

**El Impacto del Capitalismo de Vigilancia en las Relaciones Estados Unidos - Unión  
Europea Durante el Periodo 2013-2020.**

Pontificia Universidad Javeriana

Facultad de Ciencias Políticas y Relaciones Internacionales

Carrera de Relaciones Internacionales

05 de Octubre de 2022

Bogotá D.C. Colombia

**El Impacto del Capitalismo de Vigilancia en las Relaciones Estados Unidos - Unión  
Europea Durante el Periodo 2013-2020.**

Pontificia Universidad Javeriana

Nicolás Pérez Ardila

Facultad de Ciencias Políticas y Relaciones Internacionales

Directora: Merly Guanumen Pacheco

05 de Octubre de 2022

Bogotá D.C. Colombia

/

## Tabla de Contenido

|  |                                   |
|--|-----------------------------------|
| Resumen .....  | - 4 -                             |
| Introducción y Problema de Investigación .....                     | - 5 -                             |
| Capítulo 1: El Capitalismo de Vigilancia .....                     | - 9 -                             |
| 1.1 Antecedentes: La Ley Patriota .....                            | - 9 -                             |
| 1.2 Las Revelaciones de Edward Snowden y Cambridge Analytica ..... | - 12 -                            |
| 1.3 Capitalismo de Vigilancia. ....                                | - 15 -                            |
| 1.3.1 Facebook y el Capitalismo de Vigilancia .....                | <del>- 18 -</del> <del>-19-</del> |
| 1.3.2. El Ciberespacio .....                                       | - 20 -                            |
| 1.5 Estado del Arte:.....  | - 24 -                            |
| Capítulo 2: La Respuesta Europea .....                             | <del>- 26 -</del> <del>-27-</del> |
| 2.1 Respuesta mediática .....                                      | <del>- 30 -</del> <del>-31-</del> |
| 2.2 Respuesta de la UE:.....                                       | <del>- 34 -</del> <del>-35-</del> |
| 2.2.1 Derechos Digitales y reformas de la UE. ....                 | <del>- 37 -</del> <del>-38-</del> |
| 2.3 Consideraciones Generales.....                                 | <del>- 39 -</del> <del>-40-</del> |
| Capítulo 3: Un mundo redefinido por la vigilancia .....            | <del>- 43 -</del> <del>-44-</del> |
| 3.1 Resultados.....  | <del>- 44 -</del> <del>-45-</del> |
| 3.1.1 Respuesta Estadounidense: .....                              | <del>- 45 -</del> <del>-46-</del> |
| 3.3 La Redefinición del Ciberespacio .....                         | <del>- 46 -</del> <del>-47-</del> |
| 3.4 Conclusiones .....   | <del>- 48 -</del> <del>-49-</del> |
| Bibliografía: .....  | <del>- 50 -</del> <del>-51-</del> |
| Anexos.....  | <del>- 56 -</del> <del>-57-</del> |

## **Resumen**

El Internet y la digitalización han obligado a las relaciones internacionales a adaptarse a los nuevos retos y a las nuevas oportunidades que ofrecen los avances tecnológicos y a las dinámicas que el capitalismo y la globalización han implementado. El Internet se convirtió en una plataforma para el desarrollo económico, político, comercial y social a través de empresas como Facebook quienes, en los últimos años, han sido parte de los espacios de intercambio de información y conectividad entre sus usuarios y con la posibilidad de generar ingresos a través de los negocios y la publicidad. A raíz de las revelaciones de Edward Snowden y la investigación de Cambridge Analytica, se descubrió que Facebook es un intermediario de datos entre compañías de publicidad, hasta campañas políticas internacionales, que permiten la manipulación a través de la recolección y venta de datos personales de usuarios de varios países. Esto afectó las relaciones entre Estados Unidos y la Unión Europea quien ha tomado medidas de protección; sin embargo, las plataformas digitales continúan evolucionando y generando incertidumbre frente a la relación entre ambos bloques, y el futuro de la naturaleza de la política, en un marco plenamente digital.

**Palabras Clave:** Capitalismo de Vigilancia, Ciberespacio, Cooperación.

## **Introducción y Problema de Investigación**

En el año 2013 salieron a la luz pública una serie de revelaciones que comprometían a la Agencia de Seguridad Nacional (NSA) de Estados Unidos, a empresas de análisis de datos, y a las gigantes tecnológicas de Silicon Valley, principalmente a Facebook. Las primeras acusaciones vinieron por parte del ex empleado de la Agencia Central de Inteligencia (CIA) y la NSA, Edward Snowden, asegurando que estas agencias recopilan los datos personales de millones de usuarios, organizaciones e inclusive gobiernos, en las plataformas de Internet con fines de seguridad. Esto generó una serie de perturbaciones en las relaciones diplomáticas entre Estados Unidos (EE. UU.) y la Unión Europea (UE), dos actores internacionales históricamente vinculados a partir de sus valores, intereses, e historia mutua, que se traducen en la construcción de la confianza.

Las revelaciones de Snowden expusieron el gran grado de vigilancia en materia de seguridad que tiene el gobierno estadounidense sobre sus ciudadanos, tanto americanos como extranjeros, mientras que la posterior información revelada sobre la firma Cambridge Analytica y Facebook establecieron una serie de dinámicas de monetización a partir de los datos, con la particularidad de ocultar a sus usuarios qué datos se extraían y con qué finalidad. La red social, que basa casi que la totalidad de sus ingresos en publicidad dirigida a partir de los datos funcionó como proveedor de información a Cambridge Analytica para tener un amplio panorama de la información de sus usuarios. De esto último, la investigación periodística estableció que la venta de datos personales se hizo con el fin de facilitar contenido a usuarios susceptibles a cambiar fácilmente de opinión, a su vez de usuarios con tendencias definidas, para que estos votasen en concreto por la campaña presidencial de Donald Trump, y a favor de la campaña del Bréxit.

Empresas como Facebook por su lado, cuenta con más de mil millones de usuarios a nivel global, por lo tanto, la información almacenada en sus bases de datos no pertenece únicamente a ciudadanos estadounidenses; esta actividad digital es comercializada y distribuida a otras empresas, así como a agencias estatales. De la misma manera, y como consecuencia de las medidas adoptadas por EE. UU. en materia de política exterior y seguridad, a partir de los atentados del 11 de septiembre del 2001, las agencias

estadounidenses tienen cierta potestad de recopilar esta información, como se verá más adelante. Sin embargo, a raíz del escándalo de Cambridge Analytica se profundizó el debate alrededor de las nuevas dinámicas digitales y el peso de estas en las Relaciones Internacionales (RRII), abarcando desde lo económico y político, pero principalmente el ámbito comercial, donde la acumulación y ganancia traducida en datos, se recopilaban mediante el espionaje a organismos comerciales y políticos en Europa. En este caso, no son los productos y servicios aquello que es capitalizable, sino los datos del 'cliente', que sería entonces el producto, dado que el cliente son las corporaciones que monetizan y generan ingresos a partir de los datos de los usuarios.

Estas nuevas dinámicas de comunicación permitieron a otras compañías, además de las corporaciones digitales, utilizar a los consumidores como los mismos productos en el sistema, siendo su información la que es valiosa para lograr un fin determinado. Por un lado, las actuales compañías más lucrativas como Facebook han reformulado su modelo de negocio, tema que se desarrollará posteriormente, alrededor de satisfacer las necesidades del usuario a partir de la información que este provee, con el fin de dirigir publicidad específica de acuerdo con sus intereses, situación que involucra una clara invasión a la privacidad del individuo. Al no estar debidamente reguladas a nivel internacional, esto permite a las compañías emplear la información de la manera que consideren conveniente y a su vez, venderla a otras entidades que repiten esta operación con distintos fines.

Europa por su lado, avanza en el desarrollo tecnológico y digitalización de sus Estados miembros, a la vez de legislaciones y regulaciones en cuanto a la distribución de datos personales y registros digitales de su población. Esto le ha permitido a la UE mantener el equilibrio entre el desarrollo del comercio, y la protección de la libertad de sus ciudadanos.

Por lo anterior, el presente trabajo busca responder la pregunta de investigación: ¿De qué manera afectó el capitalismo de vigilancia y las revelaciones de espionaje de Edward Snowden, las relaciones entre EE. UU. y la UE, entre los años 2013 y 2020?

En ese orden de ideas, el objetivo general de esta investigación es analizar las consecuencias de las revelaciones de Edward Snowden, y el escándalo Facebook-Cambridge Analytica, para las relaciones EE. UU.- UE. Más específicamente se pretende:

1. Establecer cómo el capitalismo de vigilancia está afectando la política internacional, en particular las relaciones entre países aliados.
2. Comprender la respuesta de la UE a las revelaciones de espionaje de Estados Unidos.
3. Exponer las consecuencias del capitalismo de vigilancia, y el espionaje gubernamental, en las relaciones EE. UU.- UE, durante el período 2013-2020.

Para entender las alteraciones en estas relaciones mutuas, se usará como perspectiva teórica el constructivismo moderado, dado que el foco de la investigación son las variaciones en los valores construidos a partir de las experiencias de la realidad, habiendo elementos externos preestablecidos, es decir, construcciones y reglas presentes en el contexto de los países, como los valores producto de procesos históricos e ideologías compartidas.

La metodología usada se enfoca en el método cualitativo de análisis de prensa y bibliografía, para comparar y comprender la respuesta y las consecuencias para cada país en concordancia con los planteamientos constructivistas. Se emplearon revistas, casos, artículos, notas periodísticas, además de informes, leyes y reportes de organismos estatales, esto con el fin de establecer diferencias y similitudes entre ambos actores, y comprender el carácter de las medidas que son finalmente, la base bajo la cual se comprenden las consecuencias en las relaciones diplomáticas posteriores a los eventos.

La presente investigación estará dividida en tres capítulos a partir de los tres objetivos de la investigación. Desde el constructivismo se estudiarán las estructuras y dinámicas de las redes y el ciberespacio, además de su aproximación conceptual. En segundo lugar, el análisis de conflicto permitirá comprender la respuesta de la UE y el nuevo carácter de las relaciones entre ambos bloques. Las consecuencias se estudiarán a partir de los datos y casos analizados, las respuestas estadounidenses y el resultado en cuanto a los valores e intereses que

componían las relaciones entre ambos actores. Y, por último, se formula una conclusión que dará respuesta a la pregunta de investigación previamente formulada.

## **Capítulo 1: El Capitalismo de Vigilancia**

### **Una nueva dirección en el curso de las Relaciones Internacionales**

El desarrollo del Internet posterior a los noventa, sumado al crecimiento del ciberespacio y el traslado progresivo de las actividades políticas, económicas y sociales a este plano; y la vinculación a la política de seguridad de EE. UU. posterior a los ataques del 11 de septiembre, consolidaron el capitalismo de vigilancia, concepto original de la autora Shoshana Zuboff, como sistema relevante para las relaciones entre actores internacionales (2019). La vigilancia entre países aliados representa la traición y la ruptura de la construcción de valores e intereses mutuos y da relevancia a actores no estatales, como lo son las plataformas digitales, particularmente Facebook, que moldean la realidad del Sistema Internacional y representan un cambio en los elementos que componen la diplomacia entre ambos actores; surgen nuevos intereses y por lo tanto modificaciones en el sistema de valores y la distribución de poder.

#### *1.1 Antecedentes: La Ley Patriota*

Previo a los escándalos y las investigaciones con respecto a la vigilancia estatal, los avances digitales y los eventos en materia de seguridad generan que EE. UU. adopten una nueva postura con respecto al acceso a la información de sus ciudadanos. Posterior a los ataques terroristas del 11 de septiembre del 2001, el gobierno estadounidense bajo la recién introducida doctrina Bush, estableció una serie de lineamientos y nuevas facultades en materia de seguridad, a las agencias de seguridad estatales y de vigilancia en el marco de la Guerra contra el Terrorismo. La doctrina Bush estaba encaminada a situar los intereses norteamericanos en defensa de la libertad y la democracia, y expandir estos intereses a naciones no-democráticas particularmente en Medio Oriente.

En materia de política exterior y seguridad, la guerra contra el terrorismo trajo un despliegue masivo de programas de vigilancia, recopilación de información y seguimiento al ciudadano, justificado bajo la amenaza de un nuevo ataque terrorista y la protección de la seguridad

nacional. La ‘Ley Patriota’ de EE. UU., de acuerdo con Alba Useche (2014), sancionada posterior a los ataques talibanes, otorgó facultades al gobierno de EE. UU. de interceptar y recopilar datos de comunicaciones de sus ciudadanos tanto al interior, como al exterior del país y traspasar la privacidad de algún individuo si éste demuestra un comportamiento sospechoso y de carácter amenazante para la seguridad e intereses nacionales.

La Ley Patriota de EE. UU. regía, en teoría, para ciudadanos y empresas estadounidenses al interior y exterior del territorio americano. Sin embargo, desde su firma, existen varios interrogantes frente al verdadero carácter internacional de la ley, enfocado en la protección de los derechos a la privacidad de ciudadanos no estadounidenses. Esta ley, sin embargo, está sujeta a cambios cuando se habla particularmente de empresas, en especial de aquellas norteamericanas que tercerizan su fuerza laboral, poseen sucursales en el extranjero o recurren a la subcontratación.

Bajo ciertas circunstancias esta ley permitiría la divulgación de datos personales, si así lo requiere la empresa o individuo, bajo la sospecha de actividad criminal o terrorista (Lecours, 2007). Además, esta ley opera como un puente que permite a agencias como la Agencia de Seguridad Nacional (NSA), la Agencia Central de Inteligencia (CIA), o la Agencia Federal de Investigación (FBI), recopilar información a través de las plataformas comerciales previamente mencionadas, poniendo en tela de juicio el papel de las corporaciones, y el verdadero carácter de la seguridad y protección de los datos bajo estas compañías.

El apartado número dos y tres de la Ley Patriota sobre los Procedimientos de Control e Intercambio de Información, establece el vínculo entre socios comerciales y agentes estatales para distribuirse información mutuamente, esto con el fin de llevar control estricto sobre la información financiera de miembros de grupos terroristas. Más específicamente establecen lo siguiente:

Cuestiones específicamente relacionadas con las finanzas de grupos terroristas, los medios a través de los cuales dichos grupos transfieren fondos alrededor del mundo y dentro de los EE.UU., incluyendo mediante el uso de entidades de beneficencia, entidades sin fines de lucro, y ONGs, y la medida en que las entidades financieras en

EE.UU. participan inadvertidamente en dichas finanzas, así como el riesgo que ello representa para dichas entidades; (...) Los medios para facilitar la identificación de cuentas y operaciones que involucren a grupos terroristas, y para facilitar el intercambio de información relativa a dichas cuentas y operaciones entre las entidades financieras y las autoridades. (US Patriot Act 2001, art 2. 107-56.)

La Ley Patriota, como es posible evidenciar en los anteriores fragmentos, se enfoca en el seguimiento y control a través de la información, a entes comerciales y financieros, siendo este un método que puede resultar efectivo debido a la gran cantidad de datos que son extraídos con este propósito. Es decir, y de acuerdo con Lecours (2007) el gobierno de EE. UU. estableció acuerdos con empresas tecnológicas para transferir grandes cantidades de datos con la finalidad de hacer seguimiento y encontrar irregularidades en usuarios que los vincularan al terrorismo internacional. Además de empresas de tecnología, este mecanismo permite a EE. UU. recopilar información de sus clientes y/o consumidores.

Las implicaciones en la política internacional y las relaciones de EE. UU. a partir de la Ley Patriota son diversas. En primer lugar, este acto legislativo constituyó una redefinición en la política exterior del país, estableciendo nuevas bases a partir de un nuevo orden en el Sistema Internacional. La lucha contra el terrorismo y la doctrina estadounidense establecieron a este Estado como el hegemón occidental, instigando a los países aliados de éste, a adaptar nuevas legislaciones que, como se ha venido mencionando, satisficieran los intereses de Estados Unidos. Al estar los Estados europeos sujetos al intercambio de información con motivos de seguridad, hay un dilema de soberanía presente; desde la ejecución de esta ley ya hay presente un condicionamiento por parte de EE. UU. hacia Europa, más allá de la construcción de un sistema de confianza y valores mutuos. El establecimiento de la Ley Patriota es además un intento por ejercer control, influencia y dominio sobre el tráfico de capital humano (y en este caso su información personal) con fines económicos.

Las implicaciones para la UE se desarrollan en la búsqueda de la cooperación con EE.UU., comprendiendo que el país americano es líder en tecnologías, y, al ser aliados históricos y estratégicos, Europa no puede permitirse medidas drásticas que atenten (o desvíen) contra

los postulados de la Ley Patriota, y el compromiso europeo con la seguridad internacional en la guerra contra el terrorismo.

Si bien la responsabilidad principal de luchar contra la delincuencia y de garantizar la seguridad recae principalmente en los Estados miembros, los atentados terroristas de los últimos años han dejado patente que también es una responsabilidad común que todos ellos deben asumir juntos. La UE contribuye a la protección de sus ciudadanos actuando como **principal foro de cooperación y coordinación** entre los Estados miembros. (...) En 2014, el Consejo adoptó la estrategia de la UE contra el terrorismo y los combatientes extranjeros centrada en Siria e Irak. En dicha estrategia se definen varios ámbitos prioritarios, como la mejora de la colaboración con terceros países para detectar las redes de captación e identificar a los combatientes extranjeros (Comunicado de Prensa. Consejo Europeo, 2020).

Por fuera del discurso de seguridad, el intercambio, compra y venta masiva de datos tiene otras implicaciones, y, sumado a las revelaciones de Edward Snowden, como se podrá ver posteriormente, distante del marco legal, en materia de RRII, esto se entenderá más adelante alrededor del concepto de Capitalismo de Vigilancia. Desde este punto de vista, y en aproximación al problema de la presente investigación, se establece lo siguiente: la Ley Patriota de los Estados Unidos obedece, en teoría, a la necesidad del país de combatir y prevenir episodios como los del 11 de septiembre.

### *1.2 Las Revelaciones de Edward Snowden y Cambridge Analytica*

Pasando a los hechos, previo a la aproximación conceptual y teórica al capitalismo de vigilancia, es pertinente elaborar un resumen con respecto a las investigaciones que resultan en la aparición del capitalismo de vigilancia como sistema, y sus implicaciones inmediatas en las relaciones EE. UU.-UE.

En el año 2013, el ex agente de la Agencia Nacional de Seguridad de EE. UU., Edward Snowden reveló a investigadores y periodistas, información sobre la recopilación masiva de datos por parte de la agencia, con fines de seguridad internacional. Las investigaciones

sugirieron que Facebook operaba como intermediario al poner a disposición de agencias estatales, los datos de los usuarios. Esto se hacía mediante la actividad al interior de la red social de cada usuario y el historial digital de actividad que un usuario construye a partir de su actividad en internet (Aguilar, 2018), que eran empleados por una inteligencia artificial para diseñar un perfil completo del ciudadano en cuestión, y a partir de esto establecer si sus conductas digitales representaban un nivel de amenaza para la seguridad nacional.

Posteriormente en el año 2015, el periodista Harry Davies, consciente de que compañías de (originalmente) análisis de datos, específicamente la firma británica Cambridge Analytica, recolectaban sus datos, inicia una investigación contra la compañía para esclarecer el objetivo final de sus datos personales, además de la cantidad real de información a la cual la firma tenía acceso. Ante la negativa de la compañía por otorgar respuestas, la investigación llevada a cabo durante el año posterior arrojó a la luz resultados controversiales con respecto al uso y recopilación de datos proporcionados por Facebook. La firma Cambridge Analytica, en un principio se presentaba como una empresa dedicada a realizar perfiles digitales precisos con el fin de dirigir publicidad específica con base en los intereses de los usuarios y garantizar mayores ventas a las compañías (clientes), las revelaciones de un ex empleado de la compañía, Christopher Wylie; sin embargo, expusieron el verdadero mecanismo bajo el cual se operaba. La realidad constaba en la firma británica, efectivamente creando perfiles precisos de aproximadamente 80 millones de usuarios, pero vendiéndolos sin el consentimiento de estos, a campañas políticas, concretamente los republicanos Donald Trump y Ted Cruz en EE. UU., y la campaña a favor de la salida del Reino Unido de la UE, o Brexit.

El documental *The Great Hack* (2019) explicaba que el mecanismo consistía en Facebook como el principal recopilador de *metadatos* (concepto que será desarrollado en la próxima sección), y que posteriormente eran vendidos a Cambridge Analytica para que ésta a su vez vendiera los perfiles digitales a las campañas políticas. En este punto, y al igual que una empresa de productos y servicios regular dirigía contenido político a perfiles susceptibles a recibir positivamente este tipo de información, con el fin de reafirmar o radicalizar su postura y así garantizar el voto deseado. Por otro lado, la exdirectora de desarrollo de negocios de la

firma británica, Brittany Kaiser (2019), explicó en una serie de testimonios, cómo las campañas políticas perfilaban usuarios denominados *persuasibles*, y consistían en perfiles cuyos registros digitales denotaran posturas poco claras y con tendencias cambiantes, con el fin de ‘bombardearlos’ con contenido dirigido para reconstruir e imponer su perfil digital y que estos tomaran las decisiones que la compañía esperaba.

Las interacciones en el ciberespacio se han diversificado al nivel de empresas y Estados con mayor capacidad de acción en este plano, las cuales además cuentan con la libertad de regular y decidir sobre la mayoría del contenido que circula. De esta manera, empresas y Estados cooperan en el ciberespacio para competir y defender sus propios intereses y en el entorno reciente, las mismas técnicas empleadas por Cambridge Analytica, se utilizan por las empresas en el contexto del conflicto ciberespacial en las RRII entre intereses políticos y comerciales, empresas e instituciones, con el fin de desviar la opinión pública y radicalizar sectores de la población con fines comerciales y políticos, como bien mencionó Edward Snowden en una entrevista con El Diario de España, siendo la vigilancia un elemento de poder y no de seguridad (Snowden, 2016). Las revelaciones involucraron a las agencias de seguridad, así como cuerpos de vigilancia tales como Cinco Ojos, Estados Unidos en compañía de Reino Unido, Nueva Zelanda, Canadá y Australia establecieron una iniciativa de inteligencia e intercambio de información que se vio involucrada en el espionaje a sus ciudadanos (Sánchez, 2015).

En contraparte, la UE, a raíz de las problemáticas surgidas a partir de la Ley Patriota y las acciones tomadas tanto por empresas como agencias digitales, que se desarrollarán en el siguiente capítulo de la investigación, han tomado medidas de carácter jurídico para sancionar aquellas compañías que violen la privacidad de sus ciudadanos y distribuyan sus datos sin su consentimiento. El camino optado por la institucionalidad europea está orientado hacia el uso de la tecnología facilitando las tareas del ser humano y favoreciendo los intereses comunes. La Carta de Derechos Digitales de la UE busca establecer un límite que garantice la privacidad de los ciudadanos europeos que posean su información privada en bases de datos estadounidenses, así como un intento a la regulación y distribución de contenido digital

por parte de las empresas, y el uso que estas pueden efectuar de los registros digitales de los usuarios (Piñar, 2021).

El artículo 8 de la Carta establece que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. (...) Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. El respeto de estas normas estará sujeto al control de una autoridad independiente. (Carta de Derechos Fundamentales de la Unión Europea, Artículo 8. 2019).

### *1.3 Capitalismo de Vigilancia.*

La presente investigación parte, conceptualmente, de aquello planteado por Shoshana Zuboff como capitalismo de vigilancia, siendo este el concepto central de la investigación, y aquel que determina el comportamiento de los Estados y las variables relevantes para el propósito del proyecto. La literatura existente al respecto aborda una gran cantidad de información referente a diversos temas, pero es limitada en otros. Existen diversos consensos generales con respecto a las dinámicas al interior del ciberespacio, al traslado de las dinámicas capitalistas a las plataformas a partir de los modelos de negocio, y de las políticas existentes que moldean la realidad de las relaciones entre estados a nivel digital.

El capitalismo de vigilancia de Shoshana Zuboff (2013) se comprende como la mercantilización de datos personales, es decir, un proceso que se da a partir de múltiples reacciones y actores en el plano digital. En otras palabras, la mercancía, el objeto mediante el cual se genera la riqueza y el proceso de acumulación, se convierte en los datos personales de las personas, los usuarios. Por ende, es pertinente elaborar el concepto desde las corrientes constructivistas, particularmente el constructivismo moderado.

Los hechos expuestos sacaron a la luz un nuevo modelo predominante en los negocios, en el comercio y en la esfera política. La autora Shoshana Zuboff define como Capitalismo de Vigilancia, la ‘mercantilización’ de los datos personales, es decir, la utilización de la información personal depositada en medios digitales, con fines comerciales, capitalizables.

El capitalismo de vigilancia es también el resultado de una serie de procesos e interacciones dadas en el plano de lo digital, que derivan en la creación de nuevos actores, nuevas reglas, y nuevos intereses a satisfacer, donde la construcción del sistema, como se verá más adelante, está en constante crecimiento a partir de la información proporcionada por los usuarios. La actividad en el plano virtual de los usuarios es el elemento que permite la construcción de estructuras capitalistas, enfocando al usuario como el principal producto, desde sus datos personales, hasta los patrones de comportamiento que posteriormente son utilizados para construir un prototipo de consumidor ideal.

Zuboff (2019) ofrece un panorama del capitalismo y el mercado en el marco de la era digital donde el modelo es 'invertido' en cierta medida, dando lugar a los datos y la información como productos de intercambio monetizables, y no de bienes o productos tangibles. Las dinámicas de comercio y acumulación alrededor del capitalismo sufrieron los cambios de la evolución digital, creando nuevas corrientes e interacciones en el ciberespacio. Entre estos, el sistema, al igual que en varios puntos de la historia, se vio en la necesidad de adaptarse al cambio, y traer consigo una nueva fase en la cual los datos son la columna vertebral de los sistemas comercial y político. El desarrollo del ciberespacio ha provocado que las dinámicas capitalistas se trasladen al terreno digital, donde los negocios son mucho más rentables.

Otros autores afirman que estas dinámicas de acumulación provienen desde los años 70, cuando el modelo capitalista comprendió la digitalización como un propulsor de una sociedad que satisficiera sus necesidades de consumo a partir de lo ofrecido por el mercado global, bajo una identidad creada a partir de la digitalización (Jiménez. 2020); (Rendueles. 2020). A partir de esto, el individuo del futuro depende de la IA (Inteligencia Artificial) para realizar sus actividades, y a su vez, la IA depende de la información del individuo, presentada digitalmente como *metadatos* para predecir comportamientos y ofrecer solución a estas necesidades.

Del constructivismo es posible extraer diferentes definiciones de la literatura. Teóricamente, el constructivismo plantea la realidad como una interpretación *construida* a partir de las experiencias, interacciones y esquemas de pensamiento y valores de un individuo (Peiró. 2021). De acuerdo con esto, el individuo no es forjado por su entorno y su contexto, sino por

valores y características internas a este. Jean Piaget (1952), como uno de los principales autores de la teoría constructivista enfatiza en la importancia del desarrollo cognitivo en los primeros años, al ser el infante quien forja su realidad a partir de su aprendizaje. Esta teoría fue desarrollada principalmente en el ámbito educativo, sin embargo, es competente a una escala mayor y gracias al desarrollo teórico de diversos autores, en el campo de las RRII.

En este ámbito se desarrolla el constructivismo desde un Sistema Internacional sustentado con base en las experiencias sociales, culturales, históricas, entre otras, de los actores que hacen parte de él (Medina, 2014). De esta forma, y similar al individuo, los Estados se desarrollan a partir de las experiencias e interacciones de los elementos que lo componen, y crecen en la medida que construyen su realidad a partir de las relaciones, en este caso, con otros Estados y otros actores internacionales.

Esta teoría permite entender el componente discursivo, que es en últimas, la columna vertebral del contenido distribuido en redes sociales y aquello que permite la construcción de perspectivas y opiniones que derivan en la afinidad por determinados programas de gobierno y partidos políticos. Esta teoría parte de las ideas y su papel en el Sistema Internacional (Ayala. 2018) y, por lo tanto, es relevante a la hora de comprender el componente axiológico, no solo de los consumidores y a su vez votantes, sino el de los partidos políticos, la UE y empresas como Facebook, además de otras agencias reguladoras de contenido y de distribución de datos personales en el contexto del contenido digital.

Según Tah (2018), en las RRII, la perspectiva constructivista ofrece un escenario donde las estructuras del Sistema Internacional moldean los intereses y valores de aquellos que son parte de él, guiando su comportamiento de forma recíproca en las relaciones con otros actores. Específicamente, la corriente del constructivismo denominada constructivismo moderado, considera la construcción de la realidad y experiencias del individuo a partir de estímulos, sin dejar de lado los factores de una realidad externa establecida. Para autores como Alexander Wendt (1999) el entramado del Sistema Internacional constituye una serie de ideas compartidas de las cuales derivan los intereses de cada Estado, que a su vez están conformados por las experiencias y realidades compartidas de sus propios contextos.

En ese orden de ideas, es posible establecer en un primer momento, que las relaciones entre EE. UU. y la UE se han construido sobre una base ideológica y un conjunto de valores compartidos que han permitido el desarrollo de una buena interacción a lo largo de la historia reciente, producto, además, de experiencias históricas compartidas, cooperación en conflictos que derivaron en construcción mutua de instituciones, como lo fueron la Segunda Guerra Mundial y la Guerra Fría; creación de sistemas, etc. Partiendo de los valores de la democracia liberal y el sistema capitalista, ambos bloques han cooperado para la difusión de estos valores, a través de la ayuda mutua y los planes de desarrollo hacia otros Estados y los programas que garantizan la satisfacción a los intereses en común, ambas acciones han construido una relación de estrecha confianza.

En materia digital, las visiones de Estados Unidos están mayoritariamente orientadas al comercio, dada la ideología y los valores construidos a partir de la realidad de los creadores de las plataformas, que a su vez moldean su forma de actuar hacia el exterior (Cerrillo Garnica, 2020). La UE por su parte, no posee un porcentaje tan significativo en la participación y desarrollo de plataformas y compañías digitales como el de su contraparte, pero ha desarrollado en los últimos años un sistema de legislaciones encaminadas a proteger los valores de la libertad individual, incluyendo en esto el derecho a la privacidad, siendo líderes en materia de regulaciones para prevenir los robos de datos y la recolección no autorizada (Piñar, 2021). Lo anterior es el panorama de lo que se desarrolla como capitalismo de vigilancia, un concepto que surge a partir de las dinámicas comerciales sobre las relaciones en el ciberespacio.

### *1.3.1 Facebook y el Capitalismo de Vigilancia*

Las plataformas digitales expresan las dinámicas de este sistema a partir de su modelo de negocio, siendo una compañía cuyos ingresos se basan en la publicidad en casi que la totalidad y, como publicidad digital, los datos son el objeto de valor que permite dirigir anuncios específicos. El modelo económico monetiza los datos de los usuarios, y esto es posible únicamente gracias a la actividad e interacción de los usuarios con el contenido

digital. De igual manera, las relaciones entre actores como Facebook, Google y demás plataformas con los Estados, operan en el ciberespacio bajo principios diferentes a las relaciones del mundo físico y están estrechamente ligados a los intereses económicos de las empresas digitales, convirtiendo a estas compañías en intermediarios y proveedores de los datos, que son la mercancía bajo la cual se generan ganancias.

En el caso de Facebook, el modelo de negocio no menciona la recolección y venta masiva de datos, ni la manipulación con fines comerciales, ni la influencia e incidencia en procesos electorales; sin embargo, éste presenta las claves para entender no solo el funcionamiento de Facebook como compañía, sino su papel en el sistema capitalista de vigilancia. Ver anexo no. 1. E

El mecanismo de Facebook de publicidad dirigida representa un 98% de los ingresos de la compañía, y esta a su vez, se presenta a sí misma como un espacio o plataforma para el libre desarrollo del comercio en línea. La propuesta de valor de Facebook incluye además un método innovador en cuanto a publicidad, y es la posibilidad de distribuir contenido preciso a partir de las preferencias del usuario, y así garantizar mayores ventas y actividad digital (Audenaert. 2020). El enfoque publicitario de Facebook está encaminado, según su CEO Mark Zuckerberg (2019) a permitir la distribución de productos y servicios de manera gratuita a través de medios pagos de publicidad. A lo anterior, Zuckerberg ha enfatizado:

Nuestro objetivo es ayudar a la gente a compartir y conectarse más, (...). Los enlaces engañosos (clickbait) y otros contenidos basura pueden mejorar la interacción con la plataforma a corto plazo, pero sería una estupidez por nuestra parte mostrar estos contenidos de forma intencionada porque no es lo que quieren las personas. (2019).

Es posible ver como la compañía hace énfasis en la transformación de la red social a través del contenido dirigido, optimizando las publicaciones para mejorar la experiencia del usuario. Retomando a Zuboff, esta experiencia es precisamente el material comercializable de la compañía. Los datos como producto de compra y venta se recopilan mediante la experiencia del usuario y el carácter público de publicidad de la plataforma resultan en la monetización de las actividades del usuario en la red social. Esta actividad cumple una

función en el ciclo del capitalismo de vigilancia, al alimentar patrones de comportamiento mediante los cuales la IA predicen decisiones a futuro, además de un perfil exacto del usuario, lo cual incentiva a la plataforma a distribuir el contenido adecuado para mantener el ciclo de consumo (Zuboff, 2013).

### *1.3.2. El Ciberespacio*

Se analizará el concepto de *ciberespacio* como punto de partida para la construcción de las relaciones entre ambos bloques, su trayectoria y componentes y su convergencia con el Capitalismo de Vigilancia. Posteriormente, se explicarán los actores estadounidenses pertinentes para la presente investigación, empezando por el gobierno, particularmente la Agencia Nacional de Seguridad (NSA), y las plataformas digitales, específicamente Facebook y cómo su modelo de negocio en conjunto con las legislaciones estadounidenses posteriores a los atentados del 11 de septiembre, integran las dinámicas del capitalismo de vigilancia y construyen este sistema a partir de los datos.

Los Estados Unidos y sus empresas aprovecharon la rentabilidad de los modelos de negocio virtuales, y, aprovechando los datos de los usuarios, combinaron las estrategias comerciales y políticas para establecer la vigilancia como la base del sistema. Además, securitizaron la digitalidad mediante los datos, bajo un discurso de protección y no de vigilancia. De lo anterior, de la consolidación de las primeras estructuras privadas de Internet, sumado a los continuos avances tecnológicos, deriva lo que se conoce como *ciberespacio*, sin embargo, el interrogante con respecto a su carácter y tangibilidad es aún difuso.

El terreno digital que constituye una realidad paralela, un nuevo conjunto de reglas e instituciones que rigen el campo relacional, y nuevas dinámicas de comportamiento. Aitor Jiménez y César Rendueles (2020), establecen a la comunicación como el punto de partida del ciberespacio y las políticas tecnológicas, particularmente en tres momentos claves para la historia y el desarrollo de Internet, especialmente en la década de 1990. La aparición de la World Wide Web (WWW) marca el inicio de lo que los autores denominan la privatización de las estructuras de Internet. (Jiménez Gonzales, 2020, pp. 97); (Rendueles Menéndez, 2020,

Pp. 97) La segunda, es el nacimiento de la primera plataforma exitosa como primer navegador masivamente utilizado (Netscape), y con ella las plataformas como el terreno para las relaciones del ciberespacio, que se desarrollarán más adelante; y el tercero, las leyes adoptadas por el gobierno de Bill Clinton para extender las nuevas plataformas y avances tecnológicos virtuales, a todas las esferas de la población. De esto, Pérez Martínez (2013) en el estudio de la comunicación moderna establecen:

El ciberespacio no es una imagen reciente. No es medible y no podemos acceder a él a través de nuestros sentidos. A diferencia del espacio radioeléctrico, en la Red existen interacciones, que, aunque creadas y generadas por la programación realizada por seres humanos, tiene comportamientos característicos producto del uso de algoritmos y programas que obtienen información de los datos generados por los internautas. (p.2)

Así mismo, los actores (entendidos como aquellos individuos, colectivos, organizaciones, instituciones, Estados, etc., que interactúan en el ciberespacio) y sus métodos de interacción no son los mismos que en el mundo real. El ciberespacio cuenta con su propio conjunto de reglas, y, de la misma manera en que las disciplinas han construido bases teóricas que expliquen los fenómenos de las interacciones sociales, a su vez, existen bases teóricas para la construcción del mundo virtual (Pérez Martínez, 2013).

El Ciberespacio es, sin embargo, otra arena. Creada a través de la innovación tecnológica, son eventos que permiten a los usuarios conectar en actividades conducidas sobre campos electrónicos cuyos dominios espaciales trascienden las restricciones gubernamentales, sociales y económicas. (...) El ciberespacio es el resultado de las actividades de un grupo grande de individuos (primera imagen) operando bajo las reglas del Estado (segunda imagen), la utilización y omnipresencia del ciberespacio son transnacionales en escala y alcance (tercera imagen) (...) (Choucri, 2012, p.42).

El segundo momento clave en la historia digital, mencionado previamente, hace referencia al nacimiento de las plataformas, componente clave para entender las dinámicas digitales.

Por plataformas se entiende como el espacio donde dos o más grupos interactúan entre sí (Srnicek. 2016). Esto quiere decir que las plataformas son el terreno dentro del ciberespacio donde se llevan a cabo las interacciones que dejan residuos digitales y la infraestructura para la recolección masiva de información (Pérez. 2018).

El funcionamiento y las dinámicas del ciberespacio son posibles gracias a los sistemas de Inteligencia Artificial (IA) ideados por el ser humano. La inteligencia artificial, aseguran autores como Amy Webb (2019) no es un ordenador o un sistema físico que toma decisiones independientes, sino una serie de procesos que toma decisiones a partir de las interacciones humanas para establecer un patrón de comportamiento y así tomar una decisión a partir de estos procesos aprendidos. De igual manera, la literatura asegura que los mecanismos de ‘imitación’ presentes en las IA, son el resultado de la programación de sus creadores, los propósitos de estos y especialmente, su corriente ideológica y conjunto de principios (pp 67, 2019).

Para el caso estadounidense, los creadores de lo que Webb denomina la GMAFIA (Google, Microsoft, Amazon, Facebook, IBM, Apple), provienen del Silicon Valley, y sus creadores provienen de contextos similares, educación orientada hacia los mismos valores y principios, y una ideología clara. El rol de esta ideología, de acuerdo con el constructivismo, es el elemento que define las dinámicas relacionales en el ciberespacio y que construye la realidad del usuario, las empresas y los Estados, mediante elementos discursivos; el sistema continuamente construye realidades de acuerdo con los intereses de los actores.

Estos intereses, en resumen, parten inicialmente de la formación educativa de las cuales no solo Zuckerberg, sino las cabezas de las demás compañías Big Tech, tuvieron. El ambiente educativo estuvo caracterizado por valores comunes dentro de las universidades; a esto Amy Webb (2021) lo define como tribus de IA, como la Inteligencia Artificial está orientada hacia el interés de sus creadores. Además, la autora menciona como parte del contexto educativo de los gerentes, la creciente necesidad por establecer mejores parámetros de inclusión, no solo en sus compañías, sino en su contenido. Estos problemas identitarios, de género y demás, se tradujeron posteriormente en el ámbito laboral, concluyendo en la consolidación de un

sistema de valores ‘humanista’ y en busca de solucionar problemas de los menos favorecidos. Este conjunto de reglas y valores se tradujo en el ciberespacio también.

En la disciplina de las RRII, el ciberespacio como un nuevo terreno para las interacciones ha presentado ambigüedades en los intentos para descifrar sus características y su funcionamiento. Uno de los principales dilemas según diversos autores radica en la complejidad de las relaciones gracias al carácter cambiante y diverso del ciberespacio (Vila Seoane, 2019); (Saguier, 2019). De acuerdo con esto, la construcción per se del ciberespacio ya es un acto político, y la política es intrínseca al sistema digital (Choucri, 2012). El alcance tecnológico se expandió más allá de las Big Tech americanas, y en un espacio donde las interacciones están encaminadas a la persecución de intereses, comerciales particularmente; las empresas de otros países y sus gobiernos han desplegado todo un arsenal digital para hacer parte de un sistema extremadamente rentable (Webb, 2020).

La política al interior del ciberespacio, al igual que en el mundo real, resultó en el nacimiento de corrientes ideológicas con respecto al manejo de la información. No es únicamente el capitalismo de vigilancia, la corriente ‘ideológica’ que rige el ciberespacio. Las dinámicas de acumulación capitalistas se ven igualmente reflejadas en el ciberespacio al igual que sus contrapartes. Este es un nivel superior en el marco de las interacciones en el ciberespacio ya que involucra capital, Estados y sociedad (usuarios, empresas, organizaciones), en un contexto de desarrollo digital complejo y avanzado.

Siendo los datos y los registros de actividad la materia prima capitalizable en este sistema, es lógico que existan corrientes orientadas a la regulación, control y análisis crítico del comportamiento de corporaciones y el manejo que estas le dan a los datos en materia de privacidad, y protección de los derechos. A esta corriente se le conoce como *sociología crítica digital*, el estudio de las interacciones humanas digitales en un contexto cotidiano (Callejo Gallego, 2017), y es complementada por las consternaciones existentes frente a la protección de datos, la garantía de la privacidad y la regulación a las capacidades comerciales de las grandes corporaciones digitales, es decir la regulación al sistema extractivo fundamentado en la distribución masiva de datos. Europa en particular, ha adoptado fielmente esta corriente.

### *1.5 Estado del Arte:*

Como fue posible evidenciar después de haber establecido las previas bases, la literatura ofrece amplias definiciones sobre el desarrollo del capitalismo de vigilancia, concepto que fue planteado por Shoshana Zuboff y que ha sido analizado y reinterpretado. Adicionalmente, aquellos otros conceptos que convergen con la vigilancia, como lo son el ciberespacio y las plataformas, cuentan con diversos análisis desde la literatura analizada. Es importante mencionar que la mayoría de los autores no establecen relaciones entre los conceptos, sino que los abordan por separado o dedicándose únicamente a un concepto en particular, motivo por el cual se dificulta encontrar relaciones preexistentes entre los conceptos mencionados.

Del ciberespacio como concepto es posible encontrar diversas definiciones y maneras de comprenderlo, existiendo diversas teorías con respecto al desarrollo del ser humano como individuo en el terreno digital, al igual que las dinámicas capitalistas. Concretamente, respecto al capitalismo, a nivel digital existen estudios de diferentes corrientes como las mencionadas previamente, capitalismo de plataformas, capitalismo digital, sociología digital, entre otros. De los primeros, autores como Imanol Zuberó (2018), y Evgeny Morozov (2018) son de los primeros en mencionar modelos de negocio y extracción en el plano digital, estableciendo patrones principalmente en aquellos países que sostienen el mayor control de plataformas y compañías digitales. Otros como Javier Rivera (2018) exponen desde otra perspectiva, cómo el traslado del sistema de acumulación al ciberespacio representa un posible peligro para los sistemas políticos democráticos, las libertades individuales y, en algunos casos, la soberanía y las capacidades de los Estados (Rivera, 2018. Pp. 79-89).

Centrando al ciberespacio en materia de capitalismo digital, la literatura presenta diversos análisis al fenómeno, destacando que todos estos derivan de las investigaciones de Zuboff y son interpretaciones de la vigilancia en un sistema de acumulación. Estudios como los de Emilio Manjarrez Chavarriaga (2016) ejemplifican las dinámicas del capitalismo de vigilancia en el modelo de negocio de Facebook, como se pudo evidenciar en secciones previas, a partir de las implicaciones de estas en la vida civil y la política internacional (de

forma limitada para regiones como América Latina) y centrándose en el funcionamiento y los efectos de este sistema, en el individuo como el usuario y principal consumidor (o producto) en las plataformas.

En la disciplina de las RRII, la literatura abarca una gran cantidad de teorías y conceptos aplicados al ciberespacio. Respecto a la relevancia del capitalismo de vigilancia sobre las RRII es posible encontrar estudios con respecto al impacto de las dinámicas de espionaje y extracción masiva de datos en materia de política exterior. Autores como Ricardo Montaña (2018), o Tulio Rosembuj (2019) parten de los planteamientos de Shoshana Zuboff para analizar el impacto de estas interacciones en la política exterior de diversos países. Los estudios más específicos en esta materia se enfocan en el redimensionamiento de la política de seguridad y la política exterior concretamente de EE. UU. a partir de la construcción de las visiones de seguridad que involucran ciber política (Montero Montano. 2016); (Ybarra Martínez, 2016). Con respecto a la dirección tomada por la UE es posible encontrar diversos análisis con respecto a las acciones jurídicas que adoptó el organismo en los años posteriores a las investigaciones y revelaciones; en concreto, existe una falta de literatura que analice y aborde a profundidad y desde el componente discursivo y constructivista, las reacciones inmediatas de la UE. Las fuentes restantes establecen análisis descriptivos con respecto a casos concretos de espionaje que involucre tanto a EE. UU. como a la UE y el carácter general de las relaciones, más allá de momentos de tensión y posible crisis, desencadenados a partir de la información propiciada por Edward Snowden.

## **Capítulo 2: La Respuesta Europea**

### **De la efectividad de un organismo interestatal frente a actores no-estatales**

La complejidad de las relaciones se analizará desde la recopilación de prensa y documentos oficiales de los gobiernos, con el fin de comprender las bases relacionales y los componentes que conforman la construcción y evolución de la relación entre EE. UU. y la UE. La base epistemológica de la metodología es interpretativa, esta comprende la posición del investigador como sujeto participante en la construcción de una realidad, que no se puede distanciar de las limitaciones conceptuales que esto implica y a la vez accede a la información mediante el sesgo de su propia realidad. En el contexto de la presente investigación, el investigador es además usuario y hace parte de las dinámicas digitales que construyen la realidad individual, pero a la vez participa en la realidad colectiva de las relaciones en el ciberespacio.

A partir de los hechos, este capítulo busca comprender la respuesta de la UE a las revelaciones de espionaje y el quebrantamiento de la confianza y la traición a los valores que generó unos discursos en un primer momento, orientados a resaltar y reconstruir los ideales bajo los cuales se establecieron los vínculos entre ambos bloques. Es esto por lo que, para un análisis profundo del carácter de las reacciones de la UE frente a la problemática, deben ser abordados bajo la revisión extensa de bibliografía y prensa, entre artículos, entrevistas, columnas, etc; además de documentos oficiales, y comunicaciones tanto verbales como escritas por parte de los dirigentes de ambos bloques, que demuestren de manera concisa, los cambios que sufrieron las relaciones entre los dos actores, a partir del juicio de la opinión pública, mediática y testimonios de los mismos actores involucrados.

En primer lugar, es necesario delimitar los actores que forman parte del conflicto, su participación, valores e intereses para comprender como la UE estableció una estrategia a partir de su realidad. Lógicamente, se tomará en cuenta a la UE como organismo político, siendo el Parlamento Europeo y la Comisión, los entes que llevan a cabo las respectivas acciones; de igual manera, dentro de la UE se ven involucradas en eventos concretos que se

mencionarán a continuación, las agencias de seguridad de Alemania, Francia y el Reino Unido. La respuesta europea está encaminada a lograr la adaptación de los actores estadounidenses al marco legal y conductual de la UE, es por ello por lo que, del lado estadounidense, se tomarán en cuenta al gobierno en cabeza primero de Barack Obama, posteriormente de Donald Trump, a la Agencia de Seguridad Nacional (NSA), y a Facebook.

Delimitar los actores establece, además, las similitudes y diferencias, no solo en los valores e intereses de cada bando, sino en cuanto a los resultados a partir de las revelaciones de Edward Snowden, en materia de producción mediática, reacción de la opinión pública y de miembros oficiales de los diferentes gobiernos. El propósito de esto viene siendo comprender a profundidad la respuesta europea, y para ello es de gran importancia establecer nuevamente las diferencias en cuanto a la construcción institucional y las relaciones entre los medios, y los gobiernos.

Es por este motivo que, previo a avanzar en el desarrollo de los hechos, se presenta a continuación, la primera de dos figuras. La **figura 1** presenta una tabla que establece los actores principales y sus medios de mayor relevancia, entre otros, aquellos que más seguimiento han hecho al caso, la versión que estos dieron y su nivel de influencia sobre la respuesta, en este caso, de parte de la UE.

**Figura 1: Medios europeos.**

| <b>País</b> | <b>Medios Relevantes</b> | <b>Contenido</b>  |
|-------------|--------------------------|---|
| Reino Unido | BBC<br>The Guardian      | Informe general y bastante completo sobre los casos de espionaje estadounidense y las revelaciones de Edward Snowden, quien decidió este como el principal medio de difusión. |

|          |                               |   |
|----------|-------------------------------|---|
|          |                               | Adicionalmente The Guardian realizó importantes investigaciones vinculando al gobierno británico con la vigilancia estadounidense.  |
| España   | El País                       | El diario El País hace un seguimiento completo desde la filtración de información de Edward Snowden hasta casos concretos que incluyen Estados miembros de la Unión Europea espiando a otros gobiernos, principalmente Alemania, y cooperando con Estados Unidos. |
| Alemania | DW<br>Der Spiegel<br>Die Zeit | Similar a los medios de sus países vecinos, los medios alemanes llevaron a cabo un estudio completo evaluando los excesos de las políticas de   |

|        |            |  |
|--------|------------|--|
|        |            | seguridad y vigilancia estadounidenses en el continente. Sin embargo, demostraron que el gobierno alemán era de los principales objetivos del espionaje, y por lo tanto dedicaron sus reportajes a este enfoque. |
| Italia | L'Espresso | Sus reportajes se dieron en cercanía con la fuente primaria de las revelaciones y, con ayuda de esta lograron liberar los primeros avances de información.   |

Como se mencionó en el primer capítulo, la UE y EE. UU. comparten experiencias, historia, intereses y valores mutuos; discursiva y políticamente son bastante cercanos, en el sentido de que son democracias construidas a partir de principios de respeto por la libertad y la igualdad, constan de construcciones políticas similares, sistemas electorales compartidos y, en la historia reciente, experiencias históricas compartidas que derivaron en procesos e iniciativas de construcción y cooperación mutua. Las instituciones europeas y americanas están encaminadas a la protección de los intereses de la democracia occidental, es por ello por lo que, las primeras reacciones se producen en el marco de la duda por parte de los europeos, como se evidencia en la anterior tabla.

## 2.1 Respuesta mediática

A partir de la **figura 1** es posible evidenciar varios elementos en cuanto a la respuesta mediática por parte de la UE. En primer lugar, existen dos concepciones con respecto a la injerencia de compañías Big Tech en la privacidad de ciudadanos europeos y políticas de los países. Por un lado, diarios como BBC y El País hicieron un extenso seguimiento al tema a nivel general en cuanto a las implicaciones para la UE como bloque conjunto. A su vez, The Guardian reveló casos concretos como la posesión de información privada proveniente de las telecomunicaciones, de millones de habitantes, por parte de la NSA. Lógicamente estos tres medios hacen énfasis en sus países de origen, respectivamente Reino Unido y España.

Medios como la Deutsche Welle (DW) enfocaron su respuesta en las implicaciones de la vigilancia para Alemania, siendo este país uno de los principales afectados. Los medios alemanes además han hecho seguimiento a casos concretos no solo en Alemania sino en Dinamarca. Los medios europeos principales han hecho énfasis en la construcción histórica de las relaciones entre ambos continentes desde el establecimiento de valores comunes.

Desde otro aspecto, medios menores han además mencionado, desde una óptica institucional (respuesta que se explicará en las secciones posteriores), las implicaciones para la solidez de la UE con respecto al verdadero poder que tiene el bloque para contrarrestar las agresivas medidas de vigilancia que impone EE. UU. Entre estas, el diario El País, DW, mencionan el caso de países menores en la UE como son los Balcanes, donde existía una gran dependencia por las iniciativas de proyectos de conectividad y tecnología que ofrecía Facebook, entre otras compañías; y quienes, por cuenta de los escándalos producidos a partir de las revelaciones de Edward Snowden, decidieron acudir a mecanismos legales (al igual que Alemania) para frenar las violaciones a la privacidad.

Uno de los periódicos de mayor relevancia en Europa es el francés, Le Monde, quienes realizaron un gran reportaje refiriéndose al caso, titulado *The NSA and America's Madness*. El reportaje además de mencionar lo que otros medios constantemente mencionaron (el caso Snowden), realizó un seguimiento general a la vigilancia de la NSA que sacó a la luz varios

elementos. Con respecto a la relación EE. UU-UE, el artículo enfatiza inicialmente en conversaciones entre dirigentes, Macron y Merkel particularmente, donde se establece una postura crítica ante las actuaciones de la NSA.

“Escuchar las conversaciones privadas entre Merkel y Macron está completamente desligado a la lucha contra el terrorismo (...) El hecho de que a estas estructuras de poder se les permita existir en el corazón del gobierno estadounidense es profundamente preocupante. Nos gustaría saber si estas prácticas son producto de servicios dejados a sí mismos y en ‘piloto automático’ o si siguen ordenes de los más altos niveles de poder (Le Monde, 2015).

Posterior a poner en duda las verdaderas intenciones del gobierno estadounidense, en un ámbito claramente político, en otro artículo, Le Monde informa sobre las intenciones de Edward Snowden de cooperar con empresas europeas para proteger la información. El medio francés tiene un énfasis claro sobre la influencia en la política francesa. El reportaje no se relaciona con las estructuras económicas que componen al capitalismo de vigilancia, pero si pone en duda las intenciones del uso de datos personales.

De medios como la BBC (hay que recordar que Gran Bretaña hacía parte de la UE para el año 2014), enfocaron sus primeros reportajes en la investigación a actores exclusivamente estadounidenses. El reportaje principal de la BBC del caso, *Edward Snowden: Leaks that exposed US spy programme* (2014), expone en detalle los diferentes componentes del programa de espionaje y vigilancia de EE. UU., desde la interceptación de llamadas, hasta cables de fibra óptica intervenidos tanto a civiles como a oficiales y agentes gubernamentales, casos que se analizarán en detalle a continuación, considerando que los primeros reportes, como el de la BBC, enfatizan en las implicaciones del espionaje para Estados Unidos. Es a partir de este punto que el Parlamento Europeo como organismo de la UE, adopta lineamientos que derivan en la implementación de medidas y regulaciones a las plataformas y al manejo de datos.

Este artículo al igual que otros diarios, hicieron un seguimiento completo al caso de del espionaje estadounidense, dedicando diferentes secciones dependiendo de las acciones cometidas por el gobierno de EE. UU. El escándalo inicial, como lo menciona el artículo, está ligado al reportaje de un medio italiano, L'Espresso, quienes, a través de Snowden, descubrieron la interceptación de inteligencia americana en las redes de fibra óptica del occidente europeo en el año 2013 (BBC, 2015). Ahondando más en el medio italiano, este además incluye una entrevista al primer ministro de la época, Enrico Letta, quien negó a los medios la presencia de vigilancia americana interceptando redes italianas (Reuters Staff, 2013).

Es en este punto donde la situación adquiere un carácter más complejo; por un lado, los medios británicos, italianos, franceses y americanos (como se verá más adelante) hacen un seguimiento relativamente exacto e imparcial del caso, sin embargo, la opinión política y la relación del cuerpo institucional con la prensa y los medios ofrece un panorama distinto. Los medios realizan una denuncia a partir de la creciente desconfianza entre múltiples actores, al también involucrar la inteligencia británica como un agente cooperador con EE. UU. para recopilar información de ciudadanos, en este caso italianos. El argumento del primer ministro se centra en la solidez legal del Estado italiano para prevenir injerencia extranjera en sus comunicaciones.

Por otro lado, y de acuerdo con el diario El País (2019), la periodista española Marta Peirano, establece el revuelo y la indignación como una reacción por parte de la sociedad. En el caso de la UE, las reacciones vinieron de parte de la opinión pública, siendo el foco de la indignación el hecho de los ciudadanos europeos de saber que su privacidad es constantemente violada por una potencia extranjera. Desde los primeros reportajes, la UE hace públicas sus primeras declaraciones y posición mediante el Parlamento Europeo. Estos iniciaron retomando los valores de las sociedades democráticas y estableciendo una postura clara en contra de la extracción de datos con fines de seguridad, ante esto, el Parlamento estableció:

“los sistemas de vigilancia masiva indiscriminada por parte de los servicios de inteligencia constituyen una seria injerencia en los derechos fundamentales de los ciudadanos” (Moraes, 2014).

A partir de esto, medios alemanes como *Der Spiegel* o *Süddeutsche Zeitung* (ver Anexo 2) mostraron interés en contactar con Edward Snowden y contemplar su versión de los hechos, a la vez de entablar conversaciones con EE. UU. posterior a la respuesta de estos. El acercamiento se produce en el marco del rechazo de EE. UU. a las revelaciones, generando que Snowden opte por colaborar con la justicia alemana antes que la estadounidense. El objetivo de estas investigaciones fue el esclarecimiento de los hechos y la protección a Edward Snowden ya que, inclusive permaneciendo en Europa, podía ser blanco de persecuciones por parte de agencias de seguridad. Los reportes, sin embargo, no concluyen inicialmente sobre el grado de responsabilidad de los miembros de la UE, pero si sobre una clara indignación y percepción de una fractura en los valores que construyeron la confianza y cooperación entre ambos bloques. Sin embargo, con respecto al futuro de Edward Snowden, el Parlamento Europeo tomó la decisión de no otorgar asilo a Snowden en caso de ser procesado, bajo el pretexto de que ese tipo de competencias dependían de cada país miembro, y no del bloque regional como tal.

Como fue posible evidenciar en los párrafos anteriores, los medios que mayor énfasis hicieron en el seguimiento y vigilancia entre miembros europeos, y en cooperación con EE.UU., fueron aquellos provenientes de Alemania. Alemania es, además, el país central de la UE, cuya privacidad se ha visto más vulnerada, de acuerdo con lo revelado por Snowden. Entre estos destacan la injerencia de la inteligencia británica, francesa y danesa (esta última en menor medida) en la recopilación de datos de ciudadanos alemanes con fines políticos y en la búsqueda de beneficios por parte de EE. UU. y las empresas tecnológicas.

Existe tanta solidez, por un lado, particularmente verbal, y un carácter difuso por el otro. Esta desconexión fue evidente en otro caso relacionado igualmente a los organismos de prensa británicos y las instituciones de este país. Como fue evidente en la **figura 1**, el medio británico The Guardian jugó un papel crucial en el reporte de las relaciones entre el espionaje estadounidense y su relación con las agencias de inteligencia británicas. Ante este reportaje,

y según un reporte de Andrew Osborn (2013), el gobierno británico empezó a ejercer grandes presiones sobre la prensa con el fin de desviar la opinión pública. El resultado provocó una reacción del organismo de prensa europeo ejerciendo presión sobre Gran Bretaña para proteger el periodismo independiente y la información de interés público. Además, al inicio del documento se habló de la FISA, mecanismo legal mediante el cual se regula la inteligencia a nivel internacional; esta Corte, de acuerdo con otro informe de The Guardian, permitió recopilación indiscriminada de datos al ‘no negarse a ninguna petición de esta índole’ (The Guardian, 2016).

A nivel general, es posible evidenciar las siguientes tendencias en los medios de comunicación europeos. Existe un relativo grado de imparcialidad en términos de reportajes (la mayoría de los medios no tomaron postura contra Snowden ni omitieron información de los casos), teniendo en cuenta que la mayoría de estos hacen seguimiento a las diferentes situaciones alrededor del caso, independientemente de su país de origen. Los reportes más grandes provienen principalmente de la BBC, proveniente de Reino Unido, con énfasis en las relaciones de inteligencia EE. UU-U. E y sus objetivos frente a países como Rusia y China. La BBC, sin embargo, no realiza un seguimiento de los casos en los cuales el gobierno británico se vio directamente involucrado, diferente de medios como aquellos provenientes de Italia, quienes, una vez expuesto el caso, acudieron directamente a miembros de la política, que, como se pudo ver en el caso italiano, negaron los hechos.

## *2.2 Respuesta de la UE:*

La respuesta de la UE se da en varios niveles, previamente se evidenció el nivel mediático ya que este es útil para comprender el cuerpo de la respuesta política, dado que es la opinión pública la que, en el caso europeo, trata la situación. A partir de estas investigaciones es pertinente establecer al individuo como punto de partida en el ámbito político, siendo estos el foco principal, la mercancía, y el centro de las operaciones en el capitalismo de vigilancia. Desde el individuo hay dos elementos a tratar, por un lado, la manera en la cual este se beneficia, en teoría, de que su información sea comercializada y el contenido sea selecto

estrictamente para satisfacer sus necesidades y facilitar su vida. A partir de las investigaciones periodísticas y las revelaciones de Edward Snowden, las implicaciones para el ciudadano europeo como individuo recaen en la vigilancia extrema y la manipulación política, eventualmente, los Estados moldeando y comercializando a sus ciudadanos. Lo anteriormente dicho es posible de evidenciar en las campañas del Brexit y la presidencia de Donald Trump, añadidas a las previas investigaciones periodísticas de vigilancia entre gobiernos aliados.

Como es posible evidenciar en este primer momento, la UE tomó acción verbal, el informe del Parlamento Europeo anunció medidas y acciones para contrarrestar la vigilancia estadounidense que serían ejecutadas posteriormente, a partir del creciente descontento en la población y la opinión pública, y a su vez, denunciando una ruptura de la confianza, pero sobre todo de los valores que constituyen Estados democráticos. Entre estas podemos encontrar una serie de declaraciones oficiales y comunicados, de los cuales se podrán ver algunos ejemplos a continuación:

Referente a la transferencia de datos y la violación de la privacidad, el informe del Parlamento Europeo establece:

Considerando que la transferencia de datos personales por parte de las instituciones, organismos, oficinas o agencias de la UE o por parte de los Estados miembros a los Estados Unidos con fines policiales en ausencia de garantías y salvaguardias adecuadas para el respeto de los derechos fundamentales de los ciudadanos de la UE, en particular los derechos a la intimidad y la protección de datos personales, conllevaría que dicha institución, organismo, oficina o agencia de la UE o dicho Estado miembro sean responsables, en virtud del artículo 340 del TFUE o de la jurisprudencia establecida por el Tribunal de Justicia de la UE(29), de infracción del Derecho de la UE, que incluye cualquier infracción de los derechos fundamentales consagrados en la Carta de la UE; (Parlamento Europeo, 2013).

Las decisiones a raíz del informe del Parlamento Europeo están encaminadas hacia el enfoque jurídico en la protección de los datos y distribución de los datos, de esto, el resumen de la

Comisión Europea con respecto a la declaración de derechos digitales establece el enfoque de protección de datos personales. De la misma forma, hace alusión al *Pilar Europeo de Derechos Sociales* a partir de iniciativas de incluir los derechos digitales como derechos fundamentales en la UE (Comisión Europea, 2022).

En el ámbito legal, las iniciativas también abrieron la puerta a la adaptación a la era digital partiendo de las bases morales y legales que constituyen a la UE. Entre estas regulaciones a sus ciudadanos y empresas, se establece lo siguiente en el artículo 8 de la Carta de Derechos Digitales:

Cualquier individuo en la Unión, cuyos datos personales estén siendo procesados dentro de la Unión o donde los procesados estén relacionados a el ofrecimiento de bienes o servicios en la Unión o controlando su comportamiento dentro de la Unión, están protegidos en el marco legal adoptado por la Unión a través del artículo 8 de la Carta, y el artículo 16 del Tratado de Funcionamiento de la Unión Europea (Carta de Derechos Digitales. Artículo 8, 2019).

Lo anteriormente visto hace parte de los intentos europeos de contrarrestar la vigilancia estadounidense a raíz de las revelaciones. El informe del Parlamento Europeo es preámbulo para el conjunto de legislaciones conocida como la Carta de Derechos Digitales y el Reglamento Europeo de Protección de Datos, parte de la declaración de Principios y Derechos digitales, cuyo enfoque está en el desarrollo de las competencias y habilidades de la UE en el marco de un mundo digitalizado. Es también, en el marco del capitalismo de vigilancia, un intento por controlar el esquema de acumulación y mantener los datos, la mercancía, en manos de los individuos que los proporcionan. Esto supondría la adaptación de las empresas que entren bajo este marco legal, a respetar la privacidad y a no transformar la información en mercancía.

Por último, cabe destacar que, si bien el Parlamento Europeo criticó fuertemente a las agencias de seguridad estadounidenses por el quebrantamiento de la confianza y los valores mutuos, el organismo también adoptó medidas que se ajustaran a los intereses de seguridad internacional de EE. UU. y las medidas adoptadas a partir de la Ley Patriota. A partir de la

cooperación, la UE propone en un primer momento estrategias de comunicación para facilitar el intercambio de datos por parte de Europa hacia EE. UU., que estén relacionados con cuestiones de seguridad. Esto resulta producto de una clara debilidad en materia digital, de la UE frente al país norteamericano, y, por ende, la existencia de una dependencia debido a las amenazas externas en materia de ciberseguridad, que enfrentan los europeos constantemente (Quintana. 2014).

Comparativamente, la desventaja europea sobre la americana empieza por la tenencia de las bases de datos y la información que se almacena en estas, que, para el caso, EE. UU. cuenta con un número significativamente mayor de bases de datos que Europa. De igual manera, las grandes plataformas y compañías digitales (GMAFIA mencionada en el capítulo anterior) fueron establecidas en EE. UU. como base y operan de acuerdo con las condiciones y el contexto en el que se encuentran.

A nivel práctico, se evidenció una iniciativa conjunta para mantener los valores por parte de la UE, sin embargo, se mencionó una debilidad digital en comparación con EE. UU., esto se evidencia en los continuos intentos de espionaje, ya no desde la NSA directamente, sino entre gobiernos europeos, como se observó en los reportajes, derivando en la vigilancia continua a funcionarios además de civiles. El triunfo del Brexit en el año 2016 marcó un punto de quiebre puesto que expuso el verdadero carácter del uso de la información personal y, habiendo sucedido posterior a la respuesta de la UE, demostró que la mercantilización de los datos puede encarnar en cualquier modelo a pesar del blindaje legal e institucional.

### *2.2.1 Derechos Digitales y reformas de la UE.*

A diferencia de EE. UU., donde los intereses de las compañías digitales están poco ligados a los intereses del Estado (Webb. 2019); en la UE, por el contrario y a raíz de los escándalos, el enfoque está orientado a prestar un servicio a la comunidad y proteger la privacidad de esta, a la vez que se avanza en la cooperación entre entidades gubernamentales que impulsen el desarrollo de los Estados en materia tecnológica, y no con fines acumulativos y extractivos priorizando la ganancia comercial. Esto explica el por qué tantos países desde la opinión

pública, hasta los mismos organismos políticos rechazaron con contundencia los acuerdos comerciales y las políticas de seguridad digital estadounidenses.

Como se mencionó brevemente, en el contexto de las alianzas con EE. UU., la UE accede a cooperar con EE. UU. para contrarrestar el espionaje y la vigilancia; en ese orden de ideas, la reacción de la UE busca incidir con el fin de reformar ciertos sectores en la política digital estadounidense, a la vez que coopera con otros para su beneficio. Esto supone la creación de programas sociales y políticas públicas que guían a la UE a integrar sus esferas alrededor de la digitalidad y el ciberespacio como servicios públicos. Con respecto a sus lineamientos, la vicepresidenta para Europa Adaptada, Margethe Vestager asegura en un comunicado que:

Queremos tecnologías seguras que sirvan para las personas y que respeten nuestros derechos y valores, también cuando usemos internet. También deseamos que todo el mundo esté capacitado para participar activamente en nuestras sociedades, cada vez más digitalizadas. Esta declaración nos ofrece un claro punto de referencia en materia de principios y derechos en el mundo en línea (Vestager. 2021).

La declaración ante la comisión y la formalización de los derechos digitales en la carta de derechos, fueron la respuesta jurídica, derivada de la respuesta social que se tomó a partir de los escándalos. A partir de este punto, y el periodo de tiempo que comprende la investigación, los datos presentados están relacionados a casos concretos de espionaje, discursos y testimonios, que generaran fricciones entre EE. UU. y la UE, partiendo de las reacciones de estos últimos. Estos involucran en gran medida a Alemania dada la relevancia y el liderazgo económico que para la hegemonía de EE. UU podía significar una amenaza, hechos que fueron denunciados por países como Bélgica. El escándalo de Cambridge Analytica además estableció un punto de crisis en la diplomacia europea, al ser también partícipes del espionaje las agencias de seguridad de países como el Reino Unido, nuevamente, por el interés en las empresas y el comercio de sus aliados y aparentemente competidores.

### *2.3 Consideraciones Generales*

A partir de lo anteriormente visto y en manera de evaluación, la UE demostró un cierto grado de solidez institucional para actuar con referente a la injerencia de EE. UU. y sus empresas. Los organismos de la UE como el Parlamento Europeo coordinaron con los organismos legales para Fue posible evidenciar una respuesta mediática rápida considerando la alta difusión de los reportajes vistos, pero una demora de un año para que la UE diera una respuesta a nivel institucional que permitió la publicación de comunicados. A pesar de los desacuerdos iniciales entre los Estados miembros, se establecieron legislaciones y la Carta de Derechos Digitales, lo cual permitió la protección de datos personales hasta cierto punto. En la toma de estas decisiones no solamente se pudo ver un cuerpo institucional sólido, sino un alto grado de cooperación a partir de la protección de los valores bajo los cuales fueron construidas las relaciones entre ambos actores.

Por el otro lado, se retorna al dilema del verdadero poder que sostienen las compañías Big Tech americanas. A pesar de que la Carta de Derechos Digitales, los comunicados y las investigaciones de la prensa restringieron en un primer momento la extracción masiva de datos con fines capitalizables, hubo una respuesta contundente por parte de compañías como Facebook. Ante esto la compañía decidió retirar su oferta del continente para promover el desarrollo tecnológico, sometiendo a países con un grado mayor de atraso tecnológico a buscar alternativas menos confiables o a permanecer en desventaja en materia tecnológica.

Hasta el año 2020, y con la llegada de Donald Trump al poder y la salida del Reino Unido de la UE, el organismo se ha visto obligado a dar respuestas de carácter interno, continúa buscando la forma de adaptar las plataformas a su legislación, pero no se han logrado consolidar ni esclarecer las investigaciones que involucran a las agencias de seguridad estadounidenses. Finalmente, es necesario comprender la respuesta estadounidense frente a las acusaciones e investigaciones, al, por un lado, negar en gran medida lo afirmado por las investigaciones, pero a la vez mostrar iniciativa a cooperar bajo la administración Obama, pero con desentendimiento y poca regulación a los intereses y al actuar de plataformas como Facebook, que, independientemente tenía sus propias exigencias con la UE. Esto provocó obstáculos en el proceso de la UE de indagar e implementar medidas efectivas. Las

consecuencias de esto se expondrán desde diferentes puntos de vista en el capítulo a continuación.

De manera general es posible establecer lo siguiente; cómo fue posible evidenciar, la respuesta mediática proveniente de los principales medios de comunicación de la UE estableció como punto central de las investigaciones, el hecho de que un país históricamente aliado, la traición a la confianza y el desconcierto con respecto al alcance de la vigilancia y las preocupaciones sobre el carácter comercial de la misma. Desarrollaron un análisis completo y un seguimiento imparcial a las acusaciones de Edward Snowden y adicionalmente, establecieron contacto con el cuerpo político para dar respuestas a la situación, cerciorándose de defender, no sólo la integridad de las fuentes informativas, sino también el acceso libre a este tipo de asuntos por parte de la población.

Lo que se evidencia en Europa posterior a las reacciones inmediatas al escándalo, son esfuerzos constantes, por un lado, para mantener la estabilidad con Norteamérica, pero a la vez contrarrestando las dinámicas que violan lo establecido por la Carta de Derechos digitales, y las regulaciones al comercio y ciberespacio, que de igual forma pretenden involucrar activamente al ciudadano al poner las plataformas a su disposición y no de la forma contraria. Sin embargo, los eventos que toman lugar a partir del escándalo de Cambridge Analytica exponen a su vez, una coordinación difusa y débil entre los Estados miembros de la UE, debido a la diferencia de intereses, la posición frente al gobierno de EE.UU. y los intereses comerciales de empresas como Facebook, denotando divisiones y fracturas frente al uso de la tecnología, más que reaccionando a los intereses de seguridad de EE. UU, con los cuales cooperan aún.

Más allá de acciones verbales y escritas como los ejemplos previos, es importante recordar que la UE se constituye como organismo de integración plenamente económica. Es por esto, y como se desarrollará en el capítulo a continuación, que fracasan en establecer consecuencias de índole política, y se limitan exclusivamente a la respuesta comercial, traducida en una serie de multas y sanciones hacia compañías como Facebook y Cambridge Analytica. Estas sanciones se dan bajo las circunstancias de constantes investigaciones periodísticas como las que ya se mencionaron, que profundizaron las fracturas entre ambos

países. Las sanciones, además de restringir los accesos de las compañías (situaciones cuya efectividad será evaluada más adelante), limitan la capacidad de acción de las empresas en países menores.

Las amenazas de las empresas privadas como Facebook, de retirar sus planes respecto a proyectos de conectividad, dejando a países menos desarrollados en la UE en dilemas respecto a sus decisiones y priorizar sobre el bien de sus ciudadanos. Países menos desarrollados se vieron afectados negativamente en términos de desarrollo, pero garantizaron la protección de los derechos y la privacidad de sus ciudadanos. Dependiendo del grado de conectividad del país, la salida de los proyectos de las Big Tech trae consecuencias en cuanto a la vulnerabilidad de los Estados, caso como el de Estonia al ver su política vulnerada tras ataques masivos de hackers. Los Estados además se encuentran bajo protección y fuerte alianza con EE. UU., significando que difícilmente podrían encontrar alternativas tecnológicas con los ‘beneficios’ que las compañías norteamericanas podrían ofrecer.

La respuesta legal e institucional recalca los valores bajo los cuales se establecieron las bases para una alianza estable y duradera con EE. UU., pero dependiendo del organismo y país. Los organismos de la UE como el Parlamento Europeo desarrollaron respuestas eficaces en la diplomacia internacional para hacer llegar un mensaje contundente a EE. UU., y establecer sanciones económicas que permitieron que la compañía hiciera al menos unos ajustes menores, estas sanciones fueron principalmente multas de hasta 800mil dólares a las empresas involucradas en la UE, así como el ajuste de los términos y condiciones al reglamento europeo y llevadas a cabo por cuerpos de consumo nacional (instituciones reguladoras de cada país) (Chee. 2018).

Desafortunadamente los impactos terminan en este punto debido a que las reacciones europeas no contemplaban la posibilidad de fracturas institucionales internas, entendidas como la desconexión entre la institucionalidad europea y los gobiernos miembros. Gobiernos que además de involucrarse en los hechos, negaron las acusaciones e instigaron a la prensa a desviar la atención. No tomaron en cuenta, finalmente, que las Big Tech americanas han adquirido un poder descomunal en los últimos años, sobrepasando en ventaja a Europa en la

carrera tecnológica y, por ende, estableciendo una relación de dependencia que, sumada a la relación de poder ejercida mediante la Ley Patriota, pone a la UE en desventaja con EE.UU.

### **Capítulo 3: Un mundo redefinido por la vigilancia**

#### **Las consecuencias en las Relaciones entre Estados Unidos y la Unión Europea**

Previamente se expusieron las respuestas y reacciones que tuvo la UE ante las revelaciones de espionaje desde EE. UU., se expusieron también las implicaciones institucionales de estas respuestas y se evidenció como la complejidad de la problemática se profundizó con la consolidación del capitalismo de vigilancia, o de la vigilancia como medio de poder y ganancia. Se pudo observar cómo, a pesar de las denuncias de la UE y la indignación en la opinión pública, en cuanto a contención del espionaje y protección de los datos, no hubo un avance sustancial y significativo que posicionara al organismo como un actor competente y a la altura de EE. UU. en materia digital. Europa se apegó a su normativa y a sus principios para definir el curso de acción y las competencias que debía desarrollar para hacer frente a estas amenazas.

En el presente capítulo, se expondrán las consecuencias del capitalismo de vigilancia y el espionaje en las Relaciones entre EE. UU. y la UE, los desafíos que representa para cada bloque, y el planteamiento de un dilema con respecto al equilibrio de poder en un escenario donde plataformas y compañías pueden condicionar el comportamiento de los Estados. Se expondrán los limitantes que posee la UE posterior a las revelaciones, y los desafíos que esta tiene más allá del espionaje, en lo que compete al capitalismo de vigilancia. Esto por supuesto, involucra perspectivas comerciales, militares, sociales, entre otras, que se tomarán en cuenta en torno a las dinámicas del ciberespacio, como se estableció en el primer capítulo, para ello es necesario también comprender el curso de acción tomado por EE. UU. posterior a las reacciones europeas. Siguiendo esta lógica y con el fin de culminar la presente investigación, se expondrán los hechos de mayor relevancia que hayan ocasionado cambios estructurales en las relaciones entre ambos bloques, más allá de las respuestas europeas, y se concluirá con base en el panorama generado a partir del choque de intereses.

### *3.1 Resultados*

El punto de partida para evaluar las consecuencias del espionaje es claramente el revuelo a nivel social que generaron las revelaciones. Si bien, gracias a la difusión de diferentes discursos a través de los medios, constantemente cambiantes y en evolución, la opinión con respecto a EE. UU. se había visto modificada a diferentes puntos de vista, el país norteamericano continuaba siendo el principal aliado de la UE.

El espionaje representa un acto de traición a la confianza mutua, y, para los valores europeos, como fue posible ver, una potencia extranjera teniendo control sobre los datos personales de los ciudadanos sin estos saber con qué fines, va en contra del respeto por la privacidad y las libertades individuales, pilares de las democracias occidentales. Estados Unidos a su vez es un promotor de seguridad y democracia, como determina la doctrina Bush, esto implica un desconcierto al conocer que es esta potencia aliada la que, indiscriminadamente, recopila información de ciudadanos europeos y determina su nivel de amenaza.

La polémica desatada conllevó a una acción rápida por parte de la UE, fue posible evidenciar una cooperación y una coordinación organizada y un planteamiento rápido de posibles soluciones. A pesar de la controversia, como fue posible evidenciar en la metodología y los datos presentados, como la cercanía ideológica y las buenas relaciones con el gobierno de Barack Obama, mantuvieron la solidez institucional y facilitaron el diálogo, además de mostrar una clara preocupación por el actuar de sus propias instituciones y demostrando iniciativa a la hora de acoger los lineamientos de la política digital en Europa. Las regulaciones adoptadas en la carta de derechos digitales obligaron a las compañías a dar un paso atrás en sus modelos de negocio, y siendo estas un instrumento de poder y control, con poderosos fines políticos mediante la manipulación, generaron tensiones entre varios actores, a pesar de que las relaciones mantuvieran un perfil positivo. Esas consecuencias serán analizadas a continuación desde las implicaciones en el ciberespacio, y las iniciativas tecnológicas y de cooperación en conjunto entre EE. UU. y la UE.

### *3.1.1 Respuesta Estadounidense:*

Previamente se habló de la respuesta europea y como sus instituciones concordaron con el periodismo para mostrarse en contra de las alegaciones de espionaje y vigilancia a partir de las revelaciones de Edward Snowden, a quien, además, ofrecieron protección. Estados Unidos, por el contrario, llevó a cabo una respuesta orientada a la protección de sus intereses. Al ser Edward Snowden un ex empleado de la Agencia Nacional de Seguridad, EE. UU. emprendieron acciones legales contra este bajo varios motivos, mencionados en una demanda judicial oficial, a raíz de unas irregularidades encontradas previas a la publicación de su libro donde se aseguraba que Snowden buscaba ganancia a partir de la desinformación y la imagen negativa de las instituciones americanas. Aquí podemos evidenciar declaraciones de jueces y diputados respecto a la sentencia:

Edward Snowden violó sus obligaciones y, por lo tanto, sus ganancias financieras ilícitas deben ser entregadas al gobierno (...) (Rosen. A, 2014).

La información de inteligencia debería proteger nuestra nación, no proveer ganancia personal (Terwilliger, G).

Es de recordar, y tal como lo menciona el documento, que este tipo de acciones (Lawsuit como se conoce en inglés), son acciones de carácter civil, en el ámbito legal, se llevaron a cabo una serie de procesos sobre Edward Snowden, para posteriormente dar respuesta y explicaciones, además de proponer soluciones, que garantizaran las buenas relaciones con la UE. Similar a las instituciones europeas, el cuerpo legal de EE. UU. clasificó, posterior a las investigaciones, que los programas de vigilancia de la NSA podrían estar infringiendo la legalidad del país e incluso podrían llegar a ser inconstitucionales, según lo estableció un tribunal de justicia estadounidense en un reportaje para DW (2020). A pesar de las sanciones y los comunicados, esta Corte cooperó de forma constante con otras instituciones empeñadas a la vigilancia y la seguridad en EE. UU., como lo son el FBI y la CIA.

### *3.3 La Redefinición del Ciberespacio*

Ya fue posible comprender la creación y el posterior funcionamiento del ciberespacio, la estructura de este concepto permitió a los países relacionarse y trasladar sus dinámicas a este plano, descubriendo nuevas e innovadoras maneras de maximizar las ganancias económicas, y facilitar la vida de los ciudadanos, un nuevo terreno para las RRII. Las implicaciones de las revelaciones de Edward Snowden conllevaron al entendimiento de la opinión pública, acerca del alcance de la vigilancia en el ciberespacio; la seguridad internacional se convirtió en pretexto para recopilar información de los ciudadanos y es en este punto que las relaciones adoptan un nuevo carácter. Esto, sumado a los nuevos desafíos, conllevó a un conflicto de intereses y una competencia por el dominio del terreno digital, entre países aliados, pero introdujo, además, actores como las plataformas en el terreno de juego. Esto tuvo repercusiones internas que conllevó al desarrollo de estrategias por el dominio ciberespacial, tanto en EE. UU., como en la UE, y también Facebook. (Ver Anexo no.3 Infografía de amenazas cibernéticas a la UE).

En el caso de EE. UU., a pesar de la polémica desatada, la magnitud de las capacidades de este país en términos de políticas digitales continúa en alza. La incapacidad del gobierno y las instituciones democráticas de poner un freno a la vigilancia de la Agencia Nacional de Seguridad es a la vez un obstáculo para la UE, a la hora de esclarecer los eventos de espionaje entre gobiernos. Las agencias nacionales europeas adaptaron las dinámicas de la NSA estadounidense, provocando nuevos escándalos esta vez al interior de la UE; esto es un claro síntoma de la debilidad institucional de la UE en el momento de afrontar estas amenazas a su seguridad, y a la vez la necesidad urgente de integrar políticas digitales dentro del marco institucional del organismo. En este punto es posible evidenciar tres modificaciones clave en las relaciones de ambos bloques a nivel doméstico e internacional. En EE. UU. hay un claro interés comercial primando sobre el interés social, otorgando un mayor poder de acción internacional a compañías como Facebook, mientras que el caso europeo conllevó a la redefinición de sus políticas internas y la producción de nuevas legislaciones; estos cambios generaron distanciamientos y tensiones y a partir de estas, se explicará el posterior carácter de las relaciones a continuación.

La securitización juega un papel clave en las medidas de EE. UU. ya que tornan el componente de vigilancia como una necesidad para la seguridad nacional y, por ende, para la promoción de la democracia y los valores estadounidenses a nivel global. Por ello, orientar las políticas y las relaciones entre EE. UU y la UE, hacia los intereses militares de los norteamericanos y la OTAN, se volvió prioridad para el gobierno. Ante esto, Merle Maigre, directora del Centro de Defensa Cibernética de la OTAN estableció lo siguiente, en un reporte de la Deutsche Welle (DW, 2018):

"Desde enero de 2018, la OTAN coordina la formación de las unidades cibernéticas de los Estados miembros, pero muchos líderes políticos entienden muy poco de la materia (...) la lucha contra los ataques cibernéticos no la puede librar ningún estado por separado" (Maigre, 2018).

Con estas afirmaciones, y las respuestas dadas a las acusaciones de la UE, EE. UU. consolidaron una nueva dimensión al interior del ciberespacio, y, resaltando la cooperación y la confianza nuevamente como valor compartido, creó una relación de dependencia donde Europa es el actor menos favorecido, y le es de urgencia adoptar las medidas necesarias, propuestas por EE. UU., para hacer frente a las amenazas digitales.

Por el otro lado, dentro de la doctrina de seguridad estadounidense, no hay un desarrollo con respecto al rol que juega Facebook en la securitización del ciberespacio europeo, si bien la red social no es causante de esta, su papel como distribuidor de datos mediante su modelo de negocio, a agencias como la NSA, tuvieron el impacto institucional que se pudo observar en el anterior capítulo. Facebook, como se mencionó en los capítulos anteriores, expresa las dinámicas comerciales del capitalismo de vigilancia, el otro componente al cual la U debe estratégicamente hacerle frente dado su carácter invasivo y destabilizador, sin entrar en conflicto con los intereses de seguridad norteamericanos, pero a la vez con la oferta tecnológica de Facebook. Esto es debido a la debilidad europea en materia digital y, como es mencionado en la carta de derechos digitales, el organismo busca constantemente la cooperación mutua, por un lado, para beneficiarse de las innovaciones tecnológicas y los servicios estadounidenses en todos los campos, pero a la vez para adaptar a los actores

digitales a las legislaciones europeas, y hacer del ciberespacio un lugar de concordancia con los valores occidentales.

### *3.4 Conclusiones*

Facebook, junto con Google y Amazon son en la actualidad los mayores y principales promotores del desarrollo de tecnologías en Occidente. La superposición de una empresa en estas competencias sobre los mismos Estados ya marca un punto de inflexión clave en las RRII. La evolución a un sistema donde los datos son monetizados posicionó a Facebook como un mediador clave en el desarrollo de la estrategia de seguridad estadounidense, seguida por sus homólogos europeos. Desde las revelaciones de Edward Snowden, los gobiernos europeos y particularmente sus agencias de seguridad se vieron en una encrucijada; esto representa una dualidad entre aquello que se promueve como institucionalidad por parte de la UE, construcción ética y moral del Estado y sus intereses, pero por el otro la necesidad de vigilar a la ciudadanía en una competencia por el terreno ciberespacial.

El caso de Cambridge Analytica profundizó esta dualidad, ya que ahora se involucraba manipulación mediática con fines políticos; la consecuencia de esto principalmente fue la pluralización de actores, intereses y valores. Las relaciones con EE. UU. se vieron afectadas en este aspecto a partir de las tensiones con el gobierno Trump y el incremento del espionaje entre aliados.

En materia de vigilancia y manipulación, es evidente durante estos años un incremento en la radicalización de la población europea en diversos países; quizás el mejor ejemplo es el ascenso nuevamente de la AfD, principal partido de derecha en Alemania, obteniendo escaños en 2015 por primera vez desde la Segunda Guerra, o el crecimiento de la Liga Italiana a través de la actividad en redes sociales de sus principales miembros. Además, durante el periodo de tiempo que comprende la investigación Facebook desarrolló nuevas estrategias o incluso llegó a amenazar con abandonar sus proyectos en territorio europeo, pero sin consecuencias significativas políticas en las relaciones entre ambos bloques, diferente de las revelaciones de espionaje de las diferentes agencias.

Como conclusión, es posible decir que las diferentes tensiones generadas a partir de las revelaciones de Edward Snowden sobre espionaje y vigilancia, y la profundización de estas dinámicas en el caso de Cambridge Analytica, corresponden a un proceso de digitalización acelerada que incrementó la competencia por el terreno, gracias a la rentabilidad de las actividades en este. Los valores bajo los cuales estaban construidas las sociedades europeas y estadounidenses sufrieron un cambio drástico, la confianza y el respeto por la libertad, incluyendo las libertades individuales y el derecho a la privacidad, se vieron altamente afectados provocando tensiones, no solo entre ambos bloques, sino a nivel institucional y social, reviviendo a nivel interno antiguas discusiones y divisiones.

Si bien la UE fue eficiente y veloz al momento de responder y exigir explicaciones a EE.UU., la complejidad del asunto no derivó en soluciones efectivas. Adicional a este hecho, el ciberespacio y las dinámicas del capitalismo de vigilancia continúan avanzando más rápido de lo que, aparentemente, la capacidad institucional de los Estados puede llegar a actuar. Las consecuencias de esto incluyeron, por un lado, la redefinición de la política europea en materia digital, avances y logros significativos en materia de ciberseguridad y protección de datos; pero a nivel relacional, una división interna profunda al no tener control sobre el comportamiento de sus propias agencias, y estar sujetos a cambios externos. Es aquí donde se plantea un dilema con respecto a las compañías digitales, es pertinente preguntarse el verdadero alcance de la vigilancia y reflexionar sobre el poder que se les ha otorgado a plataformas como Facebook, en materia de manipulación a Estados enteros. ¿Está el futuro de las RRII sujeto a los intereses comerciales de las plataformas?

## Bibliografía:

- Acuerdo entre EE. UU. y UE sobre el marco de transferencia de datos personales. AFP. (2022). France 24. En: <https://www.france24.com/es/minuto-a-minuto/20220325-acuerdo-entre-eeuu-y-ue-sobre-el-marco-de-transferencia-de-datos-personales>
- Adaptación a la Era Digital. Democracia y Derechos Humanos. Los derechos fundamentales en la Unión Europea. Parlamento Europeo (2022). En: <https://www.europarl.europa.eu/about-parliament/es/democracy-and-human-rights/fundamental-rights-in-the-eu/adapting-to-the-digital-age>
- Alba Useche, D.A (2014). El espionaje y agencias de seguridad: los Estados Unidos y la Federación Rusa. Esfac Publicaciones. En: <https://publicacionesfac.com/index.php/cienciaypoderaereo/article/view/138/276>
- Amer, K. Noujaim, J. (2019) The Great Hack, Netflix
- Aust, S. Krüger, C. Scholz, M. (2019). Edward Snowden: Creo que los gobiernos europeos me tienen miedo. Die Welt & El País. En: [https://elpais.com/internacional/2019/09/13/actualidad/1568390496\\_167835.html](https://elpais.com/internacional/2019/09/13/actualidad/1568390496_167835.html)
- Ayala, E.T. (2018). International Relations from a Social Perspective. The Constructivist Approach to Explain National Identity. Universidad del Mar. Revista Mexicana de ciencias políticas y sociales. En: [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0185-19182018000200389](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-19182018000200389)
- Barnes, R. (2021). Invertir en Facebook, un modelo de negocio 100% publicitario. RLB. En: <https://rodrigolbarnes.com/2021/12/06/facebook-modelo-negocio-publicitario/#:~:text=Estrategia%20de%20Facebook,los%20de%20otras%20redes%20sociales.>
- Cómo llegamos el Ciberespacio. BBC. (2016). En: [https://www.bbc.com/mundo/noticias/2016/03/160316\\_origen\\_palabra\\_ciber\\_finde\\_dv](https://www.bbc.com/mundo/noticias/2016/03/160316_origen_palabra_ciber_finde_dv)
- EE. UU espía a Angela Merkel entre 2002 y 2013, según reporte. BBC Mundo. (2013). En: [https://www.bbc.com/mundo/ultimas\\_noticias/2013/10/131027\\_alemania\\_eeuu\\_merkel\\_espionaje\\_ng](https://www.bbc.com/mundo/ultimas_noticias/2013/10/131027_alemania_eeuu_merkel_espionaje_ng)
- Callejo Gallego, M.J. (2017). SOCIOLOGÍA DIGITAL: LA REINVENCIÓN DE LA INVESTIGACIÓN SOCIAL. BARATARIA. Revista Castellano-Manchega de Ciencias Sociales, núm. 22, pp. 231-234, 2017. Asociación Castellano Manchega de Sociología
- Castellaro, Mariano Andrés. (2012). Definiciones teóricas y áreas de investigación propuestas desde el constructivismo, en publicaciones latinoamericanas de psicología y educación presentes en la Base de Datos REDALYC. Liberabit, 18(2), 131-146. Recuperado en 10 de junio de 2022, de

[http://www.scielo.org.pe/scielo.php?script=sci\\_arttext&pid=S1729-48272012000200004&lng=es&tlng=es](http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1729-48272012000200004&lng=es&tlng=es).

- Cela, Julia R.; Parras-Parras, Alicia; y Romero-Vara, Laura (2019): " Uso de las redes sociales en diplomacia, política y Relaciones Internacionales. Análisis de la información publicada en las versiones online de dos periódicos españoles: El País y La Vanguardia". Estudios sobre el Mensaje Periodístico 25 (2), 711-726.
- Cerrillo Garnica, Omar (2019). La bandera de Francia en Facebook: un debate en torno a la identidad, la ideología y la globalización. Paakat: Revista de Tecnología y Sociedad, (17),1-17.. En: <https://www.redalyc.org/articulo.oa?id=499063348010>
- Choucri, N. (2012). Cyberspace: New Domain of International Relations. Cyberpolitics in International Relations. Pp 49-70.
- Ciberseguridad: Cómo combate la UE las amenazas cibernéticas. Consejo de la Unión Europea (2022). En: <https://www.consilium.europa.eu/es/policies/cybersecurity/>
- Cinco Días. (2022). La UE y EE. UU. llegan a un acuerdo para poder transferir datos personales con garantías para la privacidad. Cinco Días. El País. Madrid. En: [https://cincodias.elpais.com/cincodias/2022/03/25/companias/1648206086\\_138094.html](https://cincodias.elpais.com/cincodias/2022/03/25/companias/1648206086_138094.html)
- Chee, F. Y. (2018). Facebook and Twitter must comply with EU consumer rules or face sanctions. Reuters. En: <https://www.reuters.com/article/us-eu-facebook-airbnb-idUSKCN1M013I>
- Comisión Europea (2022). La Comisión ha presentado una declaración de derechos y principios digitales para todos en la UE. Comunicado de Prensa. En: [https://ec.europa.eu/commission/presscorner/detail/es/ip\\_22\\_452](https://ec.europa.eu/commission/presscorner/detail/es/ip_22_452)
- Comisión Europea (2022). Comunicado de Prensa. Commission puts forward declaration on digital rights and principles for everyone in the EU.
- Consejo Europeo. La Respuesta de la UE al Terrorismo
- Cordero, A. (2021). Dos décadas de una política exterior marcada por la “guerra contra el terrorismo”. France 24. En: <https://www.france24.com/es/ee-uu-y-canad%C3%A1/20210910-eeuu-atentados-11-septiembre-politica-externa-guerras>
- Deloivre, C. (2013). Por qué debe proteger Europa a Edward Snowden. Vox Europa. Le Monde (París). En: <https://voxeurop.eu/es/por-que-debe-proteger-europa-a-edward-snowden/>
- De Rivera, J. (2019). Guía para entender y combatir el capitalismo digital. Papeles de relaciones eco sociales y cambio global 79 N° 144, pp. 79-89
- Domínguez Cebrián, D. (2021). Dinamarca colaboró con EE. UU. para espiar a Merkel y otros políticos europeos. Internacional. El País. En: <https://elpais.com/internacional/2021->

[05-31/dinamarca-colaboro-con-ee-uu-para-espiar-a-merkel-y-otros-politicos-europeos.html](https://elpais.com/internacional/2015/04/30/actualidad/1430392574_182172.html)

Doncel, L. (2015). El escándalo de espionaje pone en apuros al gobierno de Merkel. Alemania. El País. En:

[https://elpais.com/internacional/2015/04/30/actualidad/1430392574\\_182172.html](https://elpais.com/internacional/2015/04/30/actualidad/1430392574_182172.html)

El Parlamento Europeo no otorga protección a Edward Snowden. DW. (2014). El Mundo. En: <https://www.dw.com/es/el-parlamento-europeo-no-otorga-proteccion-a-edward-snowden/a-17427665>

Estados Unidos y la Unión Europea, condenados a entenderse. Euronews. (2014). En: <https://es.euronews.com/my-europe/2014/03/19/estados-unidos-y-la-union-europea-condenados-a-entenderse>

Edward Snowden: Leaks that exposed the US spy programme. BBC News (2014). En: <https://www.bbc.com/news/world-us-canada-23123964>

Frankel, A. (2022). Facebook, Gibson Dunn face \$858K sanctions demand in Cambridge Analytica Class Action. Reuters. En: <https://www.reuters.com/legal/litigation/facebook-gibson-dunn-face-854k-sanctions-demand-cambridge-analytica-class-action-2022-04-04/>

Flores-Márquez, Dorismilda. (2016). Recordar el pasado, pensar el futuro: Sociología, comunicación y cultura digital. Espacio Abierto. 25. 215-227.

GeoIDEP. Qué Son los Metadatos. Infraestructura de Datos Especiales del Perú. En: <https://www.geoidep.gob.pe/metadatos/que-son-los-metadatos>

Gómez, J. (2013). EE. UU. indigna a Europa por un espionaje “digno de enemigos”. Internacional. El País. En: [https://elpais.com/internacional/2013/07/01/actualidad/1372630167\\_914680.html](https://elpais.com/internacional/2013/07/01/actualidad/1372630167_914680.html)

González Ferriz, R. (2022). Por qué Facebook y la UE se llevan mal. Tribuna Internacional. El Confidencial. En: [https://blogs.elconfidencial.com/mundo/tribuna-internacional/2022-02-10/facebook-union-europea-trabas-regulacion\\_3372597/](https://blogs.elconfidencial.com/mundo/tribuna-internacional/2022-02-10/facebook-union-europea-trabas-regulacion_3372597/)

Higuera, A. (2021). Estados Unidos reconoce que nos ha espiado: Así vigilaba su servicio de seguridad nacional a Europa y sus ciudadanos. 20 bits. En: <https://www.20minutos.es/tecnologia/ciberseguridad/operacion-dunhammer-dinamarca-y-estados-unidos-espiaron-juntos-a-merkel-y-otros-politicos-europeos-4714467/>

Jiménez González, A.; Rendueles Menéndez de Llano, C. (2020). Capitalismo digital: fragilidad social, explotación y solucionismo tecnológico. Teknokultura. Revista de Cultura Digital y Movimientos Sociales, 17(2), 95-101.

Lecours, A. (2007). LEY PATRIOTA DE LOS EE.UU. (USA PATRIOT ACT) Efectos extraterritoriales de la Ley Patriota de los EE.UU. – Derechos de Privacidad de ciudadanos no norteamericanos. Lecours & Lessad. La Crónica Jurídica.

- Manjarrés Chavarriaga, E. (2016). FACEBOOK EN LA SOCIEDAD DE CONTROL Aplicación simultánea del panóptico y del sinóptico en un dispositivo de vigilancia y control social. Universidad Eafit, Escuela de Humanidades. Medellín.
- Manual de legislación europea en materia de protección de datos. (2018). Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa,
- McDavid, Jodi (2020) “The Social Dilemma”, Journal of Religion & Film. Netflix.
- Medina Quintero, F.E. (2014). La teoría constructivista en las Relaciones Internacionales y la Escuela de Copenhague: la ampliación del concepto de seguridad en las Américas. Revista Análisis Internacional. Vol 5. Pp 77-85.
- Montero Montano, R. Ybarra Martínez, K. (2017). De la Ciberseguridad a la Ciberpolítica. Información Jurídica Inteligente. En: <https://vlex.com.mx/vid/ciberseguridad-ciberpolitica-698097297>
- Morozov, E. (2018). El capitalismo digital y sus descontentos. El lado oscuro de la libertad de Internet. Conferencia: lunes, 26 marzo de 2018. Seis contradicciones y el fin del presente.
- Nieves Saldaña, M. (2011). El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego. Teoría Y Realidad Constitucional, (28), 279–312. <https://doi.org/10.5944/trc.28.2011.6960>
- Parlamento Europeo. (2014). Sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior (2013/2188(INI)) Comisión de Libertades Civiles, Justicia y Asuntos de Interior Ponente: Claude Moraes
- Peirano, M (2016). La Vigilancia no tiene que ver con la Seguridad, tiene que ver con el Poder. El Diario España. En: [https://www.eldiario.es/internacional/entrevista-edward-snowden\\_128\\_4103499.html](https://www.eldiario.es/internacional/entrevista-edward-snowden_128_4103499.html)
- Peirano, M (2016). “Prefiero renunciar a mi patria que renunciar a mi voz”. El Dario España. En: [https://www.eldiario.es/internacional/teleco-usando-conectada-cordel-privacidad\\_128\\_4109554.html](https://www.eldiario.es/internacional/teleco-usando-conectada-cordel-privacidad_128_4109554.html)
- Pereda, C. (2017). Trump mantiene que fue espiado durante la campaña electoral. Estados Unidos. El País. En: [https://elpais.com/internacional/2017/03/17/estados\\_unidos/1489759521\\_742720.html](https://elpais.com/internacional/2017/03/17/estados_unidos/1489759521_742720.html)
- Pereyra, G. (2015). El estudio de la Identidad en las Relaciones Internacionales. El constructivismo como “solución” teórica temporal. Universidad Nacional de Rosario. En: <https://biblioteca.uap.edu.ar/wp-content/uploads/2015/11/2015-1-Pereyra-Doval.pdf>

- Pérez Lozano, A. (2018). Reseña/Review (Srnicek, Nick, “Capitalismo de plataformas”, Buenos Aires: Caja Negra, ISBN: 978-987-1622-68-9, 128 págs.,
- Pérez Martínez, V. (2013). El ciberespacio: ¿una realidad en construcción?
- Pérez, J. (2021) Europa y la guerra por el ciberespacio. DW. En: <https://learngerman.dw.com/es/europa-y-la-guerra-por-el-ciberespacio/a-42621169>
- Pinto, T. (2019). El legado de Snowden: Las filtraciones que transformaron internet. El País. En: [https://elpais.com/tecnologia/2019/10/07/actualidad/1570455695\\_974155.html](https://elpais.com/tecnologia/2019/10/07/actualidad/1570455695_974155.html)
- Piñar, J. L (2021). La Carta de Derechos Digitales. Hoja de ruta para la transformación digital. CMX. En: <https://cms.law/es/esp/publication/la-carta-de-derechos-digitales-hoja-de-ruta-para-la-transformacion-digital>
- Poitras, L. (2014). Citizenfour. RADiUS-TWC.
- Public law 107-56—oct. 26, 2001 uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001
- Quintana, Y. (2014). Parlamento Europeo: Los programas de espionaje masivo vulneran derechos fundamentales y deben prohibirse. El Diario España. En: [https://www.eldiario.es/turing/vigilancia\\_y\\_privacidad/nsa-parlamento-europeo-snowden-espionaje-privacidad\\_1\\_4996047.html](https://www.eldiario.es/turing/vigilancia_y_privacidad/nsa-parlamento-europeo-snowden-espionaje-privacidad_1_4996047.html)
- Real Academia Española. (2014). Diccionario de la lengua española (23a ed.)
- Reuters Staff. (2013). La UE se enfrenta a Washington por acusaciones de espionaje. Thomson Reuters. En: <https://www.reuters.com/article/oestp-eeuu-ue-espionaje-idESMAE95T00R20130630>
- Rodríguez, J.C (2017). EE. UU. Europa, Intereses Valores. Instituto Juan de Mariana. En: <https://juandemariana.org/ijm-actualidad/articulos-en-prensa/eeuu-europa-intereses-valores/>
- Sánchez, E. (2015). Escándalo de espionaje entre Alemania y EE. UU. My Europe. Euronews. En: <https://es.euronews.com/my-europe/2015/05/14/escandalo-de-espionaje-entre-alemania-y-eeuu>
- Seda Gambín, C. (2020). Crecimiento del capitalismo de vigilancia en la Unión Europea y sus amenazas a la democracia, el ejemplo de las aplicaciones de rastreo de contactos durante la pandemia de COVID-19. Universitat de les Illes Balears.
- Solis Umaña, M (2011). LIBERTARISMO Y JUSTICIA SOCIAL: LA LIBERTAD COMO VALOR POLÍTICO. Revista Humanidades, Vol. 1, pp. 1-18 / ISSN: 2215-3934 Universidad de Costa Rica, 2011

- Sparrow, T. (2013). Cómo afectan a EE. UU las acusaciones de espionaje en Europa. BBC News. En: [https://www.bbc.com/mundo/noticias/2013/10/131029\\_eeuu\\_europa\\_nsa\\_controversia\\_tsb](https://www.bbc.com/mundo/noticias/2013/10/131029_eeuu_europa_nsa_controversia_tsb)
- Srnicek, N. (2016). Capitalismo de Plataformas. Capitalismo de Plataformas. Caja Negra Editora, 2018. Pp. 39-87.
- Tah Ayala, Einer David. (2018). Las Relaciones Internacionales desde la perspectiva social. La visión del constructivismo para explicar la identidad nacional. Revista mexicana de ciencias políticas y sociales, 63(233), 389-403. <https://doi.org/10.22201/fcpys.2448492xe.2018.233.62593>
- Telesur EFE. (2015). Alemania ayudó a Estados Unidos a espiar a Francia. En: <https://www.telesurtv.net/news/Alemania-ayudo-a-Estados-Unidos-a-espiar-a-Francia-20150429-0041.html>
- The NSA and America's Madness. Pixels Editorial. Le Monde (2015). En: [//www.lemonde.fr/pixels/article/2015/06/24/the-nsa-and-america-s-madness\\_4660991\\_4408996.html](http://www.lemonde.fr/pixels/article/2015/06/24/the-nsa-and-america-s-madness_4660991_4408996.html)
- Tortosa, J.M. Estados Unidos y su “Guerra contra el Terrorismo”: continuidad o cambio. Instituto Universitario de Desarrollo Social y Paz. Universidad de Alicante.
- Tribunal de EE. UU.: Programa de vigilancia de la NSA expuesto por Snowden era ilegal. DW (2020). El Mundo. En: <https://www.dw.com/es/tribunal-de-ee-uu-programa-de-vigilancia-de-la-nsa-expuesto-por-snowden-era-ilegal/a-54818920>
- Vila Seoane, M y Saguier, M. (2019). “Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional”, en Relaciones Internacionales, nº 40, pp. 113 - 131.
- Un Futuro Digital para Europa. Consejo de la Unión Europea (2022). En: <https://www.consilium.europa.eu/es/policies/a-digital-future-for-europe/>
- Villanueva, A.V. (2013). La teoría constructivista de las Relaciones Internacionales constituye una explicación adecuada del establecimiento del espacio europeo de educación superior. Universidad de Belgrano. En: <http://repositorio.ub.edu.ar/handle/123456789/5860>
- Webb, A. (2019). La mente y las máquinas: una breve historia de la inteligencia artificial. Espíritus en la Máquina. Nueve Gigantes. Hachette Book Group, Inc., 2019. Pp 16-24.
- Webb, A. (2019).. Espíritus en la Máquina. Nueve Gigantes. Hachette Book Group, Inc., 2019. Pp 16-101.
- Webb, A. (2019).. Nueve Gigantes. Hachette Book Group, Inc., 2019.
- White House Archives. (2006). La Estrategia Nacional del Presidente para combatir el Terrorismo. Los Estados Unidos de América, Seguridad Nacional. En:

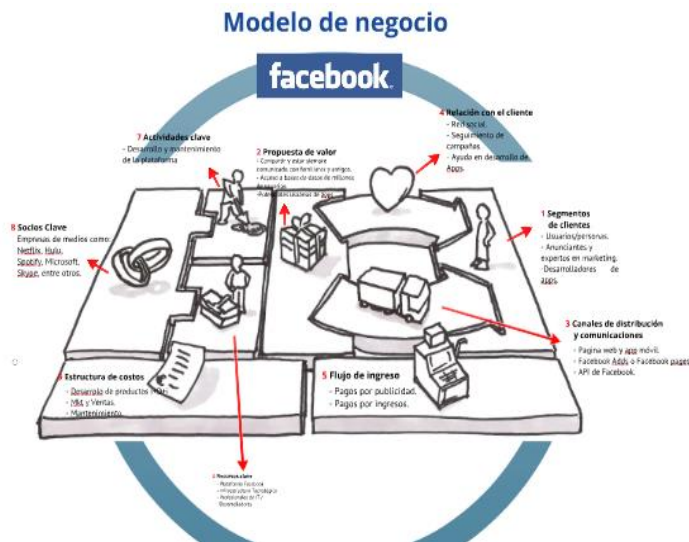
<https://georgewebush-whitehouse.archives.gov/infocus/nationalsecurity/index.es.html>

Zubero, Imanol. (2018). Capitalismo digital: el problema es el capitalismo, no la tecnología. 9-24.

Zuboff, S. (2020). El descubrimiento del excedente conductual. Los fundamentos fundacionales del Capitalismo de la Vigilancia. La Era del Capitalismo de Vigilancia. Editorial Planeta. Pp 93-139.

Zuboff, S. (2020). Los fundamentos fundacionales del Capitalismo de la Vigilancia. La Era del Capitalismo de Vigilancia. Editorial Planeta.

## Anexos



1. Modelo de Negocio de Facebook (Luna, M. 2017).

Edward Snowden Interview

## The NSA and Its Willing Helpers

In an interview conducted using encrypted e-mails, whistleblower Edward Snowden discusses the power of the NSA, how it is "in bed together with the Germans" and the vast scope of Internet spying conducted by the United States and Britain.

08.07.2013, 15.34 Uhr



6+ Einen Monat für 1 Euro

Jetzt testen > X

2. Titular de artículo publicado por Der Spiegel, referente a las revelaciones de Snowden.

## Principales ciberamenazas en la UE



**Programas de secuestro**

Tipo de ataque malintencionado en el que los ciberdelincuentes encriptan los datos de una organización y exigen un rescate para restaurar el acceso.

*El precio medio de los rescates se ha duplicado.*



**Programas malignos**

Programas informáticos malintencionados concebidos para dañar un dispositivo, perturbar su funcionamiento o acceder a él sin autorización.

*Los ataques con programas malignos en la UE se han reducido en un 43 %.*



**Criptosequestros o criptomina maliciosa**

Uso no autorizado del ordenador, el teléfono inteligente o la tableta de un usuario para minar criptomoneda.

*Las criptomonedas siguen siendo el método de pago más frecuente entre los ciberdelincuentes.*



**Ataques por correo electrónico**

Tentativas de robo de contraseñas o datos de tarjetas de crédito a través de diversas técnicas, como el phishing, el phishing de SMS y el spam.

*Los mensajes «gancho» relacionados con la COVID-19 siguen dominando los ataques por correo electrónico.*



**Violaciones de la seguridad de los datos y fugas de datos**

Divulgación de datos sensibles, confidenciales o protegidos en un entorno no fiable.

*Se ha producido un aumento de las violaciones de seguridad de datos sanitarios.*



**Ataques distribuidos de denegación de servicio**

Ataques que impiden a los usuarios de una red o sistema acceder a información, servicios u otros recursos pertinentes.

*Se han producido más de 10 millones de ataques distribuidos de denegación de servicio debido a la COVID-19.*



**Desinformación**

Ataque intencionado consistente en crear o divulgar información falsa o engañosa para manipular a la opinión pública.

*La COVID-19 es uno de los principales temas de los ataques de desinformación.*



**Amenazas no malintencionadas**

En su mayoría se deben a errores humanos, aunque también pueden darse como consecuencia de catástrofes naturales que causan daños en las infraestructuras informáticas.

*El 50 % de estos ataques se deben a fallos de configuración.*



**Amenazas a la cadena de suministro**

Ataques dirigidos contra una organización a través de las vulnerabilidades de su cadena de suministro, capaces de producir efectos en cascada.

*El 58 % de los ataques a las cadenas de suministro tiene por objetivo obtener acceso a datos.*

Fuente: Panorama de amenazas de ENISA, 2021 (cifras de abril de 2020 a julio de 2021)

### 3. Infografía Amenazas cibernéticas a la UE. (Consejo de la Unión Europea, 2021).