16. Trujillo, S., y Martinez, J. (s.f.). *Valoración de los riesgos ergonómicos por parte de las ARL cuando se desarrollan actividades de teletrabajo* (trabajo de grado). Bogotá: Politécnico Gran Colombiano - Facultad de Sociedad, Cultura y Creatividad - Programa de Gestión de la Seguridad y la Salud Laboral. Recuperado de: http://repository.poligran.edu.co/bitstream/handle/10823/1249/Art%C3%ADculo%20-%20TELETRABAJO.pdf?sequence=1&isAllowed=y.
17. Useche, D. (2013). *Las nuevas tecnologías y la disminución de la actividad física en el trabajo* (trabajo de grado). Bogotá: Universidad Nacional de Colombia - Facultad de Enfermería - Especialización en Salud Ocupacional. Recuperado de: http://bdigital.unal.edu.co/11678/3/lasnuevastecnologiasyladisminuciondelaactividadfisicaeneltrabajo.pdf.
18. Vaquero, C. (10 de enero, 2003). Ergonomía en la oficina: trabajo con videos terminales (PC). *Estrucplan*. Recuperado de: https://estrucplan.com.ar/ergonomia-en-la-oficina-trabajo-con-videos-terminales-pc/.

r.esici.11(20):347-357,2019

El ciberespacio, fuente de control y vigilancia para los ciudadanos[1]

Lina María Chaves Guerrero[2], *
Hugo Jurado Vásquez[3], **

Resumen

El Ciberespacio se considera como un espacio virtual que mantiene una conexión directa y constante de personas a través de redes; estas herramientas, además de traer grandes beneficios para un gobierno, ha generado actividades de cibercrimen y ciberseguridad, que ponen en peligro la seguridad nacional. Es por esto que varios países han tomado como medidas de protección el control y la vigilancia de esta herramienta, aunque esta estrategia da lugar a otros usos como la manipulación y la restricción de la información, situación que atenta contra un gobierno o que tiene su origen en algún tipo de ideología.

Palabras claves: seguridad nacional, ciberespacio, vigilancia, control, información de datos.

Clasificación JEL: Z0, O30, O34**.**

Cyberspace, a source of control and surveillance for citizens

Abstract

Cyberspace is considered as a virtual space that maintains a direct and constant connection of people through networks; These tools, in addition to bringing

[1] Artículo de investigación, correspondiente al proyecto de Guerra asimétrica.

[2] Estudiante de Comunicación social y periodismo, Universidad Sergio Arboleda, Bogotá, Colombia.

* linachaves14@gmail.com.

[3] Magister en Inteligencia Estratégica, Escuela de Inteligencia y Contrainteligencia - ESICI, Colombia; Ingeniero Electrónico Universidad ECCI, Colombia;

* orcid: https://orcid.org/0000-0001-8830-1139. hugo.jurado@outlook.com.

Fecha de recepción:
11 de febrero de 2019.

Fecha de aprobación:
18 de agosto de 2019.

Para citra este artículo:
Chaves, L. y Jurado, H. (2019). El ciberespacio, fuente de control y vigilancia para los ciudadanos. *Perspectivas en intgeligencia, 11*(20): 347-357.

great benefits to a government, have generated cybercrime and cybersecurity activities, which endanger national security. That is why several countries have taken the control and surveillance of this tool as protection measures, although this strategy gives rise to other uses such as manipulation and restriction of information, a situation that threatens a government or that has its origin in some kind of ideology.

Keywords: national security, cyberspace, surveillance, control, data information.

JEL classification: Z0, O30, O34.

Ciberespaço, fonte de controlo e vigilância para os cidadãos

Resumo

O ciberespaço é considerado como um espaço virtual que mantém uma conexão direta e constante das pessoas por meio de redes; Essas ferramentas, além de trazer grandes benefícios para o governo, geraram atividades de cibercrime e cibersegurança, que colocam em risco a segurança nacional. É por isso que vários países adotaram o controle e a vigilância dessa ferramenta como medidas de proteção, embora essa estratégia dê origem a outros usos, como manipulação e restrição de informações, situação que ameaça um governo ou que tem sua origem em algum tipo de ideologia.

Palavras-chave: ciberespaço, vigilância, controlo, informação de dados.

Classificação JEL: Z0, O30, O34.

"Las nuevas tecnologías de la información son un arma de doble filo:
aumenta nuestras capacidades y nuestro poder, pero a su vez hacen a sus usuarios
más vulnerables a la vigilancia y a la manipulación"
(Whitaker, 1999:128).

Introducción

El presente trabajo se propone dar respuesta a la pregunta ¿Cómo el gobierno tiene el control y el poder en el ciberespacio a fin de obtener una seguridad nacional? Para poder entender este interrogante con más claridad, se hablará primero de los conceptos claves que encierra, como *seguridad, seguridad nacional* y *ciberespacio,* los cuales disponen de varias definiciones que es posible que no encajen en muchos ámbitos.

La *seguridad* se define como un conjunto de sistemas, medios organizativos, humanos y acciones dispuestas a reducir y suprimir todo peligro y amenazas que puede afectar al ser humano, el Estado y a las entidades. Por consiguiente, el ser humano siempre anhela alcanzar una seguridad que le permita llegar a un área de confort frente a la convivencia de su comunidad. Écija (2014) afirma que "la seguridad no es estática, sino es un proceso de continuo movimiento". Para mantener esta seguridad el Estado ha formado una *seguridad nacional*, encargada de proteger los intereses del país. Para Caro (2011): "Tradicionalmente la seguridad nacional se ha concebido como el elemento garante de la identidad y supervivencia nacionales o, dicho otra forma de su independencia e integridad" (pp.50-51), como un concepto que hace parte de las cuatro dimensiones de defensa (tierra, aire, mar y espacio).

En el ámbito del espacio se ubica el ciberespacio, que Ramón (2018) define como: "realidad simulada o artificial de una persona en su entorno virtual y no físico, desarrollado a través de herramientas informáticas"; es decir que el ser humano utiliza esta herramienta para informarse y poder comunicarse con personas ubicadas a larga distancia, en tiempo real. Esta herramienta no solo trae beneficios de conocimiento y conexión, sino también se ha convertido en instrumento para la planificación de actividades ilegales, criminales y robo de información. En relación con esto último, algunos países han adoptado la restricción a la libertad de información y su accesibilidad en el ciberespacio como medidas de seguridad, con la finalidad de tener control sobre toda aquella a la que acceden sus ciudadanos.

El control del gobierno en el ciberespacio

El principal objetivo que tiene el gobierno para intervenir en el ciberespacio es su interés en la base de información que los ciudadanos exponen en la redes cada día pues, según lo que explican varios gobiernos, al tener dominio sobre esta información se garantiza un *control de importación en la opinión pública de sus ciudadanos,* lo que les permite tener un diagnóstico de los puntos de inconformidad de sus habitantes acerca del país, esto con el fin poder estructurar una estrategia de solución rápida y efectiva. Sin embargo, no en muchos países se cuenta con la opinión pública de sus connacionales en el ciberespacio; un ejemplo de ello es la República de Turquía, en donde se censura a las personas que tengan ideologías diferentes a las de su gobierno o que se expresen de una forma liderada en redes sociales; este comportamiento puede acarrear, como consecuencia, un juicio e incluso ser condenado a penas con cárcel.

Otro factor relevante para los estados es la *lucha contra el crimen*, pues son muchas las personas que difunden información falsa con el objetivo de robar bases de datos personales y fomentar delitos como los robos, los chantajes, la pornografía y demás acciones que ponen en riesgo la seguridad nacional. El gobierno, como se ha mencionado, están en la obligación de intervenir en este tipo de información, ya que expone la integridad de sus ciudadanos.

La política también se afecta desde el ciberespacio, es por eso que el gobierno tiene la responsabilidad de ejercer mayor control en este. Por ejemplo, en el año 2019, el mundo se sorprendió con la revelación del caso de Cambridge Analytica, una compañía que creó perfiles falsos con los datos de varias personas como una estrategia para manipular el proceso electoral de la campaña de Donald Trump; a pesar que este hecho vulneró los derechos de privacidad de muchos usuarios, el resultado fue la elección del ahora presidente Trump por una "fuerza colectiva", lo que demuestra que obtener la información de los ciudadanos asegura tener un control en las decisiones importantes del país.

La falsa libertad y el control en el ciberespacio

La mayoridad de usuarios piensa que tiene libertad ilimitada en el ciberespacio, ya que no se encuentra con una política de restricción que les impida entrar en diferentes plataformas y expresar opiniones, pero esta "libertad", que tanto se afirma no es real. Actualmente, ya es fuente de negocio que las páginas y portales web, redes sociales y plataformas vendan sus bases de datos a otras compañías, para ejercer actos considerados como manipulación. Un estudio elaborado por los servicios de protección forense Cifas y Forensic Pathways

demuestra que se vende información privada obtenidas de las redes sociales a personas que luego la utilizan para enviar contenido publicitario de servicios o productos –confirmado también por el portal "En TIC confío" del ministerio colombiano de Tecnologías de la Información y las Comunicaciones–:

> En una muestra de 30,000 víctimas de fraude de identidad, casi un tercio (8,646) se encontró en la web, con nombre, fecha de nacimiento, correo electrónico y número de teléfono. Más de dos tercios (69%) de las personas se encontraron en Facebook, con un 38% en Facebook y LinkedIn. Se encontró que, aunque los usuarios de 61 años o más tenían menor presencia en las redes sociales, eran más propensos a tener una cuenta comprometida a través de una violación de datos" (Cifas y Forensic Pathways, 2018).

Se comprobó que toda esta información adquirida de forma ilegal es entregada a dueños de empresas que utilizan los datos con el objeto de obtener más ganancias, que luego se vende a otras compañías con el mismo fin. Sin embargo, también se ha confirmado que no solo las empresas están vigilando constantemente a las personas, pues algunos gobiernos también están implicados en la vigilancia de los usuarios, a través de tecnologías que estos utilizan. Un ejemplo de ello es México, un país que es cliente principal de la empresa Hacking Team, compañía que ofrece servicios de espionaje a gobiernos y agencia del todo los países, con el fin de vigilar a sus ciudadanos y ejercer un control sobre ellos. Su servicio se basa en un software instalado en los cables de conexión que depura todo lo que está en el ciberespacio, es decir, que toda la información que se sube al mismo primero pasa por la agencia de gobierno encargada de esta función y ahí se hace una filtración de información en donde se decide cuál puede ser visualizada por sus ciudadanos; también permite que accedan un reporte diario de las búsquedas de información de sus habitantes, mediante la cual pueden diagnosticar la tendencia de información que ellos están recibiendo y qué tan válida es.

Dado que no solo utilizan software para la vigilancia sino además herramientas de tecnología que puede hacer mayor filtración a incluso un país en su totalidad, a continuación, se mencionarán algunas de las más utilizadas para el espionaje y vigilancia en el ciberespacio:

- *Echelon:* tiene acceso a más a 120 satélites de comunicaciones de las empresas, ciudadanos y gobierno. Según el periódico *RT en español* (2013), su mayor objetivo es espiar la inteligencia política económica y diplomática de otros países.
- *Comunicaciones por satélites:* toda señal que pasa por estos satélites se encuentra interceptada, lo que implica que toda la información del

ciberespacio llega a una torre de control, es revisada por el gobierno y allí se decide si apta para su publicación.

- *Comunicaciones sin satélite:* este sistema es controlado por una estación central que envía señales a un poste de red a más de 50 km., situación que involucra que únicamente se sube al ciberespacio lo que sea autorizado por el gobierno.
- *Internet y correos electrónicos:* Monreal (2017) lo menciona al definirlo como programas rastreadores, cuyo objetivo es encontrar información considerada peligrosa en los paquetes de datos (citado de Mariano Zafra).
- *Centro de recopilación y procesamiento:* Posted on Wed (2016) lo describe como: "las capacidades del sistema para recoger los valores atípicos, detectar la existencia de fraudes en las transacciones o llevar a cabo controles de seguridad".

Estos satélites fueron creados como estrategia militar, el primero en lanzar fue Rusia según la BBC (2017) "con el fin de obtener información de las capas altas en la atmósfera y el campo electromagnético de nuestro planeta y mayor información". Al tener todas estas herramientas garantiza mayor vigilancia y control en el gobierno.

De los anteriores planteamientos se deduce que se contradice la idea que muchos de los ciudadanos tienen sobre su autonomía en la búsqueda de información y emisión de opiniones; se ha demostrado que el gobierno lo hace de una forma muy "sutil" para que sus ciudadanos sigan compartiendo a diario su vida privada. En muchos países las medidas de control y vigilancia son más notorias y drásticas, en donde las consecuencias pueden ser carcelarias e incluso la pena de muerte aplicada a aquellas personas que no permiten que su información sea vista por el gobierno. Naciones como China, Corea del Norte, Irán, Rusia y Cuba, como las más reconocidas, tienen restringida la búsqueda de información y prohibido el uso de redes sociales que no estén autorizadas por el Estado.

Países con más restricción en el ciberespacio

China: todas las VPN (red privada virtual) de este país tienen que ser aprobadas y controladas por el gobierno y se debe cumplir con una regulación gubernamental para no poner en riesgo la seguridad del país. Son numerosas las políticas que tanto los ciudadanos como los visitantes o turistas deben que acatar al utilizar internet.

La conexión que tienen los ciudadanos chinos con el ciberespacio consiste en aplicaciones locales que son manejadas por funcionarios del gobierno del presidente Xi Jinping. Las páginas como Facebook, Google, Twitter se encuentran totalmente bloqueadas y, desde el año 1996, la organización Global Voices impuso al país una norma que implica que cada contenido cibernético que sea "sensible" para sus ciudadanos tiene que ser bloqueado. En palabras del presidente Xi Jinping:

> Sin seguridad en la red no hay seguridad nacional, no hay estabilidad económica y social, y es difícil garantizar los intereses de las masas en general. (...) No podemos permitir que internet se convierta en una plataforma para diseminar información dañina y provocar problemas con los rumores. (Marín, 2019)

Cuba: en 2018 se aprobó el Decreto 370, que compila un articulado que claramente viola los derechos humanos a la privacidad y expone la información de los usuarios en el ciberespacio. Este decreto consiste en que el gobierno tiene el control sobre todo lo que esté alojado o vaya a pasar por la internet y, como medidas de control, contempla sanciones y restricciones a equipos o a las personas que tengan la intención o que publiquen contenido que fomente la dispersión de ideologías. El gobierno dispuso todas estas medidas, de acuerdo con Pentón y Sánchez (2019), "para elevar la soberanía tecnológica en beneficio de la sociedad, la economía, la seguridad y defensa nacional".

Corea del Norte: se destaca por tener la mejor tecnología avanzada, ya sea en redes, plataformas o aparatos tecnológicos, pero esta ventaja es un arma de doble filo para la sociedad, pues la creación de teléfonos inteligentes, televisores y radios implica su configuración con los estándares gubernamentales, con el objetivo que los norcoreanos no puedan acceder a los contenidos de otros países u otros usuarios. Este aspecto se encuentra tan controlado por el gobierno, que lo único que pueden ver son las emisiones de su presidente Kim II-Sung o contenidos creados por sus ciudadanos con la vigilancia del gobierno. Ghosh y Insider (2020) aseguran que: "Escuchar radio o ver televisión extranjera es ilegal y el gobierno realiza regularmente redadas para asegurarse de que la gente no consuma nada subversivo pues podría pagar con pena de muerte".

Rusia: este país no es tan estricto como los anteriormente mencionados pero sí tiene, como proyecto para el año 2022, crear su propia red de internet, con el fin de desconectar a sus ciudadanos de una amenaza externa a futuro; sin embargo, las autoridades no tienen la intención de violar la libertad de búsqueda:

> "Todos están a favor de la libertad en internet, los autores de la ley, la administración presidencial, el gobierno, nadie es partidario de restringirla y limitar las posibilidades de trabajo en la red global", dijo a la prensa el portavoz de la presidencia rusa, Dmitri Peskov". (El Espectador, 2019)

La única regulación y control que tiene esta nación consiste en que todos sus ciudadanos están obligados, por ley, a que permitir que el gobierno guarde toda su información en la base de batos del país.

Irán: lo comentado sobre este país se puede ampliar con ejemplos como que, en el 2019, dejó a 80 millones de personas sin internet, con un apagón que duró 65 horas sin acceso a telecomunicaciones e internet, después de lo cual censuró algunas páginas pues, según la BBC (2019), su objetivo principal consistía en "prevenir el acceso e intercambio de información sobre las protestas que estallaron al país por un drástico aumento en los precios del combustible" .

Estos son unos de los países en donde los gobiernos tienen el control parcial o total y vigilancia estrecha sobre sus ciudadanos; en algunos estás determinaciones están constituidas por ley y en otros, como Irán y Rusia, poco a poco se está tomando el dominio del ciberespacio.

Conclusiones

El control del ciberespacio debería ser ejercido por un ente mixto, es decir, conformado por el gobierno y la sociedad, en donde se preserve la equidad y no se violen los derechos a la privacidad, y la libertad en los medios virtuales y alternativos, esto con el fin de favorecer el apoyo en un país que escucha los ideales, sin permitir su manipulación por parte del sector empresarial para beneficios políticos, económicos y sociales. Es evidente entonces que, para lograr esto, es necesario pedirle a los dueños de la red y de las plataformas que sean transparentes en los acuerdos para acceder a su información.

Por otra parte, es indispensable educar a la ciudadanía y generar en una cultura en la red, que genere conciencia sobre no poner toda su base de información en manos de plataformas en las que no existe claridad sobre el objetivo de obtener todo estos datos; una ciudadanía más informada y más reservada contribuye a no crear y difundir *fake news*, a propiciar el robo cibernético, a difundir pornografía, y a la divulgación no autorizada y manipulación de información. Tener mayor responsabilidad garantiza que el gobierno no requiera ejercer mayor control que el necesario en las formas individuales de

expresión y, para esto, se deben tener encuentras aspectos claves de seguridad en el ciberespacio como:

1) Leer las políticas y condiciones de los servidores.
2) Ser responsables con la divulgación de la información personal.
3) No creer y confiar en todo lo que está publicado, ser menos abiertos a todo tipo de información.

Referencias

1. Caro, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de estrategia*, 149, 47-82. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/3837251.pdf.
2. Écija, A. (04 de abril, 2014). El Ciberespacio: una herramienta de poder. *Legal today*. Recuperado de: http://www.legaltoday.com/gestion-del-despacho/nuevas-tecnologias/articulos/el-ciberespacio-una-herramienta-de-poder.
3. Duarte, M. (23 de enero, 2018). Regular el Ciberespacio. *América Latina em movimiento*. Recuperado de: https://www.alainet.org/es/articulo/190548.
4. Ministerio de Tecnologías de la Información y Comunicaciones (04 de septiembre, 2018). Su información personal podría estar en venta. *En TIC confío*. recuperado de: https://www.enticconfio.gov.co/Su-informacion-personal-podria-estar-en-venta.
5. RT (13 de agosto, 2013). Echelon: El gigante de espionaje de EE.UU. que no estaba dormido. *RT en español*. Recuperado de: https://actualidad.rt.com/actualidad/view/102742-echelon-eeuu-espionaje-nsa-guerra-fria.
6. De Monreal, F. (2017, 11 de diciembre). [Red Espía] Esquema Echelon. *Issuu*. Recuperado de: https://issuu.com/cnicnicnicnicnicnicni/docs/esquema_de_la_red_echelon.
7. Power Data (6 de abril, 2017). Los 3 principales tipos de técnicas de procesamiento y análisis de datos. *Power data*. Recuperado de: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/los-3-principales-tipos-de-tecnicas-de-procesamiento-y-analisis-de-datos.
8. Fundación Universidad Pablo de Olavide (10 de marzo, 2017). *"Los estados usan el ciberespacio para proyectar el poder y apoyar las acciones militares", según Guillen Colom*. Universidad Pablo de Olavide - Sevilla. Recuperado de: https://www.upo.es/fundaciones/los-estados-usan-el-ciberespacio-para-proyectar-el-poder-y-apoyar-las-acciones-militares-segun-guillen-colom/.
9. BBC (04 de octubre, 2017). Sputnik, el primer satélite que hizo despegar la carrera espacial entre la URSS y Estados Unidos hace 60 años. *BBC*. Recuperado de: https://www.bbc.com/mundo/media-41503825.
10. Marín, N. (24 de marzo, 2019). ¿Vigilan los gobiernos lo que haces en la red? *El Espectador*. Recuperado de: https://www.elespectador.com/noticias/el-mundo/vigilan-los-gobiernos-lo-que-haces-en-la-red-articulo-846675.
11. Pisanu, G. (21 de noviembre, 2019). Control de internet en su máxima expresión: Decreto 370 de Cuba. *accessnow*. Recuperado de: https://www.accessnow.org/control-de-internet-en-su-maxima-expresion-decreto-370-de-cuba/.
12. Pentón, M. (05 de julio, 2019). Cuba impone nuevas medidas para controlar lo que se publica en internet y las redes sociales. *El mundo heraldo*. Recuperado de: https://www.elnuevoherald.com/noticias/mundo/america-latina/cuba-es/article232324607.html.
13. Ghosh, S. (06 de enero, 2020). 10 maneras en las que Corea del Norte utiliza la tecnología para mantener a sus ciudadanos en la oscuridad respecto al mundo exterior. *Business Insider*. Recuperado de: https://www.businessinsider.es/controla-corea-norte-acceso-internet-ciudadanos-554373.
14. BBC (09 de noviembre, 2019). Irán: cómo un gobierno dejó sin internet a un país de 80 millones de personas en medio de protestas y denuncias muertes de decenas de manifestantes. *BBC*. Recuperado de: https://www.bbc.com/mundo/noticias-internacional-50489085.
15. Rosenberg, M.; Confessore, N. y Cadwalladr, C. (20 de marzo, 2018). La empresa que explotó millones de datos de usuarios de Facebook. *The New York Times*. Recuperado de: https://www.nytimes.com/es/2018/03/20/espanol/cambridge-analytica-facebook.html.
16. Véliz, C. (04 de abril, 2018). Por qué es importante proteger nuestra privacidad en internet. *The New York Times*. Recuperado de: https://www.nytimes.com/es/2018/04/04/espanol/opinion/opinion-veliz-facebook-privadidad-cambridge-analytica.html.