa, Jose *et al.* “*Estándares sobre principios generales*”, en *Derechos Humanos en la Constitución: Comentarios de Jurisprudencia Constitucional e Interamericana*, Suprema Corte de Justicia de la Nación, México, D.F. 2013

MALENKOVICH, Serge, “*¿Qué es un keylogger?*”, Kaspersky Latinoamerica, 9 de abril de 2013, disponible en: <https://latam.kaspersky.com/blog/que-es-un-keylogger-2/453/>

MARCZAK, Bill y Scott-Railton, John, “*The Million Dollar Dissident. NSO Group’s Iphone Zero-Days used against a UAE Human Rights Defender*”, Citizen Lab, Universidad de Toronto, 24 de agosto de 2016, disponible en: <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>

MARCZAK, B., Scott Railton, J. y otros. “*Hide and seek, tracking NSO Group’s Pegasus Spyware in Operations in 45 Countries*”, Munk School of Global Affairs and Public Policy, Universidad de Toronto, 19 de septiembre de 2018, disponible en: <https://citizenlab.ca/2018/09/hide-and-see-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

MARKUS, Gabriel, “*¿Por qué no existe el mundo?*”, Océano Editorial, México D.F., 2016.

MARTÍNEZ DE PISÓN, José, “*Derechos Humanos. Un ensayo sobre su historia, su fundamento y su realidad*”, editorial Egido, 1997

MENDELSON, Everett, “The social construction of scientific knowledge”, en Mendelson, et al, (comps), *The social production of scientific knowleds*, Reidel Publishing Company, Dordrecht y Boston, 1977. Traducción de Jorge Núñez Jover.

MERCA2.0, Mesa Editorial, “*Sitios Web más visitados por mexicanos*”, Revista Merca2.0., disponible en: <https://www.merca20.com/sitios-web-mas-visitados-por-los-mexicanos/>,

MILENIO DIGITAL, “PGR recibió Pegasus en 2015”, Milenio, México D.F. 28 de junio de 2017, disponible en: <https://www.milenio.com/politica/pgr-recibio-pegasus-en-2015>

MINE, Main, “La informatización de la sociedad”, en *Policy implications of Data Network Developments in the OECD*, Organización para la Cooperación y el Desarrollo Económico, Paris, 1980, Traducción de: Mario R. dos Santos. Disponible en: <http://biblioteca.clacso.edu.ar/ar/libros/critica/nro7/minc.pdf>

MITNICK, Kevin y Simon, William, “*El arte de la intrusión*”, AlfaOmega, Madrid, abril 2007

MOLET, Jorge, “Adopción de México del Convenio 108 del Consejo de Europa, protección y flujo internacional de datos”, *El Financiero*, México, 20 de junio de 2018, disponible en: <https://www.economista.com.mx/opinion/Adopcion-de-Mexico-del-Convenio-108-del-Consejo-de-Europa-proteccion-y-flujo-internacional-de-datos-20180620-0098.html>

MORRIS, Desmond, “*El mono desnudo. Un estudio del animal humano*”, Plaza & Janéz, Barcelona, 1973

MUÑOZ DE BAENA, José Luis, “Fundamentos filosóficos de los derechos humanos” en *Pasado, presente y futuro de los derechos humanos*, Comisión Nacional de los Derechos Humanos, México, 2004

NSO Group, About US, NSO Grup web page, disponible en: <https://www.nsogroup.com/about-us/>

NORA, Simon y Alan Minc, “*Informatización de la sociedad*”, Fondo de Cultura Económica, México D.F. 1980

NÚÑEZ Jover, Jorge, “Rigor, objetividad y responsabilidad social: la Ciencia en el encuentro entre Ética y Epistemología”, en *La ciencia y la tecnología como procesos sociales. Lo que la educación científica no podría olvidar*, Organización de los Estados Iberoamericanos, s.f. disponible en: <https://www.oei.es/historico/salactsi/nunez05.htm>

OLMOS, Raul; Durán, Valeria y Lizárraga Daniel, “PGR compró Pegasus a prestanombres”, Mexicanos Contra la Corrupción y la Impunidad A. C., México, D.F., 28

de Julio de 2017, disponible en:  
<https://contralacorrupcion.mx/web/pgrcompropegasus/index.html>

OLMOS, Raul, Mexicanos Contra la Corrupción y la Impunidad, “*Funcionario Federal era uno de los socios del grupo empresarial que vendió Pegasus*”, Animal Político, México, D.F. 20 de febrero de 2018, disponible en: <https://www.animalpolitico.com/2018/02/funcionario-federal-empresa-pegasus-pgr/>

OPPENHEIMER, Andrés, “*¡Sálvense quien pueda! El futuro del trabajo en la era de la automatización*”, Debate, Madrid, 2018

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS, Art. 19. Asamblea General de las Naciones Unidas. 1966

PECES Barba, G. “*Curso de derechos fundamentales. Teoría General*”, en Boletín Oficial del Estado, Universidad Carlos III, Madrid, 1995.

PÉREZ, Armando, E-mail filtrado, Wikileaks, 28 de noviembre, 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/5391>

PÉREZ Luño, Antonio E., “*Los derechos fundamentales*”, 2a. ed., Tecnos, España, 1986

PERLROTH, Nicole, “*Spyware’ Odd Tarjets: Backers of mexico’s Soda Tax*”, The New York Times, Nueva York, 11 de febrero de 2017, disponible en: [https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?\\_r=0](https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?_r=0)

POPPER, Karl, “*Conjeturas y refutaciones. El desarrollo del conocimiento científico*”, Paídos, Buenos Aires, 1983

PRATKANIS, Anthony y Aronson, Elliot, “*La era de la Propaganda. Uso y abuso de la persuasión*”, Paídos, Barcelona, 1994

PRESIDENCIA ENRIQUE PEÑA NIETO, “*Inauguración del Parque Industrial en Lagos de Moreno*”, Video almacenado en la plataforma Youtube, 22 de junio de 2017, disponible en: <https://www.youtube.com/watch?v=EqoKGVEdmPw>

PRINCE, De Solla, “*Ciencia y tecnología: Distinciones e interacciones*”, Estudios sobre sociología de la Ciencia, Editorial Alianza Universidad, Madrid, 1980.

PROCESO, Redacción “*Rechaza Balam Seguridad Privada vender el software Pegasus*”, Proceso, México D.F. 27 de junio de 2017, disponible en: <https://www.proceso.com.mx/492612/rechaza-balam-seguridad-privada-vender-software-pegasus>

QUIAN, Alberto “*El impacto político y mediático de Wikileaks*”, Editorial UOC (Oberta OUC Publishing, SL), Barcelona, Abril 2014

R3D, Red en defensa de los derechos digitales, “*El Estado de la Vigilancia, Fuera de control*”, Ciudad de México, Noviembre de 2016,. Disponible en: <https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016-FINAL1.pdf>

\_\_\_\_\_, “*Destapa la vigilancia: promotores del impuesto al refresco, espíados con malware gubernamental*”, R3D, 11 de febrero de 2017, disponible en: <https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espíados-con-malware-gubernamental/>

\_\_\_\_\_, “*A dos años de Gobierno Espía: Una cronología de la Impunidad*”, 19 de Junio de 2019, disponible en: [https://r3d.mx/2019/06/19/gobierno-espia-cronologia/?fbclid=IwAR2o\\_nbj9ytDTGY7vXHbw0KwVcFRyP15FhCfP2ZkI3zgMQDdYrFPDTo9RvE](https://r3d.mx/2019/06/19/gobierno-espia-cronologia/?fbclid=IwAR2o_nbj9ytDTGY7vXHbw0KwVcFRyP15FhCfP2ZkI3zgMQDdYrFPDTo9RvE)

R3D, ARTÍCULO 19 Y SOCIAL TIC, “*Gobierno Espía. Vigilancia sistemática a periodistas y defensores derechos humanos en México*”, Ciudad de México, junio de 2017, disponible en: <https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf>

RIVERA, Alba Nydia, “*Factores que determinan la atribución de altruismo*”, Revista Latinoamericana de psicología, vol. 12, núm. 1, Bogotá, 1980

ROBERTO Arteaga, José, “*Nextel y Iusacell concluirán fusión con AT&T en 2016*”, Forbes México, 24 de agosto de 2015, disponible en: <https://www.forbes.com.mx/nextel-y-iusacell-concluiran-fusion-con-att-en-2016/>

RODRÍGUEZ Solis, S. E-mail filtrado, Wikileaks, 19 de enero, 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/5275>

RODRIGORUIZTERESABLOG, Home, disponible en: <https://rodrigoruizdeteresa.mx/index.html>

RODRÍGUEZ y Rodríguez, Jesús, Dic. Juri. Mex., Tomo III, México 1983

ROUSE, Margaret, “*Definition Pegasus Malware*”, TechTarget SearchSecurity, última actualización, 28 de junio de 2019, disponible el: <https://searchsecurity.techtarget.com/definition/Pegasus-malware>

SAHAL, Devendra, “*Technological guidepost and innovation avenues*”, Research Policy, vol. 14 No.2, Elsevier, Amsterdam, 1985.

SALAHADINE, Fatima y Kaabouch, Naima; “Social Engineering Attacks: A survey”, en *Future Internet*, Universidad de Dakota del Norte, Grand Forks, EUA, 2 de abril de 2009, p. 5, disponible en: [https://res.mdpi.com/d\\_attachment/futureinternet/futureinternet-11-00089/article\\_deploy/futureinternet-11-00089.pdf](https://res.mdpi.com/d_attachment/futureinternet/futureinternet-11-00089/article_deploy/futureinternet-11-00089.pdf)

SCJN, Primera Sala. *Amparo en Revisión 1621/2010*, Semanario Judicial de la Federación y su Gaceta, Novena época, t. XXXIV, agosto de 2011

SCJN, Pleno. *Acción de Inconstitucionalidad 32/2012*

SCJN, Primera Sala, *Contradicción de Tesis 194/2012*, Semanario Judicial de la Federación y su Gaceta, Libro XVII, t. 1, Febrero de 2013

SCJN, Segunda Sala, *Tesis 2ª XLIV/2016 (10ª)*, Semanario Judicial de la Federación, Décima Época. Agosto de 2016

SCOTT-RAILTON, J.; Marczak, B.; Guarnieri, B. et al, “*Supporters of Mexico’ Tax Soda Targeted With NSO Exploit Links*”, Citizen Lab, Universidad de Toronto, 11 de febrero de 2017, disponible en: <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>

SEGOVIA, L.; Torres, F.; Rosillo, M.; Tapia, E.; Albarado, F, et al; “Social engineering as an attack vector for ransomware”, en *Proceedings of the Conference on Electrical Engineering and Information Communication Technology*, Pucó, Chile, Octubre de 2017

SERRA, Arthur, “Investigación en Internet y nuevos modelos de desarrollo: El proyecto i2CAT”, en Finquelievich, Susana (Coord.) *Desarrollo Local en la Sociedad de la Información: Municipios e Internet*, Editorial La Crujía, Buenos Aires, 2005

SERRANO, Sandra y Vázquez, Daniel, “*Fundamentos Teóricos de los Derechos Humanos*” Comisión de Derechos Humanos del Distrito Federal, México, D.F., s.f. p. 217. Disponible en: [https://cdhdf.org.mx/serv\\_prof/pdf/fundamentosteoricosdelosderechos.pdf](https://cdhdf.org.mx/serv_prof/pdf/fundamentosteoricosdelosderechos.pdf)

SORIANO Flores, Jesús, “*Elementos históricos y jurídicos para la conceptualización contemporánea de los derechos humanos*”, Anuario de Derechos Humanos del Instituto de la Judicatura Federal, México, 2017

SQUELLA Agustín y López Calera Nicolás, “*Derechos Humanos ¿invento o descubrimiento?*”, 1ra. Ed, Fundación Coloquio Jurídico Europeo, Madrid, 2010

SUÁREZ, Francisco, “La dependencia científica y su relación con la dependencia cultural y tecnológica”, en *Autonomía nacional o dependencia: la política científico-tecnológica*, Paídos, Buenos Aires, 1975.

TEDH, *Caso Klaas vs. Alemania*, núm. 5029/71, Sentencia de 6 de septiembre de 1978

TEDH, *Caso The Sun Day Times vs. Reino Unido*, núm. 6538/74, Sentencia de 26 de abril de 1979

TEDH, *Caso Silver y otros vs Reino Unido*, núms. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, Sentencia de 25 de marzo de 1983

TEDH, *Caso Malone vs Reino Unido*, núm. 8691/79, Sentencia de 2 de agosto de 1984

TEDH, *Caso Leander vs Suecia*, núm. 9248/81, Sentencia de 26 de marzo de 1987

TEDH, *Caso Kruslin vs. Francia*, núm. 11801/85, Sentencia de 24 de abril de 1990

TEDH, *Caso, A. vs. Francia*, núm. 14838/98, Sentencia de 23 de noviembre de 1993

TEDH, *Caso Kopp vs Suiza*, núm, 23224/94, Sentencia de 25 de marzo de 1998

TEDH, *Caso Amman vs. Suiza [GC]*, núm 27798/95, Sentencia de 16 de febrero de 2000

TEDH, *Caso Rotaru vs. Rumania [GC]*, núm. 28341/95, Sentencia de 4 de mayo de 2000

TEDH, *Caso P.G. y J.H. vs. Reino Unido*, núm. 44787/98, Sentencia de 25 de septiembre de 2001

TEDH, *Caso Perks vs. Reino Unido*, núm. 44647/98, Sentencia de 28 de enero de 2003

TEDH, *Caso Vetter vs. Francia*, núm. 59842/00, Sentencia de 31 de mayo de 2005

TEDH, *Caso Dumitru Popescu vs. Rumania*, (núm. 2), núm. 71525/01, Sentencia de 26 de abril de 2007

TEDH, *Caso S. y Marper vs. Reino Unido*, [GC], núms. 30562/04 y 30566/04, Sentencia de 4 de diciembre de 2008

TEDH, *Caso Iordachi, y otros vs Moldavia* núm. 25198/02, Sentencia de 10 de febrero de 2009

TEDH, *Caso Asociación “21 de diciembre 1989” y otros vs. Rumania*, núms. 33810/07 y 18817/08, Sentencia de 24 de mayo de 2011

TEDH, *Caso Shimovolos vs. Rusia*, núm. 30194/09, Sentencia de 21 de junio de 2011

TEDH, *Caso Khan vs. Reino Unido*, núm. 622/10, Sentencia de 20 de diciembre de 2011

TEDH, *Caso Draksas vs. Lituania*, núm. 36662/04, Sentencia de 31 d julio de 2012

TEDH, *Caso Sciacca vs Italia*, núm, 50774/99, Sentencia de 11 de enero de 2015

TESSER, Abraham y Shaffer, David, “*Attitude and Attitude Change*”, *Annual Review of Psychology*, Vol. 41, Febrero de 1990

UNESCO, *Les dimensions internacionales des droits de l’homme*. Publicado por UNESCO, 1978

UNIVERSIDAD NACIONAL DE LUJAN, “*Ingeniería Social*”, Departamento de Seguridad de la Universidad Nacional de Lujan, Buenos Aires, s/f, disponible en: <http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/11>

UNIVISIÓN

MEDIA.

[https://corporate.univision.com/?\\_ga=2.239144131.1141334171.1567794224-1636358028.1567794221#gs.lzvb8l](https://corporate.univision.com/?_ga=2.239144131.1141334171.1567794224-1636358028.1567794221#gs.lzvb8l)

VAN DIJK, Teun, “*Elite discourse and racism*”, Sage Publications Inc, Newbury Park, CA, 1993

\_\_\_\_\_ “*Ideology: A multidisciplinary study*”, Sage, Londres, 1998

\_\_\_\_\_ “Context models in discourse processing”, en Van Oostendorp, Herre & Goldman, Susan R. (coords.), *The construction of mental representations during reading*, Lawrence Erlbaum Associates. Mahwah NJ, 1999

\_\_\_\_\_ “El análisis crítico del discurso”, en *Anthropos*, Barcelona, 189, septiembre – octubre de 1999

\_\_\_\_\_ “*Ideología y análisis del discurso*”, Utopía y Praxis Latinoamericana, año 10, núm. 29 Universidad del Zulia, Maracaibo- Venezuela, Abril - Mayo de 2005

VELASCO, Alex, E-mail filtrado, Wikileaks, 29 de enero de 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/8964>

VELASCO, Alex, E- mail filtrado, Wikileaks, 26 de agosto de 2014, disponible en: <https://wikileaks.org/hackingteam/emails/emailid/6584>

VELÁZQUEZ, José M., “*Curso elemental de psicología*”, Compañía General de Ediciones, S.A., Vigésima octava edición, México D.F., 1980

VIDAURRI Aréchiga, Manuel y Soriano Flores, José, “Derechos Humanos, Concepto y Fundamento”, en *Investigaciones Jurídicas* no.79, Universidad Autónoma de Guanajuato, 2007

VILLÁS Duran, Carlos “El derecho internacional de los derechos humanos” en *Curso de Derecho Internacional de los derechos humanos*, Editorial Trotta, Madrid España, 2002

WIKILEAKS, About, disponible en: <https://wikileaks.org/What-is-WikiLeaks.html>

WIKILEAKS, Hacking Team leak, 8 de julio de 2005, disponible en: <https://wikileaks.org/hackingteam/emails/>

WORDPRESS, Home, Asaf Anzuri, disponible en: <https://asafzanzuri.wordpress.com/>