Análisis ético de la información en el escándalo Pegasus

Ethical analysis of information in the Pegasus scandal

Alberto Rafael Román Soltero
Universidad Tecnológica Latinoamericana en Línea (UTEL), México
Departamento de Investigación, Universidad Vizcaya de las Américas Piedras Negras, México
ralphroman@hotmail.com

Verónica Luna Bautista
Universidad Tecnológica Latinoamericana en Línea (UTEL), México
bautistaveronica39@gmail.com

Román Sarabia Ramos Ramos
Universidad Tecnológica Latinoamericana en Línea (UTEL), México
rsarabiar@hotmail.com

Álvaro David Lechuga Salais
Universidad Tecnológica Latinoamericana en Línea (UTEL), México
alvaro.david.18@gmail.com

Ricardo Hernández Carrasco
Universidad Tecnológica Latinoamericana en Línea (UTEL), México
Instituto de Turismo, Universidad del Mar (UMAR), México
ricardo@huatulco.umar.mx

Noé Amir Rodríguez Olivares
Universidad Tecnológica Latinoamericana en Línea (UTEL), México
Departamento de Energía, Centro de Ingeniería y Desarrollo Industrial (CIDESI), México
noeamir@gmail.com

doi: https://doi.org/10.36825/RITI.07.14.003

Recibido: Julio 16, 2019
Aceptado: Septiembre 05, 2019

Resumen: En el presente artículo se muestra un análisis ético del *Spyware* Pegasus de NSO Group, y su presunto uso inadecuado en los Estados Unidos Mexicanos. Los antecedentes del mismo, la perspectiva ética de los involucrados en torno a este escándalo periodístico, la gestión de la información obtenida y su respectivo impacto. Tomando este caso para propiciar un método inductivo de raciocinio respecto a la *Big Data* y sus implicaciones éticas, la obtención masiva de información, la forma en que se obtenga, el uso que se le da a la información y la carente regulación que tenemos sobre la misma. Fragmentando su análisis desde las diversas perspectivas posibles, siempre con un enfoque neutral, sin tomar ninguna postura partidista. Haciendo una reconstrucción de los hechos

a base de toda la recopilación de datos posible en torno al tema, analizando los resultados y obteniendo conclusiones objetivas, según lo establecido por el pensamiento científico.

Palabras clave: *Big Data, Ética, Aspectos Éticos, Programa de Computador Invasivo, Pegasus.*

Abstract: This article presents an ethical analysis of the Pegasus Spyware from the NSO Group, and its alleged misuse in the United Mexican States. The background of the same, the ethical perspective of those involved in this journalistic scandal, the management of the information obtained and their respective impact. Taking this case to promote an inductive method of reasoning with respect to Big Data and its ethical implications, the massive obtaining of information, the way in which it is obtained, the use that is given to the information and the lack of regulation that we have of the same. Fragmenting his analysis from the various possible perspectives, always with a neutral approach, without taking any partisan position. Making it a reconstruction of the facts based on all possible data collection around the subject, analyzing the results and obtaining objective conclusions, as established by scientific thinking.

Keywords: *Big Data, Ethics, Ethical Aspects, Invasive Software, Pegasus.*

1. Introducción

Diversos autores definen al *Big Data* como macrodatos (gran conjunto de información) según indica su traducción literal [1], algunos añaden al termino la necesidad de utilizar formas innovadoras para procesar esa gran cantidad de datos [2], otros autores incluso lo han llegado a contextualizar como una revolución [3], sin embargo, los autores que se han especializado en su terminología, lo determinan como un concepto cambiante según el contexto que se le dé, en continua evolución, y con el objetivo implícito de permitir una mejor comprensión y facilitar la toma de decisiones [4] [5].

Para el presente artículo, evitando un maremágnum conceptual, englobando el diverso uso que da el estado del arte, se define al *Big data* como la gestión y transición de datos que no pueden ser procesados de la manera convencional, debido a qué se presentan en formas muy diversas, con un gran volumen y velocidad, creciendo exponencialmente, qué mediante la minería de datos y dependiendo de su estratificación, análisis y objetivo de estudio, proyectan diversa información de valor para los involucrados.

Teniendo claro este concepto y tras saber que en el Fórum Económico Mundial celebrado el 2012 en la ciudad Suiza de Davos se destacó el potencial del *Big Data* literalmente como "*A new class of economic asset, like currency or gold*" (Un nuevo activo económico como el dinero o el oro) [6]. Es imprescindible pensar en la ética, su valor y la gestión de la información, como base en el desarrollo del *Big Data*, para llevar por el mejor rumbo a la humanidad, siendo ese conjunto de normas morales que rigen la conducta de la persona en cualquier ámbito de la vida [7].

Utópicamente hablando, es la llave para una economía global perfecta, teniendo conocimiento exacto sobre todos los habitantes del planeta, no solo analizándolo mediante suposiciones y muestreos, se lograría una perfecta repartición de recursos y oportunidades teniendo oferta y demanda en perfecto equilibrio. La política evolucionaría a una democracia idónea donde se cubran las verdaderas necesidades de las naciones y el mundo tome el rumbo óptimo al progreso.

La ética puede ser la clave para el desarrollo o destrucción de este mundo por medio del *Big Data*. Entre la ola de conocimiento y opiniones que existen respecto a la ciencia de datos, hay quienes definen a este paradigma tecnológico qué es el *Big Data*, como el Petróleo del futuro a lo cual aprovecharé la analogía para desarrollar lo siguiente:

Así como el petróleo ha revolucionado a toda la humanidad y el rumbo del mundo, gran parte de los problemas que tenemos en la actualidad, como lo son la contaminación y el calentamiento global, son producto de este oro negro, debido a que su explotación desmedida no tuvo, ni tiene el fin de una mejora global, y persigue

intereses personales. De la misma manera sucede con la *Big Data*, considero la ética y la filantropía son la clave para desarrollar toda esta basta y variada información de distintos usuarios, de la mejor manera posible hacia un bien común.

La ética de los manipuladores del *Big Data* en cualquier postura, (política, social o económica) es el factor clave para destruir o construir un sistema [8]. Por ejemplo: la utópica repartición de los recursos y oportunidades comerciales al rededor del globo mediante el *Big Data* (mencionada un par de párrafos con anterioridad), sería lógicamente un impacto positivo, sin embargo, bajo este mismo ejemplo, pero con un Científico de Datos que careciera de ética alguna, y tuviera una visión oportunista, teniendo esa misma base de datos, se puede dar un impacto negativo, puesto se podría desarrollar el "mismo sistema utópico de equidad" favoreciendo a ciertas empresas o gobiernos.

Otro inevitable punto a mencionar dentro de todo esto, es la Seguridad y la Privacidad, puesto desde una postura gubernamental podemos apostar en el *Big Data* una óptima seguridad nacional libre de terrorismo, teniendo pleno conocimiento de las actividades y el IoT (*Internet of Things*) de los ciudadanos y extranjeros de determinado país. Y desde esta perspectiva, esto tiene un impacto positivo. Pero afecta negativamente a nuestra sociedad, puesto la investigación en muchas ocasiones, pierde su valía si no cuenta con elementos como la privacidad, la disponibilidad y la integridad [9].

El uso de la tecnología *Big Data* es fácticamente adecuado, ya que el desprendimiento de la misma, sería tan iluso cómo sugerir un desarme nuclear global, ya que tras descubrirse un determinado factor que de poder a una nación, empresa o persona sobre otras, implica la adquisición de determinado factor, para regular los poderes, aunque exista una diplomacia que medie el trato entre estos.

Paralelamente a esto, aunque es imprescindible el uso de la tecnología, esta es solo la herramienta, para lograr a cabo el espionaje gubernamental, y la solución no se encuentra en la misma. Nos encontramos en una lucha constante de programadores que se encuentran desde las trincheras del espionaje y el anti espionaje, en la cual una toma un paso sobre la otra, para emparejarse al poco tiempo. Qué mejor referencia a esto, puede ser esa icónica fotografía de Mark Zuckerberg, creador de Facebook y reconocido programador, en la cual aparece su laptop con cinta de aislar tapando el orificio del micrófono así como de la webcam [10].

La regulación de poderes es una tendencia natural inevitable de las sociedades, así como lo es el espionaje, un software que lo permita, no debería de sorprendernos, puesto es solo una migración al terreno digital de lo que siempre ha hecho el ser humano. Hablar de ética y espionaje puede sonar contradictorio, sin embargo, a lo largo de la historia, el espionaje se ha utilizado, para facilitar el bien de sus determinadas naciones, y la subsistencia de sus sociedades. En 1987 la humanidad despilfarró cerca de 20 mil millones de dólares en actos de espionaje. Convertido en toda una industria, fue una gran fuente de empleo: en aquel entonces se estimaba que la cantidad de involucrados directa o circunstancialmente en el fisgoneo internacional podría haber ascendido a 1.25 millones de personas [11].

En los últimos veinte años, los requisitos de seguridad de la información en cualquier compañía han evolucionado, el uso generalizado del equipo de procesamiento de datos, la seguridad de la información que se consideraba valiosa para una empresa se proporcionaba principalmente por medios físicos y administrativos [12]. Sin embargo, al emigrar al terreno digital, surge la necesidad de una regulación, puesto la facilidad de realizar espionaje casero y/o laboral, e irrumpir con los derechos humanos de cualquier persona, están al alcance público digital, como se puede hacer al acceder sitios web como http://www.keylogger.org el cual nos brinda hasta 27 opciones de *Spyware*, de diversas compañías especializadas, algunas incluso, con una versión de prueba gratuita. Puesto la incursión de las tecnologías de la información ha facilitado la recolección de información de manera masiva, independientemente del uso dado [13].

Entre los varios retos que tienen el *Big Data* y su crecimiento, podríamos resaltar el hecho de que éste, al igual que la inteligencia artificial, se está desarrollando mucho más rápido de lo que estamos regulando su uso,

estudio y limitaciones. Misma noción a la cual ha hecho referencia el creador de la empresa automotriz Tesla, Elon Musk en diversas ocasiones [14].

En el desarrollo de este artículo enfocado en el caso Pegasus, describiremos los usos de la tecnología del caso para la generación de valor e innovación para el Gobierno a través del análisis del comportamiento e identificaremos los riesgos potenciales de la explotación de los datos recabados, analizando todo esto desde una perspectiva ética.

2. Metodología

Para el desarrollo del presente artículo se utilizó un método de investigación racional analítico-sintético, partiendo de la reconstrucción imparcial de los hechos, desmembrando los componentes del caso, en distintas perspectivas de estudio, dando pie a un análisis inductivo, de lo concreto a lo abstracto, desde los diversos ángulos posibles [15], generando las siguientes secciones:

- Antecedentes del caso.
- Impactos de la *Big Data*.
- Ética Corporativa y *Big Data*.

Para así, con el re ensamblaje conceptual de los componentes y los resultados del análisis de sus perspectivas, siempre apegándose al pensamiento crítico, desarrollar conclusiones sintéticas en torno al caso del “Escándalo Pegasus en los Estados Unidos Mexicanos”.

3. Antecedentes del caso

Es un claro axioma que hay una gran ola de especulación e incluso teorías conspiratorias, respecto a los casos de espionaje gubernamental realizado en México, que recientemente han salido a la luz, en esta investigación abordaremos el caso del programa malicioso de computador Pegasus de NSO Group, identificando a las organizaciones implícitas en el caso describiendo el rol que desempeñaban y el uso que dan de la *Big Data*.

Al hablar del malware Pegasus es imposible no nombrar a la compañía que le dio vida, NSO Group Technologies, una empresa tecnológica israelí, dedicada a la creación de software de intrusión y vigilancia fundada en 2010 por Niv Carmi, Omri Lavie y Shalev Hulio. Qué aunque ellos se presentan como creadores de herramientas para combatir el crimen y el terrorismo, los especialistas en seguridad describen a NSO Group como un "traficante de ciber armas" [16]. Según las pruebas de los *Spyware* desarrollados por NSO Group [17]. Es notable su amplio dominio en el *Big Data*, la programación y la minería de datos. Sin embargo su ética al momento de brindar un software que recopila información de esa forma, es nula, ya que el espionaje de ese tipo es ilegal en la República Mexicana y está claramente explícito en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares [18][19].

Aunque NSO Group es una empresa israelí, su propietario mayoritario es la firma estadounidense de capital privado Francisco Partners. Informes recientes sugieren que Francisco Partners está considerando la venta de NSO Group, con una valuación de $ 1 mil millones. Francisco Partners también posee varias otras compañías que desarrollan y venden tecnología de vigilancia masiva [20].

Otra organización que forma parte de los protagonistas de este caso es Citizen Lab, un laboratorio interdisciplinario basado en la Escuela Munk de Asuntos Globales de la Universidad de Toronto, centrado en la investigación, el desarrollo y la política estratégica de alto nivel y el compromiso legal en la intersección de las tecnologías de información y comunicación, los derechos humanos y la seguridad global. Puesto ellos fueron los que en 2016 se percataron del espionaje que se estaba realizando, utilizando un enfoque de "métodos mixtos" para la investigación, combinando métodos de ciencias políticas, leyes, ciencias de la computación y estudios de área. Su investigación incluye: la investigación del espionaje digital contra la sociedad civil, la documentación del

filtrado de Internet y otras tecnologías y prácticas que afectan la libertad de expresión en línea, el análisis de la privacidad, la seguridad y los controles de información de las aplicaciones populares y el examen de transparencia y mecanismos de rendición de cuentas y agencias estatales con respecto a datos personales y otras actividades de vigilancia [21].

Por último, se tiene como presunto culpable de este espionaje injustificado a diversas figuras de la sociedad mexicana (Véase Tabla 1), el gobierno mexicano, que según diversas pruebas ya presentadas por Citizen Lab y la opinión de expertos, como lo es Edward Snowden, ex analista agencias de inteligencia estadunidenses, mismo que comentó:

"El gobierno mexicano, que estoy bastante seguro que está en esto, no lo está admitiendo, de hecho el presidente de México lo negó, pero al mismo tiempo ordenó una investigación, pero cuando nos damos cuenta que todos estos periodistas han sido un blanco y no sólo son periodistas, es el jefe del Senado, activistas políticos, luego vemos el tipo de mensaje que se está utilizando para conseguir que ellos den clic en esos links, una cosa que cualquiera haría y echarían a andar el malware y eso es bastante común con un sistema sofisticado. Yo trabajé profesionalmente en la Agencia de Seguridad Nacional organizando este tipo de operaciones en términos de contraataque, mi trabajo era observar personas que estaban haciendo esto desde el ejército chino hacia objetivos estadunidenses. Yo reconozco el agrupamiento de objetivos, reconozco la similitud de sistemas y de infraestructura que se están utilizando".

Tabla 1. Objetivos de intentos de infección reportados entre el 1 de enero y el 1 de julio del año 2017 [20].

Nombre	Área	Organización	Puesto
Carmen Aristegui	Medios de Comunicación	Aristegui Noticias	Reportera
Emilio Aristegui	Medios de Comunicación	Aristegui Noticias	Hijo de Carmen
Rafael Cabrera	Medios de Comunicación	Aristegui Noticias	Reportero
Sebastián Barragán	Medios de Comunicación	Aristegui Noticias	Reportero
Carlos Loret de Mola	Medios de Comunicación	Televisa	Reportero
Daniel Lizárraga	Medios de Comunicación	Mexicanos contra la corrupción y la impunidad	Reportero
Salvador Camarena	Medios de Comunicación	Mexicanos contra la corrupción y la impunidad	Reportero
Mario Patrón	Derechos Humanos y Anticorrupción	Centro Miguel Agustín Pro Juárez	Director
Stephanie Brewer	Derechos Humanos y Anticorrupción	Centro Miguel Agustín Pro Juárez	Empleada
Santiago Aguirre	Derechos Humanos y Anticorrupción	Centro Miguel Agustín Pro Juárez	Empleado
Juan Pardinas	Derechos Humanos y Anticorrupción	Instituto Mexicano para la Competitividad	Director
Alexandra Zapata	Derechos Humanos y Anticorrupción	Instituto Mexicano para	Empleada

Alejandro Calvillo	Salud Pública	la Competitividad El Poder del Consumidor	Director
Luis Encarnación	Salud Pública	Coalición Contra PESO	Coordinador
Dr. Simón Barquera	Salud Pública	Instituto Nacional de Salud Pública	Científico
Sen. Roberto Gil Zwarth	Gobierno	Senado de la Republica	Senador
Ricardo Anaya Cortés	Gobierno	Partido Acción Nacional (PAN)	Presidente del Partido
Fernando Rodríguez Doval	Gobierno	Partido Acción Nacional (PAN)	Secretario de comunicaciones del partido
GIEI Investigation	Investigaciones Internacionales	Grupo Interdisciplinario de Expertos Independientes (GIEI)	Información del 2014 en torno a las desapariciones masivas de Iguala

Todas esas pruebas apuntan y se agrupan para señalar que el gobierno mexicano es responsable de esto y esto no es algo que únicamente esté diciendo Edward Snowden. Diversos medios de publicidad que escribieron el reportaje no quisieron ir más allá, autocensurándose [22], pero tanto ellos, como diversos investigadores, concuerdan en acuñar esa responsiva al gobierno federal [23] [24].

4. Impactos de la *Big Data*

Si se da seguimiento a las recomendaciones de la Fundación del Español Urgente (Fundéu BBVA), la *Big Data* es sin la menor duda, uno de los campos más importantes de trabajo para los profesionales de las TIC. No hay área ni sector que no esté afectado por las implicaciones que este concepto está incorporando; cambian algunas herramientas, se modifican estrategias de análisis y patrones de medida [25].

Al darle una correcta recolección, estratificación, interpretación, desarrollo y análisis a los metadatos, bajo la dirección de un objetivo previo planteado, se obtiene un valor agregado, mismo que no precisamente sea el buscado en el objetivo inicial, puesto dentro de ese cúmulo enorme de información, incluso después de filtrarla y quedarnos con los datos de valor para la empresa, institución o gobierno (según sea el caso), podemos sorprendernos y obtener un valor agregado de esa información que no estaba previsto. Haciendo alusión a todo esto, en este capítulo, está plasmado el impacto y uso del *Big Data* en el caso Pegasus, para así dar continuación a los antecedentes previamente presentados.

El alcance del *Spyware* Pegasus, elaborado por la empresa NSO, aunque su función y propagación es mediante móviles individualmente, es amplio ya que es capaz de burlar la seguridad de los usuarios de Android y de iOS, pese a que los equipos de Apple se consideran como unos de los más seguros del mercado [26] [27].

Sin embargo su método de propagación le brinda un alcance limitado, puesto aunque los emisores de Pegasus hayan seleccionado a sus víctimas, el *Spyware* solo se propagará en los móviles de las víctimas que caigan en la trampa al no conocer su sencillo procedimiento de instalación, el cual es el siguiente:

- Cuando una persona es atacada con Pegasus, recibe un mensaje SMS en su teléfono, el cual contiene un texto que busca persuadirlo de hacer clic en un enlace infeccioso, haciéndose pasar por una noticia, un aviso o el mensaje de un familiar o amigo. (Véase Figura 1).
- Para que el objetivo haga clic en el enlace, el atacante debe asegurarse de engañar al objetivo. En la infraestructura de NSO Group, los dominios que pertenecen a ésta buscan suplantar a otros sitios legítimos como medios de comunicación, servicios de telecomunicaciones, redes sociales, portales de gobierno, organizaciones humanitarias o aerolíneas, entre otros.
- Si la persona hace clic en el enlace, su móvil recibe inadvertidamente el software malicioso conocido como Pegasus [28].

De acuerdo con Lookout, el malware Pegasus también se puede configurar para rastrear algunos elementos de forma periódica y envíe la información de forma automática cada cierto tiempo. Cabe destacar que toda la información viaja con un fuerte cifrado que hace que sea imposible detectar al espía y de capturar la información mientras viaja [29].

Figura 1. Intentos de infección enviados a un teléfono perteneciente a la investigación GIEI cuando los investigadores estaban preparando su informe final [20].

El *Spyware* recopila información almacenada y es capaz monitorear de forma constante la actividad que se realiza en el dispositivo. De acuerdo con la empresa de seguridad *Kaspersky*, Pegasus es un *malware* modular, ya que instala los módulos necesarios para leer los mensajes del usuario y el correo, escuchar las llamadas, realizar capturas de pantalla, registrar las teclas pulsadas, acceder al historial del navegador, a los contacto, recibir video en directo de aplicaciones como *Facetime* y *Skype*, tener acceso a correos electrónicos incluso con sus datos adjuntos, activar cámaras y micrófonos y vaciar toda la información contenida en el dispositivo. Lo que lo hace capaz de espiar todos los aspectos de la vida del dueño a partir de su smartphone. Pegasus podría incluso escuchar audios codificados y leer mensajes cifrados, gracias a su keylogging y sus capacidades de grabación de audio, las cuales roban los mensajes antes de que estos se cifren.

Como podemos darnos cuenta, todos estos usuarios en dado caso de ser infectados generan una cantidad de datos sorprendente, y sin darse cuenta, qué al ser organizados como se hizo con el caso público de Malte Spitz [30], se puede generar un mapa interactivo, que se está alimentando en tiempo real, en el cual se puede tener un impacto altamente negativo, o positivo, según sea la perspectiva, puesto en un terrorista, ayudaría al gobierno

emisor de Pegasus, a descubrir una red de terrorismo, mediante una célula infiltrada, y ese mismo impacto, negativamente, es el caso tal como sucedió, espiando activistas, periodistas y demás personas ilustres que fueron espiados sin razón justificable aparente. Sin embargo sin importar el objetivo, este *Spyware* tiene un impacto social negativo, puesto irrumpe la privacidad de los seres humanos sin su autorización.

De acuerdo a lo anteriormente mencionado, el uso de la tecnología, para crear un valor agregado e innovación en el Gobierno Mexicano y el uso que este dio al software Pegasus, tomando en cuenta que los personajes ilustres que fueron motivo de espionaje, fueron espiados injustamente o no, fue extremadamente amplio y de posibilidades muy variadas. Ya que al tener acceso completo a un teléfono inteligente del vigilado, se pueden conseguir los siguientes ejemplos de valor agregado, al procesar y analizar la información obtenida:

- Mapas Geográficos Digitales del Usuario, mostrando sus rutas frecuentes, y sus posibles futuras rutas, tras elaborar un horario estimado, del sujeto investigado.
- Elaboración de un Cronograma Diario de Actividades, con la posibilidad de predecir eventos futuros, mediante la calendarización, y tendencias expuestas.
- Conocer información confidencial del usuario que haya pasado en algún momento por su correo electrónico, e incluso tener acceso a cuentas bancarias.
- Captura de imágenes, video o audio del entorno, o del usuario mismo, en el momento que se deseé.
- Conocer los contactos cercanos al usuario, y la información que este les envía.
- Posibilidad de corromper la privacidad de los contactos del usuario al conocer la información que estos mandan, creyendo que se encuentran en una línea de comunicación bidireccional.

Este último punto, es de extrema importancia, puesto la limitante tecnológica de Pegasus, no está enclaustrada en el usuario espiado, puesto al corromper su teléfono inteligente, se tiene un acceso parcial a la privacidad de los contactos que tenga el usuario. Y si el *Spyware* Pegasus, se coloca en las células correctas, pertenecientes al mismo sistema de comunicación, al compaginar la información de los usuarios vigilados, se puede obtener información relevante de todo el sistema de comunicación al cual pertenecen [31].

Identificando los riesgos potenciales de la explotación de la información recabada por Pegasus y tomando en cuenta que aunque la violación a la privacidad de todos los personajes ilustres vigilados debe ser igualmente justificada, estos, al tener diferentes profesiones, o cargos en la sociedad, son portadores de información correspondiente a distintas disciplinas, con valor y área de impacto diferente, por lo tanto se deducen diferentes posibilidades, tomando en cuenta los personajes espiados presentados en la Tabla 1.

El espionaje a publicistas, puede revelar las fuentes privadas, o infiltradas que estos tengan para tener conocimientos o sucesos previos, a revelar y/o elaborar una nota. Además de que al tener conocimiento, de lo que los publicistas saben y de su constante ubicación, permite tener consciencia del contenido que se publica y publicará por sus respectivos medios.

El espionaje ejercido sobre abogados, permite saber los recursos que estos utilizaran jurídicamente, y cuáles serán sus estrategias en sus determinados proyectos que tengan a cabo, conocer testigos o pruebas antes de que sean presentadas e ir siempre delante de ellos.

Al vigilar a los funcionarios de salud pública, precisamente los promotores del impuesto al refresco, se tiene consciencia de los recursos que estos utilizarán, como lo son investigaciones, estadísticas y demás pruebas científicas que prueban los daños en la salud ocasionados por el consumo de refresco, incluso antes de ser presentados para facilitar la legislación que les favorezca.

El espionaje de ciertas figuras políticas, permite conocer información privada de determinado partido de oposición, su postora ante determinadas situaciones, futuros contendientes políticos e incluso plagiar proyectos políticos, para presentarlos con anticipación a su autor. La vigilancia de las figuras representantes del Instituto Mexicano para la Competitividad, puede hacer fracasar, el proyecto anticorrupción presentado, puesto se puede entorpecer, la comunicación y el desarrollo del mismo.

Los investigadores internacionales, miembros del GIEI que investigaban la desaparición de los 43 estudiantes de Ayotzinapa, al ser investigados, se puede tener acceso a información relevante al caso, que sea de interés del gobierno mexicano, debido a la importancia misma de este suceso. Además de poder tener ese impacto, en sus respectivas áreas, por mencionar solo algunos ejemplos, la vigilancia, de esas personas a ese grado, puede facilitar atentar contra su vida, y la de otras personas, además de poder extorsionar a los usuarios vigilados, al tener acceso a tanta información de ellos y su entorno.

Otra parte del impacto económico y político del software Pegasus, es la reacción de las empresas privadas, y demás personajes considerados posibles futuras víctimas, al prevenir su infección con este software. Sin mencionar que Apple y Google, han reforzado sus sistemas operativos IOS y Android, respectivamente para eliminar y prevenir ante semejante amenaza.

El impacto del *Big Data* a través del software Pegasus irrumpe completamente la privacidad de las personas, violentando sus derechos humanos y generando grades sumas de bytes de información al día por cada una de ellas, teniendo un espionaje certero que al ser perfeccionado, por un *Spyware* inadvertido, (puesto esa es la única limitación en el alcance a sus víctimas de Pegasus) cambiaría al mundo tal y como lo conocemos. Propiciando una guerra de datos y *Spyware*s entre particulares y naciones, que orilla a reflexionar sobre la privacidad de los usuarios y las medidas a tomar [32].

Es necesario el desarrollo de la ciencia de datos en México, puesto en este acontecimiento, aunque el software entro maliciosamente a periodistas y activistas con un mensaje trampa, ningún mexicano se percató de ello, hasta después de hacerse pública la noticia por Citizen Lab, en Toronto Canadá.

5. Ética corporativa y *Big Data*

Existen distintos tipos de ética, como lo pueden ser la normativa, la cual es una parte de la ética que intenta formular principios generales que justifiquen los sistemas normativos; argumenta por qué se deberían adoptar determinadas normas [33]. O la ética pragmática la cual considera que los juicios morales no deberían basarse en la acción que se realiza, sino en los resultados de esa acción [34]. La ética informática se ha estudiado durante décadas, centrándose primordialmente en el impacto que las tecnologías de la información tienen sobre las diversas sociedades [35], sin embargo, hay que hacer un énfasis, en que la tecnología es el medio, pero la regulación y protección es hacia las personas que conformamos la sociedad [36].

La visión actual de la Responsabilidad Social Empresarial, dice que la actuación de la empresa contemporánea no se puede evaluar sólo en unidades monetarias, sino que debe expresar su valor por medio de una triple dimensión: económica, social y medio ambiental [37]. Esta visión refleja ya un alcance más allá de la única tarea económica que privó durante casi dos siglos desde que se perfilaron las unidades productivas gracias al uso intensivo de la nueva oferta energética (vapor, electricidad,…) y al uso muchas veces deshumanizado de la "mano de obra".

De igual forma, los sistemas normativos de conducta, por los cuales se rigen los empleados de las empresas que hacen uso de la ciencia de datos, y los metadatos, son parte del pilar ético que rige el óptimo desarrollo del *Big Data* en el mundo, puesto de esta ética corporativa nacen los objetivos y limitaciones que se dan al *Big Data*, antes de ser sancionados o regulados por la Ley de algún gobierno.

NSO Group Technologies, empresa que le dio vida al *Spyware* Pegasus, es un enigma financiero, organizacional, tecnológico y ético, del cual el mundo, lentamente y mediante diversas investigaciones, ha obtenido algo de información de las distintas áreas de la empresa, su funcionamiento, objetivos y visión. Hablando de ética y sus sistemas normativos de conducta, la Red en Defensa de los Derechos Digitales (R3D) al momento de subir un artículo digital haciendo alusión a la presión efectuada sobre Blackstone Group, para disuadir las intenciones que tiene dicho grupo en invertir en NSO Group Technologies, podemos darnos cuenta de lo siguiente:

- Existe una falta de rendición de cuentas de NSO Group respecto al uso de sus productos y servicios de forma ilegal e ilegítima en México.
- El mal uso de estas herramientas de vigilancia por parte de los clientes de la firma NSO Group han motivado el llamado de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, así como de cuatro expertos de la Organización de las Naciones Unidas y entre otros, para que se inicie una investigación independiente e imparcial en torno a estos abusos.
- También Citizen Lab de la Universidad de Toronto, exhortamos a Blackstone Group L.P. a considerar las implicaciones éticas y de derechos humanos que tiene invertir en dicha empresa.
- NSO Group solamente ha emitido un escueto mensaje sobre el tema, en el que reafirma que sus productos son comercializados únicamente a gobiernos y se declaran "horrorizados por el supuesto mal uso de nuestro producto" y que cualquier uso de este tipo "sería una violación a nuestras políticas de ética de negocios, contratos legales y a lo que defendemos como compañía" [38].

De lo cual podemos deducir lo siguiente: Aunque NSO Group afirma tener "políticas de ética de negocios" sus acciones y reacciones respecto al caso Pegasus en México demuestran alguno o varios de los posibles escenarios:

- El sistema Normativo de conducta de NSO Group es nulo, y sus declaraciones solo son mentiras para cubrir la imagen corporativa de la empresa.
- NSO Group cuenta con algún sistema normativo de conducta, pero hacen caso omiso de éste desde el momento de fijar los objetivos del producto.
- El Sistema Normativo de Conducta de NSO Group, persigue ideales diferentes de los que conocemos en la Moral Global como "Buenos" siguiendo una filosofía extremista, en la cual estén conscientes de lo que estén haciendo pero lo consideren justificable para alcanzar un fin, o sencillamente desde su perspectiva previamente establecida en sistema normativo de conducta, no está mal su forma de actuar.

En cualquiera de estos posibles escenarios o en su combinación parcial o total, NSO Group está violando el derecho humano de la privacidad y necesita un sistema normativo de conducta bien establecido y regulado.

Por su contraparte se encuentra el gobierno mexicano, del cual podemos decir que obviamente se encuentra regulado por sus propias leyes, y más allá de la pregunta anteriormente expuesta, el gobierno hizo mal uso de este *Spyware* al investigar íconos de la sociedad, que más que figurar como presuntos terroristas, es un claro axioma que su seguimiento y espionaje fue para satisfacer fines particulares de ciertas piezas dentro del gobierno. Lo cual hace deducible para la prensa, un decadente sistema normativo de conducta, el cual hace facil especular una red de corrupción dentro del Gobierno mexicano y un mal uso de estas herramientas de seguridad nacional [39].

Cómo bien expresó Carmen Aristegui "La filtración de documentos sobre la adquisición de Pegasus por la PGR confirma la necesidad de que se incorpore un Panel Independiente a la investigación" [40], ya qué es imposible que la Procuraduría General de la República sea, juez y parte en el caso Pegasus, al ella ser la que dispuso del *Spyware* inapropiadamente.

Si bien el Gobierno mexicano se encuentra saturado de leyes que teóricamente rigen el comportamiento de nuestros servidores públicos, y por su cargo gubernamental, podríamos suponer son miembros de la sociedad con un elevado sentido de la ética. Casos como Pegasus, podrían dar a entender, qué al menos algunos elementos dentro de los distintos niveles de gobierno, son células de una red de corrupción que persigue intereses personales, sobre la moral y la ley. Puesto además de comprar el *Spyware* y dar mal uso de éste, la denuncia o advertencia de la violación a la privacidad inadecuadamente no provino de ninguna dependencia del gobierno mexicano, sino como ya se ha mencionado, vino de Citizen Lab, en Toronto, Canada. Sin embargo, al ser esta una investigación científica y de un carácter neutro, no descarta la posibilidad de que estos personajes ilustres investigados por el gobierno mexicano mediante el *Spyware* Pegasus correspondan a una investigación de seguridad nacional, y por este mismo motivo el gobierno no ha aclarado el panorama al respecto.

La tercera parte implicada, Citizen Lab, laboratorio de investigación de la Universidad de Toronto, Canada. Tiene su sistema normativo de conducta, establecido bajo distintos trazados de acceso público en la página Web, mostrando un muy estructurado sistema, para docentes, administrativos y alumnos de la Institución. Siendo un ejemplo de un óptimo sistema normativo de conducta, puesto si analizamos el Código de Conducta de los estudiantes, en el apartado "C. Procedimientos", en el inciso "1. General", se encuentra el proceso que en teoría siguió Citizen Lab, tras encontrar los primeros hallazgos del *Spyware* Pegasus en México. Decisión muy acertada al tratarse de algo de esta magnitud. Puesto el sistema normativo de conducta, regula la ética de los miembros de la institución [41].

Tomando en cuenta que la ética normativa reflexiona sobre lo que es moralmente correcto y por qué, formulando principios, reglas y juicios, para argumentar acerca de lo que es bueno y correcto, justificando lo que es bueno y correcto. Y haciendo distinción entre distintas teorías normativas que se diferencian porque en cada caso derivan valores morales de deberes o de derechos. Según la teoría de los deberes, existe un conjunto deberes que el ser humano debe adquirir por naturaleza. "Esos deberes pueden ser deberes hacia Dios (honrarlo, servirlo y rezarle), hacia uno mismo (preservar la vida, buscar la felicidad y desarrollar talentos) y hacia otros. En este último caso se pueden distinguir deberes familiares (honrar a los padres y cuidar al cónyuge y a los hijos), deberes sociales (no dañar a otras personas, cumplir las promesas y ser benevolente) y deberes políticos (obedecer las leyes y tener espíritu cívico)" [42].

Por lo tanto, bajo una perspectiva ética normativa la empresa NSO Group, no cumple con deberes políticos ni sociales, ya que aunque no se ha especificado sobre la presencia de un sistema normativa de conducta, o algún sistema de regulación moral de NSO Group, y las suposiciones de prensa, o globales, dan a suponer la ausencia de este. No se puede descartar la opción de qué NSO Group obedezca deberes adquiridos naturalmente, qué se apeguen a una creencia religiosa y procuren su subsistencia sobre la de los demás.

El Gobierno Mexicano bajo esta misma perspectiva, a pesar de existir una disyuntiva entre la obviedad de una alta corrupción dentro del gobierno mexicano así como su nula presencia de ética normativa y la posibilidad de que estos personajes ilustres investigados por el gobierno mexicano mediante el *Spyware* Pegasus correspondan a una investigación de seguridad nacional, y por este mismo motivo el gobierno no ha aclarado el panorama al respecto. Es un hecho que no se están cumpliendo con los deberes políticos de una manera óptima, puesto existen huecos en el marco jurídico, entre la violación de la privacidad y el ciber-espionaje por un bien común. Y por consecuente no podemos proclamarnos como un "Estado de Derecho", concepto político utilizado para nombrar al Estado ideal de cualquier nación porque todos los poderes que conforman el estado se encuentran a derecho, es decir sometidos a la autoridad de las leyes vigentes.

Citizen Lab, a pesar de contar con un evidente sistema normativo de conducta, expuesto por la Universidad de Toronto, y ser los reveladores del caso Pegasus, y del espionaje de cada uno de los iconos mexicanos que estaban siendo espiados por el gobierno, analizando distinto material presentado, como los inicios, su forma de operar, y su transición de rebeldes a policías informáticos, como ellos mismos se han hecho llamar [43]. Hay que mencionar qué aunque han cumplido con sus deberes sociales formidablemente, han pasado por alto sus deberes políticos. Puesto aunque no han especificado su método de operación, al ver sus declaraciones y los resultados detallados que han reportado es un claro axioma que el acceso a semejante información, ha sido traspasando diversas barreras de privacidad, empezando por la empresa NSO Group, y al no existir leyes específicas que regulen este uso de *Big Data*, podemos manifestar que las acciones que ha realizado Citizen Lab, son contraespionaje industrial y posiblemente, también hayan violado parcialmente la privacidad de los elementos espiados por NSO Group, para poder verificar si eran víctimas del Software Pegasus.

Al hablar de implicaciones éticas pragmáticas, y bajo el principio qué el fin justifica los medios, podemos resumir que NSO Group, persigue intereses particulares económicos, y busca el crecimiento y desarrollo de la empresa, así como muchas otras empresas, venden productos perjudiciales para la salud, o la humanidad misma. Pero bajo el argumento de ser fuente de empleos, y propiciar un crecimiento económico, pueden tener un respaldo ético, desde su perspectiva pragmática, cerrada e irracional.

El Gobierno Mexicano, por su parte, en caso de que los personajes ilustres investigados mediante el *Spyware* Pegasus correspondan a una investigación de seguridad nacional, y por este mismo motivo el gobierno no ha aclarado el panorama al respecto. Sería un claro ejemplo de ética pragmática, puesto aunque el medio es el espionaje de unos, violando su privacidad, el fin que es la Seguridad Nacional, justificaría ese procedimiento.

Citizen Lab, al entrar bajo el rol de contraespionaje, debe manejarse mediante una ética pragmática, que les permita moralmente, acceder a cualquier información, con tal de informar sobre espionaje a gobiernos, y propiciar el bien común.

Por su parte, la Responsabilidad Social es notoriamente nula en NSO Group, contrario a Citizen Lab, puesto la responsabilidad social, es la base ética de su existir, y como un punto medio tenemos la postura del gobierno mexicano, qué al no haberse aclarado su situación, aunque la mayoría de suposiciones apunta a una amplia cadena de corrupción dentro del sistema de gobierno, que persigue intereses particulares, aun no se descarta la posibilidad de que los elementos espiados, sean objeto de estudio para un bien común.

Un aspecto fundamental al implementar un sistema normativo de conducta de una organización, depende de la región geográfica y del personal de la organización, puesto algunas de las definiciones de Moral hacen una referencia clave a costumbres y comunidad y esto es muy diverso en todo el mundo.

Gracias a la Globalización y el rumbo lento, pero seguro de una humanidad más culta nuestra Moral (aunque tiene diversas excepciones) en lo fundamental se apega y converge en un estándar de "bien y mal". Pero al existir diferencias culturales, un sistema normativo de conducta, varía en su presentación o existencia para alcanzar resultados óptimos en la organización y Sociedad.

Por ejemplo, es un axioma de fama mundial el elevado comportamiento cívico y la disciplina de los japoneses, además de ser admirable y objeto de estudio la ética empresarial de empresas originarias en tierras Niponas. No podemos hablar del modelo empresarial japonés sin hacer referencia a Konosuke Matsushita, fundador de Matsushita Electric Industrial Company, que estableció siete principios con el objetivo de lograr no solo la prosperidad de su empresa sino también del conjunto de la sociedad:

- Contribución a la sociedad.
- Imparcialidad y honradez.
- Cooperación y espíritu de equipo.
- Esfuerzo para la mejora.
- Cortesía y humildad.
- Adaptación y asimilación.
- Gratitud

Estos principios, a día de hoy, actúan como principios rectores en las grandes empresas japonesas y constituyen la base de la cultura empresarial japonesa. Si bien son admirables los resultados a través de los años con el desarrollo de estos principios, estos son muy genéricos y no corresponden a un sistema normativo de conducta como tal, pero en la cultura del sol naciente, han sido suficientes para qué de la mano del sintoísmo y budismo hayan formado, el modelo de sociedad que es ahora.

6. Conclusiones

Esta Casos como el de Pegasus, nos hacen pensar en las mentes académicamente brillantes qué se encuentran detrás de toda esa programación informática y Administración empresarial. Haciendo referencia a esto, me es imposible no mencionar el caso Enron, a partir del cual se empezó a cuestionar la ética de los MBA y encontrar una relación inversa entre Conocimientos y Ética, siendo un parteaguas, para las Universidades de prestigio alrededor del mundo, para implementar sistemas de enseñanza, que en realidad mostrarán la importancia de la ética en la sociedad y negocios, puesto en diversos estudios se comprobó que los estudiantes de estas prestigiosas

universidades, veían a la ética solo como una materia, perseguían únicamente intereses económicos y un alto porcentaje, dependiendo el estudió, confesó robaría si tuviera la oportunidad y el riesgo fuera poco [44] [45] [46] [47].

La estructura de toda organización, son las personas que la manejan, y hasta que estos directivos y piezas clave, entiendan que apoyar a la sociedad es apoyarse a ellos mismos, lograremos un desarrollo económico, y no solo un crecimiento.

El impacto del *Big Data* a través del software Pegasus irrumpe completamente la privacidad de las personas, violentando sus derechos humanos y generando grandes sumas de bytes de información al día por cada sujeto investigado, particularmente al caso Pegasus, no se puede realizar un juicio ético respecto a la posición del gobierno mexicano, puesto aunque los medios y el razonamiento cotidiano, podría hacernos pensar que se está dando un mal uso del software, al aun no estar aclarado el panorama, no tenemos la certeza, de que la investigación de estos personajes ilustres sea por seguridad nacional.

Tomando siempre en cuenta que el factor clave a relucir en este caso, más allá de la participación del Citizen Lab, del Gobierno Mexicano y de NSO Group, es la falta de regulación en materia de *Big Data*, puesto si ya hubiera alguna regulación específica respecto a las condiciones para irrumpir la privacidad con el fin de garantizar la seguridad nacional, o al uso de ciber-espionaje de parte de los gobiernos, la polémica desarrollada al cabo de estos últimos meses, habría tenido una resolución legal. Puesto el prolongamiento de estas regulaciones, nos harán llevar estas hipótesis de impacto, a su comprobación, misma que sin importar la gravedad, será negativa si carece de regulación.

Es evidente el interés del Gobierno Mexicano en el *Big Data*, y la expectativa de poder, control y seguridad que este puede tener en una organización, recopilando enormes cúmulos de información, para después procesarla, e incluso realizar predicciones mediante el uso de algoritmos, sin embargo el medio de recolección de toda esta información, infringe la privacidad de sus ciudadanos, y los ciudadanos que se eligieron para ser sujetos de estudio o espionaje, son una muestra qué refleja el mal uso del software, para supuestos intereses particulares, a través de la manipulación de datos personales, mismos a los cuales debemos dar una definición clara, para no caer en percepciones subjetivas, y ya qué no existe una definición en la RAE, podemos inclinarnos por la definición presentada en el marco jurídico mexicano.

Citando al Estudio Teórico Conceptual, de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia, y sin adentrarme totalmente en su contendido. Según Oscar R. Puccinelli, no todos los datos de carácter personal cuentan con la misma estrictez en la tutela y se diferencian en: a) los datos que son de libre circulación, como los de identificación: nombre, apellido, documento de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; b) los de circulación restringida a un sector o actividad determinada, que son susceptibles de tratamiento en tanto se presente una causa de justificación legítima y con las limitaciones que resulten de esa especialidad; y

c) los de recolección prohibida, porque afectan la intimidad personal o familiar, que son los denominados datos sensibles [48].

Haciendo referencia a la Ley de Protección de Datos de Carácter Personal o LOPD, es necesario se haga caso oportuno al principio de minimización, que establece que sólo deben guardarse aquellos datos personales que sean necesarios para conseguir objetivos legítimos y especificados. Otro principio importante para proteger la privacidad, también recogido en la LOPD, es el de "información y consentimiento" según el cual debe explicarse a los individuos qué uso se dará a la información que se recoja sobre ellos y éstos, a su vez, deben poder decidir si quieren o no que se recojan sus datos [49].

Además, haciendo referencia a la acción jurisdiccional Habeas Data [50], es necesario que los individuos tengan acceso a los datos que se recogen sobre ellos, como lo propone el Estudio Teórico Conceptual, de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia y el proyecto "midata" del gobierno de Reino Unido [51], cuyos objetivos son, por un lado, conseguir que las empresas proporcionen a

los consumidores acceso electrónico y seguro a los datos personales que han recogido sobre ellos y, por otro, animar a las empresas a desarrollar aplicaciones que ayuden a los consumidores a usar sus datos de forma efectiva.

Necesitamos un gobierno Integro, preparado y que marche jurídicamente a la vanguardia de la tecnología, para poder regular sus diversas implicaciones. Teniendo en cuenta, que además de la constante actualización que abarque y regule las nuevas tecnologías, la clave se encuentra en respetar dicho sistema jurídico, puesto no puede existir una perspectiva de Liderazgo, si el gobierno mismo hace caso omiso a las leyes con las cuales busca regular a la sociedad. Logrando así nuestro anhelado y malamente ya publicitado "Estado de Derecho"

Paralelamente a esta supuesta falta de ética del gobierno mexicano, podríamos analizar la postura de NSO Group, afirmando que ellos venden un malware desarrollado para el espionaje de presuntos terroristas, y apoyar a reforzar la seguridad nacional, por lo tanto no se hacen responsables del mal uso de este. Pero la ONU subrayó que estos hechos constituyen una injerencia arbitraria en la vida personal, prohibidas por el derecho internacional [52].

Espiar a presuntos terroristas, infringiendo sus derechos humanos, puede o no ser considerado un acto ético, al hacerse con el fin de garantizar la seguridad nacional. Como ciudadanos de un mundo en el cual cada día se vacía más información en medios digitales, debemos estar pendientes de la regulación de nuestra privacidad.

7. Referencias

[1] Rossell, D. (2014). Macrodatos y estadística: la perspectiva de un estadístico. *Mètode: Revista de difusión de la Investigación*, (83), 50-57.

[2] IT Gartner Glossary. (2001). *Big Data*. Recuperado de: https://www.gartner.com/it-glossary/big-data/

[3] Zamora Estrada, C., Vargas-Hernández, J. G. (2018). Percepción ciudadana del open data y la innovación en México. *Revista de Investigación en Tecnologías de la Informació*n, 6 (11), 86-95.

[4] De Mauro, A., Greco, M., Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. *Library Review*, 65 (3), 122-135. doi: 10.1108/lr-06-2015-0061

[5] Camargo-Vega J. J., Camargo-Ortega J. F., Joyanes-Aguilar, L. (2015). Conociendo Big Data. *Revista Facultad de Ingeniería*, 24 (38), 63-77. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292015000100006&lng=en&tlng=es

[6] Lohr, S. (2012). *Opinion | Big Data's Impact in the World*. Recuperado de: http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?mcubz=3

[7] Rivera-Flores K. Y., Garrafa-Torres O. M., Sifuentes-Ocegueda E. L. (2018) La gestión de información, estrategia clave en la enseñanza de la investigación. *Revista de Investigación en Tecnologías de la Información*, 6 (12), 21-27.

[8] Himanen, P. (2002). *La ética del hacker y el espíritu de la era de la información*. Recuperado de: http://eprints.rclis.org/12851/1/pekka.pdf

[9] Batista Díaz, C. M., Lujo Aliaga, Z., Cedeño Galindo, L. V., Pérez Céspedes, A., Pantaleón Fernández, R. E. (2018). Propuesta e implementación de la arquitectura de la red LAN en la empresa Acinox Las Tunas. *Revista de Investigación en Tecnologías de la Información*, 6 (11), 1-6.

[10] ABC Tecnología. (2017*). ¿Por qué Mark Zuckerberg tapa la webcam de su ordenador?*. Recuperado de: http://www.abc.es/tecnologia/redes/abci-mark-zuckerberg-tapa-webcam-ordenador-201606221255_noticia.html

[11] Weinstock, V. (2009). *La Ética del Espionaje. Emeequis*. Recuperado de: http://www.m-x.com.mx/xml/pdf/187/64.pdf

[12] Tripp-Barba, C., Aguilar Calderón, J. A., Zurita Cruz, C. E. (2018). Esquemas de fingerprinting como protección de los derechos de autor. *Revista de Investigación en Tecnologías de la Información,* 6 (11), 7-12.

[13] Díaz Rosabal, E. M., Díaz Vidal, J. M., Gogoso Vázquez, A. E., Sánchez Martínez, Y., Riverón Rodríguez, G., Santiesteban Reyes, D. C. (2018). Presencia de las TIC en las investigaciones sociales. *Revista de Investigación en Tecnologías de la Información*, 6 (11), 19-24.

[14]El Mundo. (2017). *Elon Musk: "Hay que regular la inteligencia artificial antes de que se convierta en un peligro"*. Recuperado de: http://www.elmundo.es/tecnologia/2017/07/18/596dc3acca4741ea3b8b45a0.html
[15]Rodríguez Jiménez, A., Pérez Jacinto, A. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela De Administración De Negocios*, (82), 175-195. doi: https://doi.org/10.21158/01208160.n82.2017.1647
[16]BBC Mundo. (2017). *NSO Group, la misteriosa empresa capaz de hackear iPhones con un sólo clic que ha operado en Panamá y México - BBC Mundo*. Recuperado de: http://www.bbc.com/mundo/noticias-37197250
[17]El Economista (2017). *Sospechan mayor espionaje del gobierno mexicano*. Recuperado de: http://eleconomista.com.mx/sociedad/2017/02/13/sospechan-mayor-espionaje-gobierno-mexicano
[18]Proceso (2017a). *Espionaje y paranoia de un gobierno en desgracia*. Recuperado de: http://www.proceso.com.mx/491803/espionaje-paranoia-gobierno-en-desgracia
[19]Proceso (2017b). *La PGR compró a prestanombres el malware espía Pegasus*. Recuperado de: http://www.proceso.com.mx/496696/la-pgr-compro-a-prestanombres-malware-espia-Pegasus
[20]Scott-Railton, J., Marczak, B., Razzak, B., Crete-Nishihata, M., Deibert, R. (2017). *Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware - The Citizen Lab*. Recuperado de: https://citizenlab.ca/2017/07/mexico-disappearances-nso/
[21]Citizen Lab. (2017). *The Citizen Lab*. Recuperado de: https://citizenlab.ca/about/
[22]Hincapié, S., López, J. (2018). Violencia contra periodistas y rendición social de cuentas: el caso mexicano. *Ciencia Política*, 13 (26), 127-152. doi: https://doi.org/10.15446/cp.v13n26.70224
[23]Godoy, E., Tourliere, M. (2017). *En el caso Pegasus, el gobierno mexicano es responsable: Edward Snowden.* Proceso. Recuperado de: http://www.proceso.com.mx/499488/en-caso-Pegasus-gobierno-mexicano-responsable-edward-snowden
[24]Bonifaz, R., Delgado-Ron, A. (2018). Casos verificados de uso ilegítimo de software de vigilancia por parte de gobiernos de América Latina 2015-2016. *Revista PUCE*, (106), 315-333.
[25]Tascón, M. (2013). Introducción: Big Data. Pasado, presente y futuro. *Telos: Cuadernos de Comunicación e Innovación*, (95), 47-50.
[26]El Universal. (2017a). *Así funciona Pegasus, el Spyware usado contra periodistas*. Recuperado de: http://www.eluniversal.com.mx/articulo/nacion/seguridad/2017/06/19/asi-funciona-Pegasus-el-*Spyware*-usado-contra-periodistas
[27]El Universal (2017b). *Pegasus el software espía definitivo para IOS y Android*. Recuperado de: http://www.eluniversal.com.mx/articulo/techbit/2017/04/20/Pegasus-el-software-espia-definitivo-para-ios-y-android
[28]Expansión. (2017). *12 claves para entender qué es el Spyware Pegasus y cómo funciona*. Recuperado de: http://expansion.mx/tecnologia/2017/06/19/12-claves-para-entender-que-es-el-*Spyware*-Pegasus-y-como-funciona
[29]Publimetro México. (2017). *Así funciona Pegasus, el software que puede tener total acceso a tu celular*. Recuperado de: https://www.publimetro.com.mx/mx/tecnologia/2017/06/19/asi-funciona-Pegasus-software-puede-total-acceso-celular.html
[30]Peirano, M. (2017). *¿Por qué me vigilan, si no soy nadie?*. *TEDx*. Recuperado de: https://www.youtube.com/watch?v=NPE7i8wuupk&t=161s
[31]Telemetro (2017). *Pegasus ¿El espía perfecto?*. Recuperado de: http://www.telemetro.com/nacionales/reportajes/Pegasus-espia-perfecto_3_1041225915.html
[32]Mancilla-Gonzales de la Cotera, E. (2019). *La paradoja de la privacidad de la información en los servicios de Internet*. (Tesis Maestría). Ciencias de la Administración, ESAN University.
[33]Von-Kutschera, F. (1982). *Fundamentos de ética*. Madrid: Cátedra.
[34]Vargas-Mendoza, J. E. (2008) *Ética Pragmática: Lecturas para un seminario*. México: Asociación Oaxaqueña de Psicología A.C.
[35]Bynum, T. W. (2000). The foundation of computer ethics. *Computers and Society*, 30 (2), 6-13.
[36]Quigley, M. (Ed.). (2005). *Information security and ethics: Social and organizational issues*. IGI Global.
[37]Uniapac. (2012). *Protocolo de responsabilidad social empresarial centrada en la persona*. Uruguay: Uniapac Latinoamericana.

[38]R3D. (2017). *Organizaciones enviamos carta a Blackstone Group sobre posible inversión en NSO Group*. Recuperado de: https://r3d.mx/2017/08/01/organizaciones-enviamos-carta-a-blackstone-group-sobre-posible-inversion-en-nso-group/

[39]Aguilar Calderón, P. A. (2015). ¿Derecho Informático o Informática Jurídica?. *Revista de Investigación en Tecnologías de la Información*, 3 (6), 19-24.

[40]Aristegui, C. (2017). *Como PGR compró 'Pegasus', se necesita Panel Independiente que investigue #GobiernoEspía: ONG's*. Recuperado de: http://aristeguinoticias.com/2906/mexico/como-pgr-compro-Pegasus-se-necesita-panel-independiente-que-investigue-gobiernoespia-ongs/

[41]Code of Student Conduct. (2017). *Room 106, Simcoe Hall 27 King's College Circle University of Toronto, Toronto, Canada*. Recuperado de: http://www.governingcouncil.utoronto.ca/Assets/Governing+Council+Digital+Assets/Policies/PDF/ppjul012002.pdf

[42]Montuschi, L. (2002). *Ética y razonamiento moral: Dilemas morales y comportamiento ético en las organizaciones*. Buenos Aires: Universidad del Centro de Estudios Macroeconómicos de Argentina (UCEMA). Recuperado de: http://hdl.handle.net/10419/84263

[43]Elash, A. (2017). *How The Citizen Lab polices the world's digital spies*. Recuperado de: https://www.csmonitor.com/World/Passcode/2016/1222/How-The-Citizen-Lab-polices-the-world-s-digital-spies

[44]Kliksberg, B. (2005). El papel que pueden desempeñar la cultura y los valores éticos en la lucha por la transparecia. Trabaj presentado en el *Seminario Internacional Hacia una cultura de la Transparencia*, Guatemala.

[45]Kliksberg, B. (2007). *Educar en Ética empresarial en Iberoamérica: un desafío impostergable*. Nueva York: Fundación Carolina.

[46]López Navarro, M. Á., Segarra Ciprés, M. (2011). Actitudes de los estudiantes de administración de empresas hacia la responsabilidad social corporativa y la ética empresarial/Attitudes of business administration students towards corporate social responsibility and business ethics. *Revista Complutense de Educación*, 22 (2), 235-248.

[47]Mollo Brisco, G. F., Solari, E. (2009). Ética y formación profesional. Trabajo presentado en el *IX Congreso Internacional de Administración y XVI Congreso de Administración del MERCOSUR*, Buenos Aires.

[48]Puccinelli, O. (2004). Protección de Datos de Carácter Personal. Buenos Aires, Argentina: Ed. Astrea.

[49]Velásquez, H. (2014). *Big Data en el "Universo Compliance"*. Recuperado de: http://www.diariojuridico.com/big-data-en-eluniverso-compliance/

[50]Montejano C., Ayala L. (2009) *Datos Personales. Estudio Teórico Conceptual, de su regulación actual y de las iniciativas presentadas para la creación de una Ley en la materia.* Recuperado de: http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-24-09.pdf

[51]Cable, V. (2014). *Providing better information and protection for consumers. Department for Business, Innovation & Skills*. Recuperado de: https://www.gov.uk/government/policies/providingbetter-information-and-protection-for-consumers/supportingpages/personal-data

[52]Servicio de Noticias de las Naciones Unidas. (2017). *La ONU condena el espionaje a periodistas y activistas en México*. Recuperado de: http://www.un.org/spanish/News/story.asp?NewsID=37575#.WZnPVyjyjIU

