Comentario Internacional No. 19, 2019
ISSN 1390-1532 • eISSN 2631-2549

Ciberseguridad y Derechos Humanos: respuestas estatales e individuales a las revelaciones de espionaje de Snowden

*Daniel Crespo-Pazmiño**

Resumen

Cuatro días después del retiro del asilo de Assange, el gobierno ecuatoriano anunció que sufrió más de cuatro millones de ciberataques. Es claro que el ciberespacio es un entorno que no está exento de riesgos, oportunidades e intereses. Las respuestas políticas de distintos actores reposicionan el debate sobre el papel de informantes y Estados en la defensa de la seguridad en Internet. La ciberseguridad es más que la protección de ataques a infraestructuras críticas, también envuelve la defensa virtual de los derechos de las personas. Mediante un análisis basado en la ciberseguridad y en la economía política internacional, este trabajo evidencia la manera en que diversos actores responden a la problemática de la seguridad y el respeto de los derechos.

Palabras clave: Ciberseguridad, economía política internacional, derechos humanos, hegemonía, panóptico, espionaje, Snowden, Internet.

Cybersecurity and Human Rights: state and individual responses to Snowden's espionage revelations

Abstract

Four days after the withdrawal of Assange's asylum, the Ecuadorian government announced that it suffered more than four million cyberattacks. Clearly, the cyberspace is an environment that is not exempt from risks, opportunities, and interests. The political responses of different actors reposition the debate on the role of informants and States in the defense of Internet security on the. Cybersecurity is more than the protection of attacks on critical infrastructures; it also involves the defense of the virtual rights of the people. Through an analysis based on cybersecurity and international political economy, this paper demonstrates the way in which different actors respond to the problem of security and respect for rights.

Keywords: cybersecurity; international political economy; human rights; hegemony; panopticon; espionage; Snowden; Internet.

---

* Máster en Relaciones Internacionales con mención en Seguridad y Derechos Humanos, Facultad Latinoamericana de Ciencias Sociales (FLACSO) sede Ecuador ‹dfcrespofl@flacso.edu.ec›.
Recibido: 24 de abril de 2019 | **Revisado**: 13 de octubre de 2019 | **Aceptado**: 1 de enero de 2020
Para citar este artículo: Crespo-Pazmiño, Daniel. "Ciberseguridad y Derechos Humanos: respuestas estatales e individuales a las revelaciones de espionaje de Snowden". *Comentario Internacional,* n.º 19 (2019).
doi: 10.32719/26312549.2019.19.3

Introducción

El pasado 11 de abril de 2019 Ecuador anunció su decisión de retirar la condición de asilo diplomático a Julian Assange, fundador del portal Wikileaks. Cuatro días después, el gobierno del Ecuador anunció que sufrió más de 4 millones de ciberataques luego del retiro del asilo.[1] Es claro que se vive en una era donde el Internet no solo es un espacio de acceso a información y comunicación, sino que también es un escenario de conflicto en el que existen riesgos, oportunidades e intereses. Así, las respuestas a políticas por actores no estatales son evidentes y reposicionan el debate sobre el papel de informantes y Estados en la defensa la seguridad en el Internet. Esta situación acontece particularmente en un momento en el que se observa cómo las amenazas de actores no estatales se encuentran cada vez más presentes en la política; motivo por el cual los Estados necesitan ser aún más conscientes de las nuevas dinámicas de ofensiva en sus consideraciones de seguridad estatal y ciudadana.

La ciberseguridad consiste en la protección de ataques direccionados a infraestructuras críticas, así como también envuelve la defensa de los derechos y libertades de las personas en el ciberespacio. Esto incluye a los ataques digitales, como el robo de información o la violación de la privacidad. Dichas amenazas pueden provenir de actores no estatales difusos –hackers, terroristas–, o generarse en instituciones y empresas que buscan ejercer influencia y control en diferentes esferas para sus intereses económicos o políticos. Dichos altercados se pueden entender como ejercicios de dominación que se ejercen mediante estructuras económicas, tecnológicas y culturales, como lo es el Internet. Por ello, los medios electrónicos de comunicación acuñan y articulan cada vez más información compleja que puede ser utilizada para suplir necesidades, tales como el comercio, la lucha contra el crimen y la institucionalización de valores y normas para ejercer control.

En esta lucha de poder y control también se destaca la presencia de actores no estatales, que gracias a los avances tecnológicos de la globalización, denuncian los actos de influencia ciberespacial y la violación de la privaci-

1. Teresa Menéndez, "40 millones de ciberataques tras detención de Assange", *Ecuavisa*, 15 de abril de 2019.

dad. Si bien el caso de Assange, fundador del portal Wikileaks, es conocido por revelar distintos cables diplomáticos sobre el comportamiento militar o espionaje en Naciones Unidas, es importante destacar que dichas revelaciones se produjeron en un contexto apartado del periodismo tradicional, en vista de que no se basó con un proceso de verificación de fuentes de información y edición para evidenciar la información de manera imparcial y oportuna. El caso Snowden, no obstante, sí contó con el respaldo de un proceso de verificación de fuentes y edición periodística para exponer las acciones de vigilancia masiva de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés). Con ello mostró deficiencias de ciberseguridad de individuos y Estados y fue clave para la modificación de la legislación americana y suspensión de uno de los programas de vigilancia denunciados.

Por ende, el presente trabajo se enfoca en determinar la manera en que diversos actores responden a la problemática de la seguridad y el respeto de los derechos y libertades en un entorno que, con el avance tecnológico, no vuelve más anónima la interacción en el Internet, sino más personal. Para ello, en primera instancia, se presenta el funcionamiento del sistema de vigilancia masiva denunciado por Snowden. Segundo, se estudia el debate entre ciberseguridad y libertades individuales en el Internet. Por último, se abordan las consecuencias políticas y económicas de las revelaciones de Snowden en el contexto de la ciberseguridad, tanto para actores estatales –Estados Unidos y la Unión Europea– como para actores no estatales –empresas y el público en general–.

Materiales y métodos

El desarrollo del presente análisis partió de una revisión de la literatura existente sobre el caso tratado y en torno a la vinculación entre ciberseguridad y derechos humanos. Para ello, se inició con una revisión sistemática exploratoria analítica de revistas indexadas, libros y diarios destacados sobre los incidentes de espionaje y ciberseguridad relacionados con el caso Snowden mediante el método deductivo. Paso siguiente, con ayuda del método inductivo se procedió a vincular y sintetizar los hechos más relevantes con visiones conceptuales basadas en teorías de seguridad y de la economía política internacional.

De esta forma, tras una detenida revisión de fuentes bibliográficas, se logró identificar la cronología de los hechos del caso Snowden y la impor-

tancia del debate de la ciberseguridad y de las libertades individuales en el Internet. Una vez estudiados dichos elementos, se pudo visibilizar la manera en que dichos componentes encajan dentro de un marco conceptual que analiza y explica las respuestas de diferentes actores ante la evolución de la dinámica entre seguridad y derechos humanos dentro y fuera del ciberespacio para con ello, contestar la problemática que guía la investigación.

Discusión y resultados

El sistema de vigilancia masiva revelado por Snowden

El 6 de junio de 2013, los diarios The Guardian y The Washington Post inician una serie de publicaciones que explican el funcionamiento de una amplia red de vigilancia tecnológica de la NSA. De acuerdo con información de Edward Snowden, un exanalista de la NSA, dicha red accedía a la información personal de millones de personas en todo el mundo a través de tres diferentes tipos de recolección de información: intercepción de información mediante cables submarinos de Internet y empresas de telecomunicaciones; almacenamiento de *metadatos* de la navegación en Internet y llamadas telefónicas; y vigilancia direccionada a teléfonos de líderes políticos mundiales, junto con aplicaciones de control a distancia.[2] La NSA, a través de estos programas, vigilaba la información que se extendía desde las redes sociales, llamadas telefónicas o correos electrónicos, hasta la información almacenada en repositorios digitales online.

En primer lugar, la intercepción de cables submarinos de Internet, con programas como *Upstream* o *Tempora*, involucraba la implementación de interceptores en los cables de fibra óptica de conexiones propias y de otros países, como Reino Unido, Francia y Alemania.[3] La recolección de información también se realizaba a través de empresas de telecomunicaciones y redes sociales, como *Google*, *Skype* o *Facebook*, mediante programas tales

2. Ewen MacAskill, "NSA paid millions to cover Prism compliance costs for tech companies", *The Guardian*, 23 de agosto de 2013; James Ball,"Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data", *The Guardian*, 28 de enero de 2014; Peter Taylor, "Edward Snowden interview: 'Smartphones can be taken over'", *BBC*, 5 de octubre de 2015.
3. MacAskill, "NSA paid millions to cover Prism compliance costs for tech companies".

como *Xkeyscore* y PRISM.[4] En esta práctica se forzaba a empresas privadas a recolectar regularmente información personal para ser luego entregada a los servicios de inteligencia. Además, con ello era posible monitorear la información de usuarios específicos sin su autorización legal o el conocimiento de sus usuarios.[5] De acuerdo con Minin,[6] la capacidad de intercepción del Internet de los diferentes programas de vigilancia podía llegar a cubrir hasta el 75 % del tráfico de Internet en territorio estadounidense.

Segundo, la práctica del almacenamiento de datos e información sobre la navegación en Internet y llamadas telefónicas, también conocida como recolección de *metadata*, consistía en la recolección de datos relacionados al historial de las páginas web visitadas, la ubicación, preferencias y tiempo de permanencia en un portal web. De igual manera, la *metadata* de llamadas telefónicas almacenaba información sobre los contactos, la duración de la llamada, la frecuencia de contacto y horarios. Esto también se producía con respecto a mensajes de texto y otras señales de audio y video que se transmitían por computadores y teléfonos inteligentes.[7] Con la información recolectada se generaban redes inteligentes para revelar patrones de comportamiento y vinculación de los usuarios.[8]

Tercero, y posiblemente una de las razones que más repercutió en la esfera política, se encuentra la vigilancia direccionada a teléfonos de líderes políticos mundiales. De acuerdo con las revelaciones, la NSA estableció una red de vigilancia a 35 jefes de Estado, particularmente en la Unión Europea, como en el caso del expresidente François Hollande y la canciller alemana Ángela Merkel, así como en el grupo de los BRICS conformado por Brasil, Rusia, India, China y Sudáfrica.[9] Igualmente, se reveló la exis-

4. James Ball,"Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data", *The Guardian*, 28 de enero de 2014.
5. Gleen Greenwald, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, 6 de junio de 2013.
6. Dimitry Minin, "Revelations of Edward Snowden – Geopolitics and Lessons to Draw", *Strategic Culture Foundation*, 28 de octubre de 2013.
7. MacAskill, "NSA paid millions to cover Prism compliance costs for tech companies"; Ball,"Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data"; Taylor, "Edward Snowden interview: 'Smartphones can be taken over'".
8. Edward Snowden, "Here's how we take back the Internet", Entrevistado por Chris Anderson, *TED Talks*, 2014.
9. Claudi Pérez y Lucía Abellán, "Estados Unidos espió los teléfonos móviles de 35 líderes mundiales", *El País*, 25 de octubre de 2013.

tencia de aplicaciones de control a distancia que pueden encender un equipo celular, revisar información almacenada y enviar datos sobre su ubicación, de manera que se transforman en un receptor de las conversaciones del usuario.[10]

Las revelaciones del caso Snowden constituyen un punto de inflexión en cuanto a revelaciones de material confidencial por la cantidad de programas expuestos y especialmente por la manera en que se produjeron.[11] Así, la dinámica de las revelaciones constituyó en una de las claves que reposicionó la visión de seguridad sobre la vigilancia digital que hizo posible cambios en el uso de información digital a nivel global, a diferencia de otras revelaciones digitales. En efecto, a continuación se presentan las diferencias entre las revelaciones de Snowden y las conocidas filtraciones de Wikileaks.

Las filtraciones de Wikileaks –caso Assange– envuelven la revelación de distintos cables diplomáticos sobre el comportamiento militar estadounidense, las comunicaciones de embajadas estadounidenses, y la vigilancia dentro de Naciones Unidas.[12] En este caso, es importante destacar que dichas revelaciones despertaron diversas críticas por parte de líderes políticos y periodistas. Como menciona Muñoz,[13] las filtraciones proporcionadas por Wikileaks se produjeron en un contexto apartado del periodismo tradicional, en el que no se realizaron procesos de verificación de datos o mención de fuentes. Además, no se contó con profesionales de medios de comunicación, como reporteros o procesos de edición, que garanticen mostrar la información con imparcialidad y de manera oportuna.[14] De igual manera, distintos gobiernos expresaron la necesidad de espacio confidencial para conversaciones diplomáticas y expresaron que por la manera en que se expusieron las filtraciones podían repercutir en los derechos y libertades de cientos de personas vinculadas en conflictos bélicos.[15]

---

10. Ball, "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data"; Taylor, "Edward Snowden interview: 'Smartphones can be taken over'".
11. Zygmunt Bauman, et.al, "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology* 8, n.º 2 (2014): 121-44.
12. Päivikki Karhula, "What is the effect of WikiLeaks for Freedom of Information?", *The International Federation of Library Associations and Institutions*, 5 de octubre de 2012.
13. Sergio Muñoz, "Las diferencias entre Assange y Snowden", *Letras Libres*, 15 de abril del 2019.
14. José Cervera, "Assange contra Snowden: parecidos y diferencias", *El Diario*, 6 de enero de 2014.
15. Karhula,"What is the effect of WikiLeaks for Freedom of Information?".

El caso Snowden, en cambio, sí contó con el respaldo de un proceso de verificación de fuentes y edición periodística en su proyecto de denuncia de las acciones de vigilancia masiva de la NSA. Con ello, diversos periodistas coinciden que se trató de una revelación sobre el abuso de autoridad en medios de comunicación profesionales, tales como los diarios The Guardian, The New York Times y The Washington Post.[16] Por ello, se destaca que se contó con el pleno conocimiento de la fuente de información primaria y que también existió un proceso de comprobación de los documentos revelados, puesto que el exanalista de la NSA consiguió la información por sí mismo y la presentó al periodista de The Guardian, Gleen Greenwald.[17] Además, las revelaciones mostraron las deficiencias de ciberseguridad de individuos y Estados, las cuales ocuparon un papel clave en el debate sobre seguridad y libertades en el Internet a nivel mundial, que, en consecuencia produjeron la modificación de la legislación americana y suspensión del programa de recolección de metadatos denunciado.[18]

Frente a las revelaciones del exanalista de la NSA, el 7 de junio de 2013, el entonces presidente Obama realizó una rueda de prensa sobre los programas de vigilancia revelados en los medios de comunicación.[19] En dicha declaración expresó que los programas de la NSA si existían mas no operaban de la manera en que se presentaron. Puntualizó además que nadie escuchaba las llamadas, ni interceptaba los mensajes y que todos los programas eran empleados para la lucha contra el terrorismo.[20] De manera similar, el 8 de junio de 2013, el Director Nacional de Inteligencia estadounidense, James Clapper, emitió una declaración sobre la recolección de datos de fuentes extranjeras. En dicho informe se estableció que el programa PRISM consistía en un sistema autorizado y legítimo para la recopilación de información, el cual se encontraba bajo la aprobación y supervisión de una corte federal especial para dichos asuntos.[21]

16. Gleen Greenwald, *No Place to Hide* (Nueva York: Metropolitan Books, 2014); Cervera, "Assange contra Snowden: parecidos y diferencias".
17. Muñoz, "Las diferencias entre Assange y Snowden".
18. Fatimetou Zahra Mohamed Mahmoud y Akram M. Zeki, "Edward Snowden disclosures turn the fears of surveillance into reality: the impact and transformation in information security", *Journal of Theoretical and Applied Information Technology* 83, n.º 2 (2016): 173-9.
19. Josh Richman,"President Obama defends surveillance programs in San José Speech", *The Mercury News*, 7 de junio de 2013.
20. Lucy Madison, "Obama: 'Nobody is listening to your telephone calls'", *CBS*, 7 de junio de 2013.
21. James Clapper, "Facts on the Collection of Intelligence Pursuant to Section 702", *Office of the Director of National Intelligence*, 8 de junio de 2013.

Con ello, la respuesta estadounidense sobre las revelaciones de Snowden consistió en dos posiciones generales. En primer lugar, se procedió a negar que los programas de la NSA atentaran contra los derechos y libertades de nacionales y extranjeros. Así también, se sostuvo que en ningún momento la agencia recurría a prácticas de espionaje a través de escuchas telefónicas, intercepción de correos electrónicos o vigilancia digital no autorizada por una orden legal. Segundo, el gobierno estadounidense, mediante fiscales generales, condenó las revelaciones hechas por el exanalista y presentó una denuncia penal en su contra por el robo de propiedad del gobierno, comunicación no autorizada de información nacional de defensa y la filtración de documentos de inteligencia ultra secretos a una persona no autorizada.[22] Estos cargos se realizaron con la alegación de que dichas acciones atentaban contra la protección de la seguridad nacional.

El debate de la ciberseguridad y respeto de las libertades individuales

En el presente estudio se ha evidenciado la existencia de un debate existente entre la búsqueda de la seguridad nacional y el respeto de derechos y libertades, particularmente en el entorno digital del Internet. Este ciberentorno es de reciente aparición y precisa de herramientas de análisis para entender y explicar el debate sobre las revelaciones del exanalista de la NSA. Para ello, en el acápite en cuestión se estudia la dinámica del Internet, la ciberseguridad, poder y hegemonía desde las visiones neoliberal y crítica de la economía política internacional (EPI), a modo de compaginar los conceptos para visualizar sus similitudes y complementación mutua en el caso de estudio.

En primer lugar, el Internet es definido como una "red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación".[23] Esta red tiene sus inicios en los años sesenta, durante el período de la Guerra Fría, cuando Estados Unidos establece una serie de interconexiones de redes para po-

22. Peter Finn y Sari Horwitz, "U.S. charges Snowden with espionage", *The Washington Post*, 21 de junio de 2013.
23. Real Academia Española, *Diccionario de la lengua española,* 23.ª ed., 2018.

der acceder a su información de índole militar remotamente.[24] A partir del establecimiento del denominado Protocolo TCP/IP, el Internet comenzó a crecer rápidamente superando a otros medios de comunicación hasta establecerse como la red de información y comunicación global más grande del siglo XXI.[25] Además, bajo esta dinámica, la red global funciona como medio de apalancamiento dada su capacidad de almacenamiento, acceso de información y comunicación instantánea. Así también, adquiere un valor estratégico por su capacidad de facilitar actividades en escenarios tan diversos, tales como negociaciones comerciales, la educación o un espacio de diálogo social a gran escala.[26]

En este sentido, con la llegada de los procesos de globalización, el Internet se consolida como un espacio de interacción mundial que acorta y disuelve las barreras estatales y políticas. Dentro de este ciberespacio se fomentan las relaciones intergrupales e individuales, se visibilizan los sucesos locales a nivel mundial y se crea un entorno de desarrollo económico y modernización social, donde Estados, corporaciones e individuos participan libremente.[27] Adicionalmente, el Internet sirve como sitio clave para el almacenamiento de sistemas críticos de información de sus actores –Estados, corporaciones, individuos–. Dichos actores son cada día más dependientes de tal entorno por la facilidad de almacenamiento y acceso a información de valor a cualquier hora y desde cualquier lugar.[28]

No obstante, al hablar del Internet surge también la problemática del estado de naturaleza de libertad perfecta, en la que no existe una autoridad central aparente que haga las veces de un Estado soberano para establecer normas básicas de convivencia, con respeto de los derechos de quienes interactuaran en su espacio virtual y su seguridad. Por ende, sus actores pueden realizar actividades positivas o negativas entre sí, que impactan en el mundo real.[29] De esta forma, se crea la noción de *ciberseguridad*, que, según la Unión Internacional de Comunicaciones, es definida como "el conjun-

24. Andrés Delgado, "Gobernanza del Internet en Ecuador: Infraestructura y acceso", *Encuentro Nacional de Gobernanza del Internet en Ecuador 2014*, noviembre 2014.
25. Ibíd.
26. Robert Keohane y Joseph Nye, *Poder e Interdependencia: La Política Mundial en Transición* (Buenos Aires: Grupo Editor Latinoamericano, 1988).
27. Delgado, "Gobernanza del Internet en Ecuador".
28. Sally Burch,"La Gobernanza mundial de Internet", *Línea Sur* 3, n.º 9 (2015): 23-36.
29. Ibíd.

to de herramientas políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones formación y practicas idóneas que se pueden utilizar para proteger los activos de la organización y los usuarios en el ciberentorno"[30] Así, en la era de la información, la ciberseguridad desempeña un aspecto clave al configurarse como una quinta dimensión del conflicto moderno.[31]

Por ende, los ataques producidos en el Internet son considerados como embestidas de origen social o político y su impacto alcanza a organizaciones estatales y no estatales, así como a personas.[32] Dada la importancia de la información, diversas entidades establecen medidas de control a partir del monitoreo del tráfico en Internet.[33] Sin embargo, la estructuración de la información en su monitoreo da paso a que los datos privados pasen obligatoriamente por servidores de control mayormente estadounidense, lo que crea la posibilidad de ser atacado por hackers a través de sus procesos de robo digital.[34] De esta forma, se presenta una dinámica de poder en la información digital, la cual no solo acarrea información sobre vínculos sociales básicos, sino que también comprende información estratégica que puede moldear la dinámica de los mercados internacionalmente. En ese sentido, se pueden afectar las políticas y regulaciones de diferentes países, en la medida que se comprometa su valor, dado que ninguna información está exenta de ser violentada.[35]

Por tanto, nace el discurso de la vigilancia masiva en el Internet para la defensa de los intereses estatales en el ciberespacio. De acuerdo con Carracedo,[36] dicha arquitectura digital de control es similar a la de un súper panóptico virtual, que ejecuta un sistema de vigilancia descentralizado a manera de control normalizador de la sociedad. De acuerdo con Foucault,[37]

---

30. Jennie Lincoln, "Ciber-seguridad en Cultura de Inteligencia", *Cultura de Inteligencia* (2014): 329.
31. Robert Vargas Borbúa, Luis Recalde Herrera y Rolando P. Reyes Ch., "Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa", *URVIO, Revista latinoamericana de Estudios de Seguridad*, n.º 20 (2017): 31-45.
32. Lincoln, "Ciber-seguridad en Cultura de Inteligencia".
33. Feibert Guzmán, "Impacto del cibercrimen: bajo la realidad aumentada", *Memorias Congreso Internacional Crimen económico y fraude financiero y contable*, n.º 2 (2017): 67-79.
34. Ibíd.
35. Vargas, Recalde y Reyes, "Ciberdefensa y ciberseguridad, más allá del mundo virtual".
36. José-David Carracedo,"La vigilancia en sociedades de la información. ¿Un panóptico electrónico?", *Política y Sociedad* 39, n.º 2 (2002): 437-55.
37. Michel Foucault,*Vigilar y Castigar: nacimiento de la prisión* (Argentina: Siglo XXI Editores Argentina, 2002).

el panóptico es un sistema de vigilancia centralizada que se instauró en las cárceles como una forma de control normalizadora y que se extrapola también a la sociedad e incluso al entorno internacional. Esta es una medida que busca el aprovechamiento y direccionamiento de las masas en pro del mejoramiento de las mismas en aspectos puntuales que precisen ser corregidos. El principal objetivo del panóptico consiste en lograr que todos los individuos de un entorno sean útiles, primero a sí mismos y, en consecuencia, al conjunto de la dinámica establecida en la sociedad.[38] Además, dicho sistema instrumentalizaba el poder de las fuerzas sociales a manera de un amplificador de la producción, del desarrollo económico y de la difusión de la instrucción, con el fin de elevar el nivel de moral pública que otorga la legitimidad a la hegemonía.[39]

Dentro del esquema del panóptico de Foucault se describe la idea de la inspección central y vigilancia omnipresente para cuatro objetivos específicos. Primero, se genera efectos de incertidumbre en el vigilado sobre la presencia física del vigilante y la instauración implícita del vigilante en la conciencia del interno.[40] Segundo, la celda se convierte en un espacio de asilamiento o experimentación donde se administran procedimientos correctivos necesarios. Tercero, se establecen clasificaciones de tipo moral y racional sobre el comportamiento de los individuos vigilados. Por último, se plantea un principio de transparencia y deber que sugiere la necesidad de diseñar una estructura centralizada para vigilar a los internos y la posibilidad de que dicho trabajo estatal sea fiscalizado por el pueblo; de forma que cualquier miembro de la sociedad tendría derecho a comprobar cómo funcionan dichas instituciones.[41]

De esta forma, el panóptico global se concibe por la gestión descentralizada de información necesaria para temas de averiguación, autentificación, gestión económica, financiera, social y de seguridad.[42] Así, las revelaciones de Snowden explican que se había establecido un medio de control hegemónico mediante las grandes transnacionales de telecomunicaciones, como *Google* o *Facebook*, con un sistema que buscaba recopilar y gestionar

38. Ibíd.
39. Carracedo,"La vigilancia en sociedades de la información".
40. Ibíd.
41. Ibíd.
42. Ibíd.

los datos de millones de usuarios para suplir necesidades del comercio, la lucha contra el crimen y terrorismo. En efecto, en el caso de que un actor se *desviase* de los intereses hegemónicos en dicha arquitectura, sería fácilmente localizable para ser corregido por su *propio* bien.[43]

De esta manera, la dinámica estratégica de la ciberseguridad del Internet del gobierno de Obama se consolidó a través de mecanismos digitales de posicionamiento hegemónico de control sobre el ciberespacio. Dicho sistema se valió de la capacidad norteamericana de poder inteligente al combinar la producción intelectual tecnológica y el poderío económico en tres frentes puntuales.[44]

Primero, se encuentra la monopolización de servicios digitales por compañías de telecomunicaciones, como *Google*, *Facebook*, *Hotmail*, *Amazon* o *WhatsApp*. Mediante tales empresas se absorbe y opaca a otras compañías de actividades similares, así como también se aglutina aproximadamente el 90 % del flujo de telecomunicaciones mundiales.[45] Segundo, se divisa la imposición de normas digitales y el control sobre las patentes de plataformas digitales. En este campo se destaca el control que ejerce el idioma inglés en el lenguaje de programación, el cual da vida a la comunicación online, al igual que los derechos de autor sobre la construcción de plataformas modernas de información. Tercero, la dominación es ejercida mediante proyectos de vigilancia masiva que han cobrado fuerza y visibilidad en los últimos años, sobre todo tras las revelaciones del caso de estudio.[46] Además, existe una tendencia de diferentes plataformas a solicitar información personal adicional para el acceso al servicio, por ejemplo un número de teléfono o ubicación física a tiempo real.[47]

---

43. Antonio Gramsci, *Further selections from the prison notebooks* (Londres: Electric Book Company, 2001); Carracedo,"La vigilancia en sociedades de la información. ¿Un panóptico electrónico?"; Foucault, *Vigilar y Castigar*.
44. Felicity Ruby, "Cinco Ojos sobre el Planeta", *Línea Sur* 3, n.º 9 (2015): 37-51; Burch,"La Gobernanza mundial de Internet"; Vargas, Recalde y Reyes, "Ciberdefensa y ciberseguridad, más allá del mundo virtual".
45. Bauman, et.al., "After Snowden: Rethinking the Impact of Surveillance"; Delgado, "Gobernanza del Internet en Ecuador"; María Fernanda Espinosa, "Espionaje electrónico: implicaciones en la protección de las soberanías y los Derechos Humanos", *Línea Sur* 2, n.º 6 (2013): 55-62.
46. Bauman, et.al., "After Snowden: Rethinking the Impact of Surveillance".
47. Kriti Singh, "Understanding Augmented Reality (AR) Game and its Implications on Security", *Centre for Air Power Studies*, 3 de octubre de 2016.

En efecto, dichas revelaciones desataron el enojo de diversos líderes internacionales, entre ellos, la canciller alemana Ángela Merkel, el expresidente francés François Hollande y la expresidenta de Brasil, Dilma Rousseff.[48] Dichos mandatarios enfatizaron que la vigilancia socavaba la reacción de confianza de sus países con la nación norteamericana, así como la dinámica económica bajo la cual establecían negociaciones, acuerdos o relaciones de confianza, que autorizaban el almacenamiento de información sensible en servidores estadounidenses.[49] De esta forma, los líderes estatales y la sociedad civil posicionaron su firme intención de establecer medidas para responder a las políticas hegemónicas de ciberseguridad estadounidense, las cuales serán analizadas en el siguiente apartado.

Respuestas estatales y no estatales al espionaje

Siguiendo el argumento previamente expuesto, tras las revelaciones de Snowden, la comunidad europea, en especial, Alemania y Francia, posicionaron mecanismos de respuesta contra hegemónica en las esferas político-social, legal, tecnológica y comercial. Dichas contestaciones significaron el detrimento del poder estadounidense tanto en sus niveles de accionar duro y blando, como en su estructura de dominación hegemónica establecida.

En primer lugar, las revelaciones sobre el accionar estadounidense en la gobernanza del Internet significaron una pérdida significante del poder blando norteamericano, representado por la caída del nivel de confianza de los ciudadanos, sobre todo europeos, en los sistemas de información americanos. Es así que un sondeo realizado por la empresa de análisis de datos Annalect,[50] reveló que más de la mitad de usuarios del Internet (europeos y americanos) se mostraron preocupados por la falta de privacidad en la red luego de las revelaciones de Snowden.

48. Bauman, et.al., "After Snowden: Rethinking the Impact of Surveillance".
49. Ian Traynor, "NSA spying row: bugging friends is unacceptable, warn Germans", *The Guardian*, 1 de julio de 2013.
50. Annalect, "Annalect Q2 2013 Online Consumer Privacy Study Americans' Concerns About the Privacy of Online Information Jump in the Wake of NSA Disclosures", *Annalect*, 2013.

Similarmente, la tercera parte de los encuestados afirmó que tomó medidas de seguridad para proteger su privacidad cambiando los ajustes de seguridad de buscadores, aplicaciones de geolocalización, el uso de cookies y modificando información de redes sociales.[51]

De igual manera, una encuesta llevada a cabo por la empresa Angus Reid Group y el diario Die Welt reveló que la confianza del público alemán hacia Estados Unidos descendió de un 76 %, que se mantenía en la visita de Obama en el 2009, a un 35 %, luego de las declaraciones del sistema de espionaje.[52]

En el aspecto político, a la luz de las revelaciones de Snowden, los principales representantes europeos del momento, la canciller alemana Angela Merkel, el presidente francés Hollande y el Parlamento Europeo, especificaron que Estados Unidos debía cambiar su accionar para continuar con las negociaciones comerciales con sus países y restaurar la confianza perdida.[53] En ese sentido, si bien la interdependencia compleja sugiere que las relaciones comerciales interdependientes dificultan la posibilidad de conflicto a raíz de las revelaciones, también establece que la pérdida de confianza o poder blando repercute en el margen de acción estadounidense para conseguir resultados favorables en escenarios de negociación.[54]

En segundo lugar, a partir de dichos incidentes, el Parlamento Europeo impulsó una serie de resoluciones[55] en las que reconoció la importancia de la cooperación entre Estados Unidos y la Unión Europea en la lucha contra el terrorismo. No obstante, señaló su inquietud por el espionaje y lo caracterizó como una violación a la privacidad y protección de los datos de los ciudadanos europeos. Por tal motivo, se incentivó la creación de un fondo para la consolidación de servidores y plataformas digitales europeos con la

51. Ibíd.
52. Spiegel Online, "German Trust in United States Plummets", *The Spiegel*, 8 de noviembre de 2013.
53. Jonathan Marcus, "Hollande: Bugging allegations threaten EU-US trade pact", *BBC*, 1 de julio de 2013; Parlamento Europeo, *Resolución sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE*, 4 de julio de 2013. P7_TA(2013)0322; Toni Paterson, "Surveillance revelations: Angela Merkel proposes European network to beat NSA and GCHQ spying", *The Intedepdent*, 16 de febrero de 2014.
54. Keohane y Nye, *Poder e Interdependencia: La Política Mundial en Transición*.
55. Las resoluciones del Parlamento Europeo fueron: P7_TA(2013)0322, P7_TA(2013)0449 y P7_TA(2014)0230.

finalidad de reducir la dependencia de servidores estadounidenses y procurar la libertad y privacidad de sus ciudadanos y residentes.[56]

Paralelamente, en la 68ª Asamblea General de Naciones Unidas, Brasil y Alemania señalaron que las actividades de espionaje virtuales atentan contra la soberanía estatal y que bajo ningún concepto de lucha por la seguridad y soberanía, se debe transgredir la seguridad y derechos de otros estados soberanos.[57] En efecto, diversos países propusieron un proyecto conjunto de ciberdefensa para el uso de sistemas de software alternativos destinados a proteger la integridad de la información sensible, mediante sus propios sistemas de cables de fibra óptica.[58] De esta manera, se instó a la generación de políticas de democratización del Internet para evitar tanto la monopolización de los sistemas tecnológicos, como la sensibilidad a los ataques externos de hackers y el acceso en condiciones igualitarias a la red.[59] Con tal medida, además, se buscó establecer mecanismos supranacionales de respuesta hegemónica que rectifiquen los desequilibrios de la red y establezcan sanciones a comportamientos agresivos contra los actores en uso de dicho sistema.[60]

En tercer lugar, fruto de los planteamientos sociopolíticos y legales explicados, se generó una suerte de nueva hegemonía y estrategia de ciberseguridad a nivel europeo. Esta respuesta, se evidenció en el cambio progresivo de la estructura de ciberseguridad de una visión de seguridad estatal a una de lucha en pro de la seguridad humana, basada en la transparencia y participación en los procesos.[61] Así, a nivel tecnológico y económico, se evidenció una nueva producción de redes informáticas vinculadas a los servicios de comercio y de almacenamiento de información reservados para la zona europea. Esta iniciativa de respuesta se produjo también a través de la

56. Parlamento Europeo, *Resolución sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE*, 4 de julio de 2013, P7_TA(2013)0322, *Resolución sobre la Suspensión del acuerdo SWIFT como resultado de la vigilancia de la Agencia Nacional de Seguridad de los EE.UU.*, 23 de octubre de 2013, P7_TA(2013)0449., Resolución sobre la liberación del potencial de la computación en la nube en Europa, 10 de diciembre de 2013, P7_TA(2013)0535.
57. Bauman, et.al., "After Snowden: Rethinking the Impact of Surveillance".
58. Burch, "La Gobernanza mundial de Internet".
59. Delgado, "Gobernanza del Internet en Ecuador".
60. Burch, "La Gobernanza mundial de Internet".
61. Daniel Castro y Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness", *Information Technology & innovation Foundation*, 9 de junio de 2015.

creación e implementación de aplicaciones y sistemas informáticos alternos, así como con la relocalización de servidores digitales destinados a servicios de comercio e infraestructuras críticas; todo esto para evitar la injerencia de las leyes norteamericanas en su información.[62]

De esta forma, las revelaciones de Snowden influenciaron políticas digitales tanto en la sociedad civil como en los líderes de la Unión Europea y países como Brasil, los cuales decidieron cambiar sus políticas de almacenamiento y gestión de información digital personal. Por tanto, servidores de diferentes empresas –*Hotmail*, *Dropbox*, *Google*, *IBM* o *CISCO*–, que tradicionalmente gestionaban el 90 % de la información depositada en plataformas de almacenamiento en nube –mediante servidores localizados en territorio estadounidense–, tuvieron que iniciar un proceso de restructuración.[63] Con ello, las empresas se desplazaron a otros territorios, mientras que otras compañías establecieron sus propias plataformas virtuales de información.[64]

De acuerdo con un estudio realizado por *The Information Technology & Innovation Foundation*, la pérdida de confianza de la sociedad civil europea y el deseo de respuesta social contra el control hegemónico estadounidense en las empresas digitales de almacenamiento en nube, se evaluó en pérdidas de entre USD 21, 5 a 35 mil millones entre 2013 y 2017.[65] También existieron costos económicos significativos adicionales en empresas localizadas en territorio estadounidense. Diversas empresas, tales como *Facebook*, *Whats App*, *Hotmail* o *Google*, se vieron forzadas a reformar sus políticas de recolección de metadata y establecer cambios en sus sistemas de almacenamiento.[66] Igualmente, el 17 de enero de 2014, Obama presentó modificaciones a las leyes y ordenó que se cierre el programa de almacenamiento de metadatos por el gobierno.[67]

---

62. Ibíd.
63. Guzmán, "Impacto del cibercrimen: bajo la realidad aumentada".
64. Castro y McQuinn, "Beyond the USA Freedom Act".
65. Dicha cifra aproximada y de difícil especificación se debe a la naturaleza de los mercados digitales internacionales, donde diversas empresas mencionaron pérdidas estimadas y costos de relocalización de sus servidores fuera del territorio estadounidense; Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry?", *The Information Techonogy & Innovation Foundation*, 5 de Agosto 2013.
66. Ibíd.
67. The White House, "FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program", *The White House*, 27 de marzo de 2014.

De igual manera, es importante destacar que Estados Unidos sufrió un revés en su influencia política y económica luego de que la UE estableciera nuevas normas sobre el uso de protocolos de intercambio de información en el denominado *Safe Harbor*. Esto resultó en complicaciones para el proceso de negociación del acuerdo transpacífico de libre comercio (TTIP). Consecuentemente, dicho tratado no logró llegar a un acuerdo base entre las dos economías previo a la transición del gobierno de Obama al de Trump (quién más adelante canceló por completo dicha negociación).[68] Además, el supervisor de la protección de datos de la UE o *European Data Protection Supervisor*, emitió un informe en el que establecía que para el 2011, la información de clientes europeos almacenada en servidores estadounidense se valoraba en 315 millones de euros; cifra que Estados Unidos no recuperaría con el cambio de servidores de los diferentes países.[69]

En conjunto, la respuesta europea a nivel, social, político, económico y tecnológico significó un revés en la hegemonía estadounidense, al forzar el cambio en los sistemas digitales estadounidenses que tuvieron influencia directa en el sistema estructural de ciberseguridad americano, así como en su poder duro y blando sobre el Internet. Dada la relación asimétrica de interdependencia económica de ambos socios, Estados Unidos y sus empresas transnacionales de telecomunicación se vieron en la necesidad de adaptar sus políticas de ciberseguridad y de ceder poder de influencia, para facilitar el retorno de la dinámica de cooperación eficaz entre dichos actores, previo a las revelaciones de vigilancia.

De esta forma, se evidencia la estrategia de contestación hegemónica generada por las políticas adoptadas por actores como la Unión Europea y la pérdida de poder estadounidense. Tal contestación se produce como resultado de las acciones de un actor no estatal que se apoyó en los medios de comunicación internacionales para apalancar su voz y generar un sentimiento de malestar en el statu quo de momento. Así, se produjo un cambio en la agenda política internacional y también se afectó a la economía esta-

68. Comisión Europea, "Transatlantic Trade & Investment Partnership Stakeholder Presentations Event", *Trade Europa-European Commission*, 12 de marzo de 2014.
69. EDPS, "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", *The European Data Protection Supervisor*, 26 de marzo de 2014.

dounidense y su sistema de recolección y estructuración información, establecido como un súper panóptico digital.

Conclusiones

En conclusión, luego de estudiar el funcionamiento del sistema de vigilancia masiva denunciado por Snowden y las diversas respuestas que surgieron ante dicha estructura, se evidenció que un actor no estatal, como Snowden, a partir del apalancamiento tecnológico de la globalización, denunció una estructura de control estatal. Con ello, se produjo la alteración de la agenda política internacional de seguridad, así como la generación de conciencia en la ciudadanía y Estados sobre el uso y protección de la información privada. Además, las revelaciones jugaron un papel clave en cambios estructurales que tuvieron efectos económicos y legales en Estados Unidos y en su sistema de recolección y estructuración de información. De esta manera, Estados, individuos y empresas responden a la problemática de seguridad y del respeto de derechos y libertades de dos maneras primordiales: la primera consistió en la denuncia de altercados a los derechos y la segunda se basó en la respuesta tecnológica de seguridad ante los sistemas revelados.

Por una parte, actores como la Unión Europea y su sociedad civil denunciaron que las prácticas de vigilancia atentaban contra los derechos y libertades y retiraron considerablemente su confianza en servicios y sistemas estadounidenses. Esto se presentó principalmente en las declaraciones oficiales del parlamento europeo, las de diferentes jefes de Estado y en encuestas realizadas a la sociedad civil. Por otra parte, las revelaciones también generaron una respuesta tecnológica y comercial, en la que Estados, empresas y el público en general alteraron sus prácticas de ciberseguridad. Así, Brasil y la Unión Europea fueron motivados a establecer sistemas de comunicación y servidores alternativos para su interacción en Internet. Las personas, también, conscientes de los riesgos en la red, cambiaron sus preferencias de seguridad y de servicios web. Similarmente, diversas empresas estadounidenses adquirieron la necesidad de desplazar sus servidores a otros países para recuperar confianza y evitar pérdidas mayores en servicios digitales, como lo es el almacenamiento en nube.

El caso de estudio mostró la importancia de considerar adecuadamente el rol de los actores estatales y no estatales en pro de la seguridad humana

y no simplemente en función de intereses hegemónicos individuales, dado que la comunidad internacional se enfrenta cada día a problemáticas más difíciles y novedosas, tales como el terrorismo o los ciberataques en Internet. Asimismo, la dinámica de vigilancia masiva se puede entender como un medio poder para la dominación a través de un sistema de súper panóptico digital. Por ende, con las revelaciones de Snowden y el cambio de las políticas de seguridad, se marcó un hito en la dinámica de poder económico y político del sistema internacional, provocando un retroceso en el poder de la NSA y un mejoramiento en la percepción del bienestar económico y social internacional. Todo esto, en una época donde el avance tecnológico desarrolla al Internet como un entorno cada vez menos anónimo, por lo que el respeto de los derechos en dicha plataforma se vuelve un factor más decisivo sobre el futuro del poder y sistema mundial.

Bibliografía

Annalect. "Annalect Q2 2013 Online Consumer Privacy Study Americans' Concerns About the Privacy of Online Information Jump in the Wake of NSA Disclosures". 2013. ‹https://bit.ly/37qq5Qr›.

Ball, James. "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data". *The Guardian*. 28 de enero de 2014. ‹https://bit.ly/38DdaLa›.

Bauman, Zygmunt, Didier Bigo, Paulo Esteve, Elspeth Guild, Vivienne Jabri, David Lyon, y R. B. J. Walker. "After Snowden: Rethinking the Impact of Surveillance". *International Political Socilogy* 8, n.º 2 (2014): 121-44. doi:10.1111/ips.12048.

Burch, Sally."La Gobernanza mundial de Internet". *Línea Sur* 3, n.º 9 (2015): 23-36.

Carracedo, José-David. "La vigilancia en sociedades de la información. ¿Un panóptico electrónico?". *Política y Sociedad* 39, n.º 2 (2002): 437-55.

Castro, Daniel. "How Much Will PRISM Cost the U.S. Cloud Computing Industry?", *The Information Techonogy & Innovation Foundation*. 5 de Agosto 2013. ‹https://bit.ly/2Glgqi6›.

Castro, Daniel y Alan McQuinn. "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness". *Information Technology & innovation Foundation*. 9 de junio de 2015. ‹https://bit.ly/36stXPj›.

Cervera, José. "Assange contra Snowden: parecidos y diferencias". *El Diario*. 6 de enero de 2014. ‹https://bit.ly/36kxQ9f›.

Clapper, James. "Facts on the Collection of Intelligence Pursuant to Section 702". *Office of the Director of National Intelligence*. 8 de junio de 2013. ‹https://bit.ly/2Gqx9Ap›.

Comisión Europea. "Transatlantic Trade & Investment Partnership Stakeholder Presentations Event". *Trade Europa - European Commission*. 12 de marzo de 2014. ‹https://bit.ly/30P1su0›.

Delgado, Andrés. "Gobernanza del Internet en Ecuador: Infraestructura y acceso". *Encuentro Nacional de Gobernanza del Internet en Ecuador 2014*. Noviembre 2014. ‹https://bit.ly/38BgZjR›.

EDPS. "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy". *The European Data Protection Supervisor*. 26 de marzo de 2014. ‹https://bit.ly/2Gh7dYd›.

Espinosa, María Fernanda. "Espionaje electrónico: implicaciones en la protección de las soberanías y los Derechos Humanos". *Línea Sur* 2, n.º 6 (2013): 55-62.

Finn, Peter y Sari Horwitz. "U.S. charges Snowden with espionage". *The Washington Post*. 21 de junio de 2013. ‹https://wapo.st/37mUJdu›.

Foucault, Michel. *Vigilar y Castigar: nacimiento de la prisión*. Argentina: Siglo XXI Editores Argentina, 2002.

Gramsci, Antonio. *Further selections from the prison notebooks*. Londres: Electric Book Company, 2001.

Greenwald, Gleen. "NSA Prism program taps in to user data of Apple, Google and others". *The Guardian*. 6 de junio de 2013. ‹https://bit.ly/30NWGgz›.

_____. *No Place to Hide*. Nueva York: Metropolitan Books, 2014.

Guzmán, Feibert. "Impacto del cibercrimen: bajo la realidad aumentada", *Memorias Congreso Internacional Crimen económico y fraude financiero y contable*, n.º 2 (2017): 67-79. doi: 10.22209/Cice.n2a08.

Karhula, Päivikki. "What is the effect of WikiLeaks for Freedom of Information?". *The International Federation of Library Associations and Institutions*. 5 de octubre de 2012. ‹https://bit.ly/30NLYXo›.

Keohane, Robert y Joseph Nye. *Poder e Interdependencia: La Política Mundial en Transición*. Buenos Aires: Grupo Editor Latinoamericano, 1988.

_____. "Power and Interdependence in the Information Age". *Foreign Affairs*, n. º 5 (1998): 81-94.

Lincoln, Jennie. "Ciber-seguridad en Cultura de Inteligencia". *Cultura de Inteligencia* (2014): 328-35.

MacAskill, Ewen. "NSA paid millions to cover Prism compliance costs for tech companies". *The Guardian*. 23 de agosto de 2013. ‹https://bit.ly/3aHlZFq›.

Madison, Lucy. "Obama: 'Nobody is listening to your telephone calls'". *CBS*. 7 de junio de 2013. ‹https://cbsn.ws/3ayHOHc›.

Marcus, Jonathan. "Hollande: Bugging allegations threaten EU-US trade pact". *BBC*. 1 de julio de 2013.‹ https://bbc.in/2tEwQ2x›.

Menéndez, Teresa. "40 millones de ciberataques tras detención de Assange". *Ecuavisa*. 15 de abril de 2019. ‹https://bit.ly/38zG1jo›.

Minin, Dimitry. "Revelations of Edward Snowden – Geopolitics and Lessons to Draw". *Strategic Culture Foundation*. 28 de octubre de 2013. ‹https://bit.ly/3aFKUcv›.

Mohamed Mahmoud Fatimetou Zahra y Akram M. Zeki, "Edward Snowden disclosures turn the fears of surveillance into reality: the impact and transformation in information security". *Journal of Theoretical and Applied Information Technology* 83, n.º 2 (2016); 173-79.

Muñoz, Sergio. "Las diferencias entre Assange y Snowden". *Letras Libres*. 15 de abril del 2019. ‹https://bit.ly/36rmeB8›.

Parlamento Europeo. *Resolución sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE*. 4 de julio de 2013. P7_TA(2013)0322. ‹https://bit.ly/2NYeU9I›.

———. *Resolución sobre la Suspensión del acuerdo SWIFT como resultado de la vigilancia de la Agencia Nacional de Seguridad de los EE.UU*. 23 de octubre de 2013. P7_TA(2013)0449. ‹https://bit.ly/38FMrxB›.

———. *Resolución sobre la liberación del potencial de la computación en la nube en Europa*. 10 de diciembre de 2013. P7_TA(2013)0535. ‹https://bit.ly/2TV5tvy›.

———. *Resolución sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos*. 12 de marzo de 2014. P7_TA(2014)0230. ‹https://bit.ly/3aHoRlG›.

Paterson, Toni. "Surveillance revelations: Angela Merkel proposes European network to beat NSA and GCHQ spying". *The Independent*. 16 de febrero de 2014. ‹https://bit.ly/2tMHXX3›.

Pérez, Claudi y Lucía Abellán. "Estados Unidos espió los teléfonos móviles de 35 líderes mundiales". *El País*. 25 de octubre de 2013. ‹https://bit.ly/36lCaEX›.

Real Academia Española, *Diccionario de la lengua española*, 23.ª ed. 2018. ‹https://dle.rae.es›.

Richman, Josh. "President Obama defends surveillance programs in San José Speech". *The Mercury News*. 7 de junio de 2013. ‹https://bayareane.ws/2vd3TLc›.

Ruby, Felicity. "Cinco Ojos sobre el Planeta". Línea Sur 3, n.º 9 (2015): 37-51.

Singh, Kriti. "Understanding Augmented Reality (AR) Game and its Implications on Security". *Centre for Air Power Studies*. 3 de octubre de 2016. ‹https://bit.ly/2tEBIVn›.

Snowden, Edward. "Here's how we take back the Internet". Entrevistado por Chris Anderson. *TED Talks*, 2014. ‹https://bit.ly/2GhdgMn›.

Spiegel Online. "German Trust in United States Plummets". *The Spiegel*. 8 de noviembre de 2013. ‹https://bit.ly/2Oc9atp›.

Taylor, Peter. "Edward Snowden interview: 'Smartphones can be taken over'". *BBC*. 5 de octubre de 2015. ‹https://bbc.in/2RrP1l7›.

The White House. "FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program". *The White House*. 27 de marzo de 2014. ‹https://bit.ly/37qICfc›.

Traynor, Ian. "NSA spying row: bugging friends is unacceptable, warn Germans". *The Guardian*. 1 de julio de 2013. ‹https://bit.ly/37rMGMy›.

Vargas Borbúa, Robert, Luis Herrera Recalde y Rolando P. Reyes Ch. "Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa". *URVIO, Revista latinoamericana de Estudios de Seguridad*, n.º 20 (2017): 31-45. doi: ‹10.17141/urvio.20.2017.2571›.