NADA ES LO QUE PARECE: EFECTOS DEL MUNDO VIRTUAL

VULNERABILIDAD DE LA SEGURIDAD INFORMÁTICA: CASO DE RUSIA GATE

Presentado por:

VALENTINA MAYO CASTRO

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

PROGRAMA RELACIONES INTERNACIONALES Y ESTUDIOS POLÍTICOS

BOGOTÁ

2020

INTRODUCCIÓN

El desarrollo informático, y con ello la globalización, son hoy en día un tema de gran trascendencia en el mundo; que si bien, han cambiado e impulsado los avances tecnológicos favoreciendo en su mayoría a los individuos, no dejan de ser un tema que pone en riesgo la seguridad no sólo de los sujetos sino de los Estados en general; ya que a medida que avanzan los programas tecnológicos se incrementan a su vez las violaciones a los sistemas informativos gubernamentales por medio de softwares que buscan robar información Nacional.

A causa de lo anterior, en diferentes Estados se han presentado casos que involucran el robo de información y espionaje, tal como lo es el tan sonado caso del 'Rusiagate', en el que grosso modo se denuncia por parte de la inteligencia de Estados Unidos la intervención de Rusia en las elecciones presidenciales de dicho país en el año 2016 (Arenas, 2019).

En este sentido, el estudio de las Relaciones Internacionales cobra un papel importante en el manejo de la crisis que este caso deja, puesto que se analiza desde diferentes perspectivas y enfoques los resultados que pueda traer para la Seguridad Internacional, teniendo en cuenta que Estados Unidos y Rusia son potencias globales que a su vez discrepan en sus orientaciones políticas conllevando a tensiones en el Sistema Internacional.

Para lograr entender lo que hay detrás del caso de Rusiagate, se realizó una investigación cuyo objetivo principal fue: Analizar la política de privacidad de datos de Estados Unidos frente a la política de Rusia, y con ello identificar cómo la globalización, y el mal uso de medios tecnológicos, ponen en riesgo la seguridad Nacional de Estados Unidos tal como se evidencia en el caso del Rusiagate de tal manera que altera las Relaciones Internacionales entre Estados. Para lo anterior, se identificaron mediante un estudio cualitativo diferentes bases de datos que demostraron el manejo político que tenía cada país para así evitar la intromisión de otro agente gubernamental, a su vez se utilizó un enfoque cuantitativo para comparar la seguridad informática en Estados Unidas, Rusia y la Unión Europea y determinar sus capacidades de protección cibernética

En síntesis, para responder el objetivo principal, fue necesario indagar en los hechos que llevaron a la violación de seguridad Nacional y espionaje en Estados Unidos por parte de Rusia, para lo cual, se analizaron los siguientes temas, en primer lugar, la política de protección de datos, en segundo lugar, la política de datos en Estados Unidos, Rusia y la Unión Europea, en tercer lugar, las leyes de protección de datos entre Estados Unidos y la Unión Europea y finalmente, el estudio de caso del Rusiagate.

PLANTEAMIENTO DEL PROBLEMA

Actualmente, se puede decir que el mercado de la tecnología podría dominar el mundo, dado el uso masivo de GAFA[1], donde a diario se comparten diversas publicaciones, noticias, imágenes, videos, entre otros, sin embargo, la globalización y el desarrollo tecnológico se ve envuelto en una encrucijada debido al mal uso de datos personales, donde demuestra la

[1] Acrónimo para definir Google, Apple, Facebook y Amazon

vulnerabilidad que tiene un individuo al integrarse en un medio tecnológico. Son múltiples las situaciones que se pueden presentar por hackers a través de la red, como lo son, fraudes bancarios, el robo de identidad, hurto de contraseñas y correos electrónicos además de información privada que flagela al ser humano a tal punto que se presentaron 3.2 millones de informes de ciberdelito en Estados Unidos en el año 2019 (FEDERAL TRADE COMMISSION, 2019).

No obstante, los delitos informáticos trascienden fronteras, donde no sólo se ve afectado el individuo como tal, sino que este delito afecta a las Naciones, principalmente con el objetivo de robar información predominante en temas de seguridad Nacional, Economía y Relaciones internacionales, utilizando entre otras cosas medios electrónicos y humanos como espías que incumben dentro de cada gobierno para obtener datos necesarios, siendo esto un gravamen a la estabilidad política del gobierno. En este sentido, se puede determinar que la seguridad en relación con la globalización se encuentra en un grave peligro, Pero, ¿A qué hace referencia la seguridad? “La seguridad, consiste en un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo, si la seguridad se aborda desde el tema disciplinario el concepto se puede definir como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, o gobierno” (Romero Castro, Figueroa Morán, & Murillo Quimiz, 2018, pág. 25).

En consecuencia, como se ha expuesto anteriormente, el mantenimiento de la información personal y Estatal se encuentra en un momento crítico dado los bajos mecanismos de seguridad como softwares que den un aval de protección informática, por ello, a través de esta investigación es importante analizar cómo los diferentes medios virtuales (GAFA: Google,

Apple, Facebook y Amazon), llegaron a consolidarse como 'el gran imperialismo digital', a tal punto de ser un actor importante ante el Sistema Internacional; además de ello, es necesario determinar si hubo alguna relación con el caso del Rusiagate (BBC NEWS, BBC NEWS, 2019)

En este sentido y con el fin de responder al objetivo principal de esta investigación[2], se analizarán los siguientes temas, (I). La política de protección de datos, (II). La política de datos en Estados Unidos, Rusia y la Unión Europea. (III). Las leyes de protección de datos entre Estados Unidos y la Unión Europea y finalmente, el estudio de caso del Rusiagate.

1. Política de Protección de Datos

Para entender un poco sobre las dinámicas que los gobiernos aplican en los ciudadanos específicamente con la protección de datos, a continuación, se expondrá cómo se rigen las leyes de tratamiento de datos y que tan seguro puede estar el consumidor a la hora de compartir sus datos personales en Internet

En este sentido, la investigadora Beatriz Redondo realizó un análisis sobre la protección de datos, en su escrito ultimó que a menudo los titulares de los periódicos Nacionales se ven acaparados por noticias de delitos informáticos, hecho que genera pánico y desconfianza en la sociedad, además de ello culpan al Estado por no tener una normatividad y regulaciones claras frente a estos actos (Beatriz Redondo Tejados, 2019). Los datos personales son un tema muy importante para los usuarios de redes tecnológicas y también para los gobiernos, en el que dichos 'consumidores' se enfrentan a una variedad de regulaciones en diferentes países con diferentes

[2] Analizar la política de privacidad de datos de Estados Unidos frente a la política de Rusia y con ello identificar cómo este tratamiento incidió en el manejo gubernamental que conllevo a tal crisis

visiones; de esta manera, se debe revisar cómo cada uno de estos países protege los datos, para tal fin a continuación, se analizará la Política de Protección de Datos en Estados Unidos y Rusia.

1.1. Política de Protección de Datos Personales en Estados Unidos

Estados Unidos (EEUU), es una de las naciones, que hoy en día no cuenta con leyes predominantes en el tratamiento de Protección de Datos. Dado que una gran cantidad de compañías globales de Internet tienen su sede en los EE. UU. (Google, Facebook, etc.). No obstante, hay dos conjuntos de leyes que brindan alguna orientación sobre la futura regulación de los Estados Unidos:

1. El Estado de California aprobó la Ley de Privacidad del Consumidor de California (CCPA por sus siglas en inglés) que entra en vigor en el presente año (2020), inspirada en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, la cual se refiere a: "La proporción de una variedad de derechos de privacidad para los consumidores de California. Las empresas reguladas por el CCPA tendrán una cantidad de obligaciones para los consumidores, incluidas las divulgaciones, el Reglamento de protección general de datos (RGPD)[3], como los derechos de los interesados en los datos de consumidores y una "exclusión" para determinadas transferencias de datos" (Microsoft, 2020).

[3] Es un reglamento del Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea, cuyo fin es reforzar y unificar la protección de datos para todos individuos de la Unión Europea

2. Estados Unidos también acordó un conjunto mínimo de estándares de privacidad, según lo definido por la Asociación de Asia y el Pacífico (APEC) con 21 países, incluidos Japón, Canadá y México.

El gran cambio llegó en 2018, cuando California aprobó el California Consumer Privacy Act (CCPA), una norma conocida en Estados Unidos por imponer por primera vez, niveles de protección de datos muy similares a los presentes en el RGPD[4]. El CCPA de California responsabiliza a todas las empresas del manejo seguro de los datos personales. También, exige que los usuarios estén informados sobre cómo se usan esos datos y si esos datos se ven comprometidos de alguna manera.

Asimismo, la protección de datos en Estados Unidos es un escenario complejo, por un lado, porque ante los ojos europeos, los estándares de protección de información personal siempre han sido laxos más aún desde que entró en vigor el RGPD. Por otro lado, porque en Estados Unidos la legislación para el tratamiento de datos varían entre Estados, lo que implica diferentes niveles de seguridad y exigencias dependiendo de dónde opere cada empresa. Desde mediados del año 2018, la protección de datos en Estados Unidos volvió a saltar a las portadas cuando Donald Trump firmó en el 2019 una ley para permitir a los Proveedores de Servicios de Internet (ISP), vender datos de los consumidores sin consentimiento previo, invalidando así una norma impulsada por Obama que dictaba lo contrario (Teleam Internacional, 2019). Aunque las empresas de Internet como Facebook, Google y demás aplicaciones ya tenían acceso a datos personales como nombres, números telefónico, además de ubicación en tiempo real (esto al

[4] Reglamento de protección general de datos

aceptar la política de privacidad de cada aplicación para acceder a ella), se sigue recopilando datos de los consumidores sin tener el permiso previo, por ello, los Proveedores de Servicio de Internet (ISP) pueden ir más allá y acceder a la información completa sobre todos los sitios web que visita un consumidor.

En consecuencia, la Comisión Federal de Comunicaciones (FCC, una agencia independiente del gobierno de EE. UU) apoyó la decisión de invalidar esta parte del plan de la era Obama para regular Internet. Por otro lado, según Ajit Pai, director de la FCC, la normativa impulsada por Trump favoreció la competencia en el mundo digital para que fuera más equilibrada. Sin embargo, defensores de los derechos de Internet como el grupo internacional GAFA, mencionados anteriormente, se han mostrado indignados por esta ley que tachan de norma para beneficiar a las corporaciones frente a los internautas.

1.2. Política de Protección de datos personales en Rusia en Relación la Unión Europea

La relación de protección de datos entre Rusia y la Unión Europea (UE) tienen como base jurídica el Acuerdo de Colaboración y Cooperación donde los objetivos comunes en su marco institucional se encuentra el campo de la tecnología, de tal forma que la UE contempla una ley de privacidad de datos para todos los países pertenecientes a la organización. Por otra parte, Rusia, cuenta con una legislación vigente de control y uso de datos en las compañías Nacionales e Internacionales y de cualquier entidad que pueda causar problemas en los usuarios de medios tecnológicos, por esta razón, las empresas que manejan datos personales lo rige el Reglamento General de Protección de Datos (GDPR) que se promulgó en abril de 2016 y entró en vigencia el 25 de mayo de 2018.

1. El GDPR se aplica a cualquier forma de datos personales definida como cualquier dato que por sí mismo, o cuando se combina con otros datos a los que el poseedor pueda acceder y puede usarse para identificar a un individuo (Diario Oficial de la Unión Europea, 2016).
2. El GDPR se aplica a cualquier organización que recopile, almacene o procese los datos personales de los residentes de la UE, ya sea que la organización se encentre o no ubicada dentro de Unión Europea. GDPR está destinado a ser una ley integral de privacidad de datos para los países miembros de la UE, pero cada país debe aprobar sus propias regulaciones para monitorear y hacer cumplir GDPR dentro de sus fronteras (Diario Oficial de la Unión Europea, 2016).
3. GDPR ofrece a las personas el derecho a solicitar la eliminación o corrección de sus datos personales y exige a las empresas que cumplan con esas solicitudes (Diario Oficial de la Unión Europea, 2016).

Por consiguiente, la revista Forbes enfatizó una publicación que presume la entrada en vigor de Rusia en las enmiendas a la Ley Sobre Datos Personales[5] que desde 2006 ha llevado a cabo unos cambios autorizados por ambas cámaras del parlamento nacional, donde se aprobó esta ley que obliga a los sitios de Internet que almacenan información personal de los ciudadanos a guardarla dentro del país, y todas las compañías de Internet tendrán que trasladar los datos de ciudadanos rusos a servidores ubicados dentro de la Nación o sus sitios serán bloqueados (FORBES, 2016).

[5] La ley determina que a partir del 2016 todas las compañías de Internet tendrán que trasladar los datos de ciudadanos rusos a servidores ubicados dentro del país o sus sitios serán bloqueados. Eso probablemente afecte a las redes sociales con sede en Estados Unidos, como Facebook, dicen analistas (FORBES, 2016).

A su vez, el Kremlin[6] adoptó una ley a comienzos de año que le da a las autoridades el poder para bloquear sitios web considerados extremistas o una amenaza al orden público sin una orden judicial. Por otra parte, el presidente Putin ha adoptado una postura cada vez más conservadora desde que enfrentó protestas masivas contra su regreso al Kremlin en 2012. Los manifestantes usaron las redes sociales para compartir sus posturas críticas hacia las autoridades y para coordinar sus movimientos, se trata de una de las leyes más discutidas tanto por la sociedad rusa como por la comunidad profesional, que se enfrenta diariamente a amenazas de la piratería cibernética y el espionaje electrónico.

1.3. Legislación de protección de datos entre Estados Unidos y la Unión Europea

Una de las políticas más relevantes dentro de la Unión Europea es La Privacy Shield[7], sin embargo, ha quedado en un segundo plano por la obligatoriedad de cumplimiento en relación con el RGPD, aunque se revisa anualmente y presenta múltiples modificaciones en los últimos tiempos con el fin de adecuarse los estándares de la normativa europea. No obstante, aunque se encuentran diferentes normatividades en Rusia como en Estados Unidos, la correlación con la UE, radica en la 'neutralidad' de esta Organización Internacional a la hora de ejecutar mecanismo de cuidado de datos, pero, la gran diferencia entre Estados Unidos y la Unión Europea radica en las competencias a la hora de legislar, donde en el caso de Europa recaen sobre el Parlamento Europeo y en el caso de Estados Unidos le compete a los Estados., esto provoca es que, mientras que en la UE se cuenta con 'una norma para gobernarlos a todos'

[6] La residencia oficial del presidente de la Federación Rusia y la sede permanente del Gobierno Ruso

[7] In the 2015 Screams case, the Court of Justice of the European Union (CJEU) declared the European Commission's 2000 decision on the 'adequacy' of the EU-US Safe Harbour regime invalid. This regime had formed the legal basis to allow transfers of data, for commercial purposes, from the EU to the United States of America (USA). (European Parliamentary Research Service, 2018)

(European Parliamentary Research Service, 2018), en Estados Unidos, cada estado cuenta con su propia legislación de protección de datos a la que debe acogerse. A raíz de la aprobación del RGPD, y las presiones desde Europa por un endurecimiento de las normativas varios estados modificaron sus leyes o introdujeron cláusulas nuevas. En síntesis, se debe determinar que a pesar de las diferencias legislativas, realmente quien se encuentra en riesgo son los usuarios que dejan en la red diferentes tipos de información donde estos poderosos monopolios empresariales están haciendo grandes negocios absorbiendo cantidades astronómicas de información obtenida por contratos que no se suelen leer, por ignorancia o porque algunos usuarios que solo quieren beneficiarse con la gratuidad de estos servicios, sin importar cómo se utilice su información.

2. RUSIAGATE

"Internet facilita la información adecuada, en el momento adecuado, para el propósito adecuado"
(Bill Gates[8])

De todas las controversias que han rodeado a Donald Trump desde su campaña electoral hasta su actual rol como presidente de Estados Unidos, el vínculo que tiene el Gobierno de Rusia con el de Estados Unidos no consigue apartarse, ya que siempre da de qué hablar ante la comunidad internacional. Esto se debe al escenario mediático cuando en los diarios más importantes como el The New York Times revelaron que agentes de inteligencia interceptaron las comunicaciones cuando descubrieron que Rusia estaba intentando alterar la elección presidencial 'hackeando' al Partido Demócrata (The New York Times, 2017), seguido a esto la Convención Nacional Demócrata, denunció que el sitio de filtraciones de WikiLeaks publicó

[8] "Entrepreneur and businessman Bill Gates and his business partner Paul Allen founded and built the world's largest software business, Microsoft, through technological innovation, keen business strategy and aggressive business tactics" (BIOGRAPHY, 2020)

20.000 correos electrónicos internos de ese partido, que habían sido robados por hackers (WikiLeaks, 2016).

Para entender un poco sobre este escándalo, del que incluso hoy en día se sigue teniendo relevancia internacional, es necesario tener conocimiento de la relación entre la Nación Rusa respecto a diferentes organismos de inteligencia usados para obtener información, además de los actores implicados en estos hechos. Más allá de que las noticias sean falsas o solo sean simples acusaciones, las campañas políticas difamatorias detectadas en el proceso eleccionario de Trump con la intervención de corporaciones globales de Internet, generaron un debate inédito sobre el impacto negativo de las redes sociales, insertas en corporaciones globales que manejan oscuramente nuestros datos, para el 2016 fue el año en que se generó esta situación donde se debatió sobre la responsabilidad de las plataformas en las campañas políticas y el indebido uso de datos personales (BBC NEWS , BBC MUNDO, 2017). La versión oficial sobre el Rusiagate se basa en que Trump ganó las elecciones presidenciales del 2016 con ayuda de Rusia, sin embargo, el reporte final del fiscal Robert Mueller había concluido que no hay colusión, pues en el principio de la investigación sea firma que ex oficiales de diferentes agencias de inteligencia de Estados Unidos como la Agencia Central de Inteligencia (CIA) y la Agencia de Seguridad Nacional (NSA), demostraron que nunca existió un hackeo por parte de la inteligencia Rusa al Comité Nacional Demócrata (DNC).

Por consiguiente, la operación Rusiagate tiene como participantes a miembros de la CIA, FBI[9] , NSA y MI6[10], uno de ellos es Christopher Steele[11], que fue pagado por la campaña de Hillary

[9] Agencia de Gobierno de Estados Unidos
[10] Agencia de Inteligencia secreta de Reino Unidos
[11] Ex Oficial de la Agencia de Inteligencia Británica MI6

Clinton y el Comité Nacional Demócrata para asociar a través de su informe que existía una colusión con Vladimir Putin y Donald Trump. Steele admitió en una corte de Londres que fue contratado para ayudar a Hillary Clinton a disputar la contienda de las elecciones del año 2016, con estas declaraciones varios demócratas buscaban implicar reuniones entre funcionarios del kremlin y los abogados de Trump, para ver cómo se realizaban los pagos a hackers Rusos que intervenían en las computadoras del Comité Nacional Demócrata, no obstante, las investigaciones terminaron en el año 2018 dado que no se encontraron pruebas que concluyeran la relación entre Donald Trump y el gobierno de Rusia.

Frente a ello, está en cuestionamiento la intervención del Gobierno Ruso en los asuntos internos de Estados Unidos. Por otra parte, se comprobó la aparición de Fake News[12] generadas por Rusia a través de las redes sociales y las características puntuales que utilizaba el gobierno generó que este escándalo llegara al congreso de EE. UU, acusando a Facebook, Google y Twitter por sus roles en la injerencia rusa en la campaña de Trump. Facebook terminó admitiendo el uso de su red para llevar propaganda rusa a 126 millones de estadounidenses, ellos mismos reconocen el daño que Internet está ocasionando, estos riesgos empeoran cada año y que las soluciones deben encontrarse urgentemente, “Dos de cada cinco estadounidenses vieron publicaciones que tendrían como objetivo interferir en la política estadounidense” (EL MUNDO, 2017). Pero eso no fue todo, luego estallaron en la escena pública otras intervenciones como la de Cambridge Analytica, cuyo objetivo era influenciar los comportamientos políticos y

[12] Noticias falsas que tergiversan información por medio de las Redes Sociales

comerciales de las personas, sin embargo, esta compañía usó datos obtenidos inapropiadamente de Facebook para tratar de influir en procesos electorales como la elección presidencial.

Además del planteamiento anterior, también estuvo involucrada la compañía Internet Research Agency, que está vinculada al Kremlin, hizo unas 80.000 publicaciones entre enero de 2015 y agosto de 2017. Esas publicaciones alcanzaron a 29 millones de estadounidenses. La compañía creada por Mark Zuckerberg también reconoció que Internet Research Agency invirtió cerca de 100.000 dólares para 3.000 anuncios en unas 470 páginas que ya han sido cerradas (EL MUNDO, 2017). Los contenidos de estas publicaciones estaban relacionados con la raza, la religión, los derechos a las armas y con la orientación sexual y de género.

OPINIÓN PERSONAL

A través de este ensayo de investigación se pudo evidenciar que la globalización, y con ello los avances tecnológicos, dejan consigo muchos desafíos para la protección y seguridad Nacional de cada Estado. Además, que estos hechos alteran el sistema internacional puesto que hay nuevas amenazas tal como lo denomina Mary Kaldor[13] en su libro "Las nuevas guerras. Violencia organizada en la era global" en el que enfatiza en una serie de reconceptualizaciones como consecuencia de la globalización, que han venido afectado de una u otra manera a los Estados, tal como se pudo evidenciar en el caso del Rusigate.

[13] Profesora de Relaciones Internacionales e investigadora en la Universidad de Sussex (Reino Unido), ocupó la prestigiosa cátedra Jean Monnet de Estudios Europeos. En la actualidad es catedrática de Gobernanza Global en la London School of Economics, donde dirige el Programa para la Sociedad Civil Global. (COMPARTE LIBROS, 2016)

En este sentido, la intervención de Rusia en los sufragios presidenciales del año 2016 cuyo ganador es el hoy presidente Donald Trump, deja en vilo la legitimidad de las elecciones de ese año, arrojando dudas sobre la legalidad de Trump como presidente, por ello, el caso de el Rusiagate, es un hecho que dado la injerencia de Rusia en Estados Unidos no sólo genera incertidumbre en los ciudadanos, sino que pone en tela de juicio la democracia estadounidense. En consecuencia, deja claro la falta de garantías tecnológicas que tiene EEUU y que pone en riesgo la Seguridad Nacional, en vista de la manipulación de una potencia extranjera con la que además ha tenido diferentes enfrentamientos políticos a través de la historia.

Por otra parte, la suplantación de identidad, el robo de información, el espionaje y la creación de nuevos softwares maliciosos, no son un tema nuevo, queda en entredicho la falta de recursos que tiene el Estado para prevenirlos. Estados Unidos, es una muestra de ello, a pesar de ser uno de los países más avanzados en materia tecnológica no ha logrado prevenir ni tomar las medidas necesarias ante los delitos informáticos. Sin embargo, este no es único problema que tiene, pues el uso masivo de las diferentes plataformas virtuales (GAFA), son una modalidad de obtención de datos además de difusión de Fake News, de esta manera buscan alterar a la sociedad generando incertidumbre sobre la legitimidad del gobierno.

En síntesis, a pesar de las especulaciones que ha tenido el caso de el Rusiagate, deja claro que no hace falta ser un experto en el manejo de softwares para incumbir en la política interna de Estados Unidos, puesto que el uso masivo de redes sociales y la divulgación de información, son ejes de conspiración que influye en la percepción política del país. Si bien, aún quedan las sospechas de que el Kremlin tiene información detallada sobre los políticos Demócratas y Republicanos con el fin de hacer campañas de desprestigio o ciberataques que afecten las

próximas elecciones presidenciales con el fin de incumbir en los asuntos internos de Estados Unidos.

Referencias

Arenas, D. (22 de 10 de 2019). América Latina en Movimiento. Obtenido de https://www.alainet.org/es/articulo/202775

BBC NEWS. (15 de FEBRERO de 2017). BBC MUNDO. Obtenido de BBC MUNDO: https://www.bbc.com/mundo/noticias-internacional-38974595

BBC NEWS. (06 de junio de 2019). BBC NEWS. Obtenido de BBC NEWS: https://www.bbc.com/mundo/noticias-48542153

Beatriz Redondo Tejados. (2019). Protección de datos en Estados Unidos. Protección de datos en Estados Unidos, pág. 52.

BIOGRAPHY. (8 de ABRIL de 2020). Bill Gates Biography. Obtenido de Bill Gates Biography: https://www.biography.com/business-figure/bill-gates

Diario Oficial de la Unión Europea. (2016). REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Obtenido de REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO: https://www.boe.es/doue/2016/119/L00001-00088.pdf

EL MUNDO. (31 de octubre de 2017). EL MUNDO. Obtenido de EL MUNDO: https://www.elmundo.es/internacional/2017/10/31/59f84fd5e5fdead57e8b4627.html

European Parliamentary Research Service. (Julio de 2018). European Parliament. Obtenido de European Parliament: https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf

FEDERAL TRADE COMMISSION. (2019). INSURANCE INFORMATION. Obtenido de INSURANCE INFORMATION: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#:~:text=Of%20the%203.2%20million%20identity,percent%20reported%20money%20was%20lost.

FORBES. (2016). Rusia aprueba ley para proteger datos personales en la red. FORBES.

Microsoft. (22 de 02 de 2020). Ley de privacidad del consumidor de California (CCPA). Obtenido de Ley de privacidad del consumidor de California (CCPA): https://docs.microsoft.com/es-es/microsoft-365/compliance/offering-ccpa?view=o365-worldwide

Romero Castro, M. I., Figueroa Morán, G. L., & Murillo Quimiz, Á. L. (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Ciencias Área de Innovación y Desarrollo, 25. Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Teleam Internacional. (2019). Trump promulgó la ley que permite a proveedores de Internet vender datos de usuarios. Obtenido de

https://www.telam.com.ar/notas/201704/184652-trump-ley-datos-personales-internet-venta-datos-personales.html

The New York Times. (2017). The New York Times. Obtenido de The New York Times: https://www.nytimes.com/es/

WikiLeaks. (2016). WikiLeaks. Obtenido de WikiLeaks: https://wikileaks.org/