Revista Ensayos Militares
vol. 1 - nº 2 - 2015, pp. 85-98

ISSN 0719-6334 / versión impresa
ISSN 0719-6989 / versión en línea

La libertad en el ciberespacio: ciberseguridad y el principio del daño

Liberty in Cyberspace: Cybersecurity and the Harm Principle

Sebastián Koch Merino*
Centro de Estudios Estratégicos
Academia de Guerra del Ejército de Chile

Resumen: Sobre la base de distintas concepciones teóricas de libertad a sus límites en el ciberespacio, a la ciberseguridad y al principio del daño, se buscará analizar hasta qué punto y en qué circunstancias le es válido al Estado entrometerse en los espacios de libertad de los que los individuos gozan en el ciberespacio. Asimismo, se evaluarán los requisitos para que dicha intromisión sea fundada y legítima y se analizarán aquellas situaciones en las que el Estado debe respetar de manera irrestricta la libertad y la privacidad de los individuos en el ciberespacio.

Palabras claves: Ciberseguridad – Libertad – Ciberespacio – Principio del Daño – Ciberinteligencia

Abstract: Based on different theoretical conceptions of liberty, its limits in cyberspace, on cybersecurity and on the Harm Principle, this article seeks to analyse up to which point and in what circumstances a State is able to validly enter an individual's space of liberty in cyberspace. Thus, the conditions for a legitimate and founded intromission will be evaluated and the situations in which a State must unrestrictedly respect the liberty that individuals enjoy in cyberspace will be analysed.

Key words: Cybersecurity – Liberty – Cyberspace – Harm Principle – Cyberintelligence

Fecha de recepción: 31 de agosto de 2015
Fecha de aceptación y versión final: 16 de octubre de 2015

* Sebastián Koch Merino es Cientista Político de la Universidad Diego Portales, Licenciado en Estudios Europeos de la Universidad de Concepción y en Seguridad Humana de la Universidad de Łódź, Polonia. Actualmente se desempeña como Investigador y Analista del Centro de Estudios Estratégicos de la Academia de Guerra (CEEAG). Email: sebastian.koch@acague.cl

Introducción

"Lo cíber" hace alusión a elementos pertenecientes al ciberespacio o bien empleados por medio de este.[1] En el plano de la Seguridad y Defensa, es la manera en que estas se conducen en el ciberespacio. Esta investigación analizará la libertad de la que gozan las personas en el ciberespacio y el efecto del accionar estatal respecto de esta.

La obtención de información de importancia política, estratégica y operacional acerca de los aliados/adversarios es una actividad que los Estados llevan a cabo hace bastante tiempo con las operaciones de inteligencia. Con el nacimiento y proliferación de Internet, la función de inteligencia debió adaptarse a esta nueva dimensión.

Gran parte del ciberespacio está ocupado por personas naturales, sea a modo de pasatiempos/ocio, o bien en cuanto a herramienta para desarrollar sus funciones tanto cotidianas como laborales. El Estado, para garantizar su ciberseguridad, lleva a cabo un proceso de recopilación de información y de confección de informes a base de los insumos que obtiene del ciberespacio, muchos originados en los espacios de libertad y de privacidad de las personas. Aquí yace el problema: es esencial determinar qué elementos presentes en el ciberespacio son privados/públicos y qué elementos son cerrados/abiertos. De no hacerse correctamente esta diferenciación es posible que injustificadamente se den limitaciones a la libertad e intromisiones en la privacidad de las personas en el ciberespacio.

Los casos Wikileaks y Snowden revivieron una antigua problemática: la pugna entre libertad y seguridad, lo que en el ciberespacio se traduce en libertad vs. ciberseguridad; el denominado ciberdilema.[2] Basado en esto se plantea la siguiente pregunta: ¿hasta qué punto las operaciones de ciberinteligencia no interfieren infundadamente con la libertad? Así, se busca comprender en qué situaciones es posible que de manera válida se intervenga en la libertad y en la privacidad de los individuos en el ciberespacio.

En primer lugar, debe tenerse claro el concepto de ciberseguridad. A continuación deben delimitarse las operaciones de ciberinteligencia. Además, es necesario poner atención al tipo de acto que se está realizando en el ciberespacio y al tipo de información al que se accede. Asimismo, es necesario indagar en torno a algunas concepciones de libertad y a la validez de su limitación. La apreciación conjunta de

1 Emilio Sánchez de Rojas, "¿Ciber…qué? La ciberseguridad", *Ejército*, vol. 837 (2010), p.138.

2 José María Molina, "Cyberdilemma", Instituto Español de Estudios Estratégicos nº 115 (noviembre 2013), p. 1 (en línea) [Fecha de consulta 10.06.2015] http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO115-2013_Cyberdilemma_JM.MolinaMateos.pdf

estos elementos permitirá analizar la limitación de la libertad de los individuos en el ciberespacio por parte de un Estado que busca garantizar su ciberseguridad.

Ciberespacio, ciberseguridad y ciberinteligencia

El ciberespacio se ha vuelto parte integral de las distintas actividades individuales, empresariales y estatales. Hoy la gran mayoría de estas —incluso las funciones de Seguridad y Defensa— tienen un marcado componente digital, desarrollándose por medio de las tecnologías de la información y del ciberespacio. Esta nueva dimensión supone además una ampliación de las alternativas de participación y de oportunidades –lo que ha incidido en la expansión en su uso– tanto para el Estado como para las empresas y para la sociedad civil, pero a su vez crea oportunidades de acción estratégica para eventuales adversarios estatales y no estatales.[3]

La ciberseguridad ha sido catalogada de amorfa.[4] Su significado está en un área gris, con poco acuerdo a nivel doctrinario. Ha sido definida como la sumatoria de planes de contingencia individuales, poco relacionados con riesgos sistémicos, con soluciones aisladas —*adhoc*— y no relacionadas con las capacidades o con la cooperación.[5] Pese a ello se entiende que es la situación de ausencia de amenazas realizadas por medio de, o dirigidas a, las tecnologías de la comunicación y de la información y a sus redes.[6] Cuando las amenazas en el ciberespacio toman la forma de ciberterrorismo o de ciberguerra, constituyen amenazas a la seguridad nacional.[7] Lo mismo sucede si estas suponen un peligro para la infraestructura crítica. Por tanto, los Estados buscan evitar el surgimiento de dichas amenazas o bien ponerles término para así garantizar su ciberseguridad.

Una primera alternativa para hacer frente a dichas amenazas podría ser el control del ciberespacio por parte del Estado, monitoreando de manera preventiva las actividades que ahí se llevan a cabo, limitando el margen de acción del individuo, pasando a llevar su libertad. Dicha opción ha sido sumamente controvertida y rechazada, al igual que cualquier intento de regulación *ex ante* del ciberespacio.[8]

---

3 David Betz & Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, London: International Institute for Strategic Studies, 2011, p. 10.

4 Alexander W. Vacca, "Military Culture and Cyber Security", *Survival*, vol. 53, nº 6 (2012), p. 159.

5 Eneken Tikk, "Ten Rules for Cyber Security", *Survival*, vol. 53, nº 3 (2011), p. 119.

6 Sánchez de Rojas, op. cit., p. 138.

7 Ibidem, p. 140.

8 Eguskiñe Lejarza, "Ciberguerra, los escenarios de confrontación", Instituto Español de Estudios Estratégicos n.º 14 (febrero 2014), p. 2 (en línea) [Fecha de consulta 10 de junio de 2015] http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

Los ciberataques provienen de enemigos de difícil dilucidación, ocultos tras la denominada niebla de la red[9], dificultando el accionar estatal. Los Estados están en una posición incómoda, ante un escenario complejo y difícil de afrontar, por las características de los atacantes, de las amenazas y por la imposibilidad de interferir en el ciberespacio con el consentimiento ciudadano. Y ante su incapacidad de controlar esta dimensión recurre a otras medidas.

La información estratégica es esencial para comprender los propósitos y el accionar de un adversario.[10] La recopilación de esta depende de la función de inteligencia, la que busca conocer al enemigo, sus capacidades y sus medios, así como las propias capacidades y propios medios, evaluando las posibilidades reales de uso.[11] Así, el Estado tiene de manera anticipada la información necesaria para asegurar su desarrollo y para tener la capacidad de pronosticar tendencias.[12] Conocer correctamente al adversario, las amenazas, sus eventuales consecuencias y las posibles soluciones son algunos de los elementos que puede proporcionar la inteligencia. Al ser desarrollada en el ciberespacio, se habla de ciberinteligencia.

La ya mencionada niebla de la red añade un factor extra de incertidumbre, cuyo sorteo depende de la información disponible en él. Esta información proviene de diversas fuentes que pueden ser cerradas o abiertas, distinción de suma importancia.

Debido al grado de presencia del individuo en el ciberespacio, la información relativa a estos es igualmente cuantiosa. Las redes sociales —Facebook, Twitter y otras— se caracterizan por almacenar contenido personal de los usuarios. La configuración de privacidad del usuario y el medio empleado dentro de la red social o medio digital influye en la catalogación de una fuente como abierta o cerrada: por ejemplo, un Tweet abierto es distinto de un mensaje privado vía Facebook. Un correo electrónico necesariamente es una fuente cerrada, al igual que la correspondencia tradicional.

El tipo de fuente al que se acceda en el marco de las operaciones de ciberinteligencia resulta de primordial importancia para determinar si se está mermando o no la libertad de las personas en el ciberespacio, así como para evaluar la factibilidad del accionar estatal. De la misma manera, es esencial determinar si la actividad que se busca detener supone un daño en potencia, además de evaluar si constituye

9 Ibidem, p. 1.

10 José Frías, *Nuestra guerra y nuestra paz (una estrategia para la paz)*, España: Servicio de Publicaciones del EME, 1984, p. 42.

11 Ibidem, p. 262.

12 Guillermo Holzmann, "La función del sistema nacional de inteligencia en un Estado democrático", *Política*, vol. 35 (1997), pp. 100 y 106.

o no una amenaza a la seguridad nacional. Sobre la base de estas consideraciones y a las distintas concepciones de libertad, se buscará determinar hasta qué punto el Estado puede operar en el ciberespacio sin incurrir en limitaciones infundadas a la libertad, además de evaluar en qué casos —extraordinarios— es justificada una limitación a la libertad de las personas en el ciberespacio por parte del Estado.

Libertad

Según lo que se tenga por libertad, variará la tolerancia respecto del accionar estatal en el ciberespacio, así como las causas que lo motivan.

La libertad es un concepto que ha sido sistemáticamente estudiado en la Teoría Política. Además de ser parte del trinomio que se hizo famoso durante la Revolución Francesa —libertad, igualdad, fraternidad—, esta se ha convertido en un principio regidor de la política y en un valor orientador de preferencias políticas.[13]

La libertad ha sido concebida de distintas maneras. Para algunos tiene tres concepciones fundamentales: como autodeterminación, como la necesidad de que dicha autodeterminación sea garantizada y como posibilidad de elección.[14] Otros reconocen la vasta pluralidad de significados del concepto, así como los distintos campos en los que se aplica.[15]

En el siglo XIX, Benjamin Constant distinguió lo que los antiguos tenían por libertad de lo que los modernos tenían por libertad. Para los antiguos, era la libertad para accionar e influir en la esfera pública de su Estado de manera directa, tomando participación de los asuntos políticos y reconociendo una completa sumisión del individuo para con su Estado. La colectividad era autoridad y su voluntad primaba por sobre la voluntad individual, siendo soberanos en las cuestiones públicas y esclavos en los asuntos privados. Sin tener noción alguna de los derechos individuales, el individuo estaba perdido en la colectividad[16], pero siempre manteniendo su influencia directa en los asuntos públicos. Los modernos, siendo representados en los asuntos públicos, ejercían su soberanía de manera indirecta. Su libertad se vinculaba con el libre albedrío en los asuntos

13 Antonio María Baggio et al., "Seminario "Libertad, Igualdad, ¿Fraternidad?", *Revista de Ciencia Política*, nº 27, vol. 1 (2007), p. 134.

14 Nicola Abbagnano, *Diccionario de filosofía*, México: FCE, 1987, p. 738.

15 José Ferrater Mora, *Diccionario de filosofía,* Madrid: Alianza Editorial, 1980, p. 1968.

16 Óscar Godoy, "Selección de textos políticos de Benjamin Constant", *Estudios Públicos*, vol. 59, invierno (1995), pp. 53-54.

privados, abogando por una menor intervención estatal. De esta manera los modernos, libres en el ámbito privado, tenían una soberanía restringida en lo público, al incidir indirectamente en la vida política del Estado[17]; perdidos en la multitud, privilegiando los asuntos privados por sobre la participación directa en los asuntos públicos, no eran capaces de percibir la influencia que podrían haber ejercido en estos.[18] Los antiguos entendían la libertad como la correcta distribución del poder, mientras que los modernos la entendían como las garantías estatales para la esfera privada[19]; ideales de libertad incompatibles entre sí.[20]

John Stuart Mill establece que la libertad es la limitación del poder que el gobernante puede ejercer sobre la comunidad que gobierna, sea por garantías inherentes a la persona humana, anteriores al Estado —derechos o libertades civiles— o bien mediante *checks* o controles constitucionales; los intereses de la ciudadanía debían ser tenidos en cuenta para la toma de decisiones en los asuntos más importantes.[21] Para él, la libertad dependía de que la autoridad del gobernante no fuese ejercida de manera arbitraria, sino que respetando elementos superiores a los deseos del gobernante: el ordenamiento jurídico y los derechos anteriores al Estado.

Isaiah Berlin se refiere a dos ideas de libertad: libertad negativa y libertad positiva.[22] La libertad negativa está relacionada con la inexistencia de constreñimientos sobre la persona, permitiendo que sea/haga aquello de lo que es capaz, sin la interferencia de terceros. Se relaciona con "estar libre de algo".[23] La libertad positiva se relaciona con "ser libre para algo". Esta concepción apunta a que las personas son dueñas de sí mismas y son capaces de idear planes y objetivos y de concebir sus propios medios para su eventual realización.[24] La libertad negativa es la ausencia de limitantes a la libertad, mientras que la libertad positiva es la libertad de acción de la que gozan los individuos.

En relación con esto, Pettit establece que la libertad negativa propuesta por Berlin se basa en la ausencia de interferencia; se es libre negativamente hasta que se interfiera en alguna de las actividades deseadas.[25] Por su parte, la libertad

17 Ibidem, pp. 52-54.
18 Ibidem, p. 58.
19 Ibidem, Loc. Cit.
20 Bobbio, Norberto, *Liberalismo y democracia*, México: Fondo de Cultura Económica, 1989, p. 8.
21 John Stuart Mill, *On Liberty,* New York: Bantam Classics, 2008, p. 4.
22 Isaiah Berlin, *Libertad y necesidad en la historia*, Madrid: Ediciones de la Revista de Occidente, 1974, p. 136.
23 Ibidem, p. 145.
24 Ibidem, pp. 145-146.
25 Philip Pettit, *Republicanismo. Una teoría sobre la libertad y el gobierno*, Barcelona: Editorial Paidós, 1999, p. 35.

positiva supone el autodominio del hombre.[26] Considera que esta distinción ha generado la ilusión en la Teoría Política de que únicamente existen dos tipos de libertad.[27] Establece que la distinción hecha por Berlin no cubre todo el espectro en cuanto a concepciones de libertad, ya que autodominio y ausencia de interferencia no son sinónimos. Debido a que los tipos de libertad propuestos por Berlin dejan un área gris entre sí, Pettit propone un tercer tipo de libertad situado entre estos.[28] Ahí sitúa la libertad como no dominación, que tiene elementos en común con la libertad negativa —foco en la ausencia de algo— y con la libertad positiva —foco en la autodominación—. Para ser libre desde la no dominación es necesaria la inexistencia de una relación de amo-esclavo o amo-siervo; nadie debe ser capaz de interferir de forma arbitraria e impune en lo que un individuo busca llevar a cabo.[29] Establece que la dominación es distinta de la interferencia: puede haber dominación sin interferencia e interferencia sin dominación; puedo estar sometido a la dominación de alguien, pero eso no implica que él vaya a hacer uso de esas facultades e intervenga en mis elecciones, así como puedo no estar sometido a dominación alguna, pero sufrir interferencias injustificadas e infundadas.[30]

Hayek entiende la libertad como el estado que se produce por la reducción a su más mínima expresión de la coacción que pueden ejercer ciertas personas/grupos[31]; mientras menor sea la coacción que distintos actores puedan ejercer sobre mí, más libre seré. No se cierra únicamente a la presión de un Estado sobre los individuos, sino que reconoce además otras fuentes de coacción distintas del Estado. A mayor limitación de las formas de coacción, más libre se vuelve el objeto de dicha coacción.

Lo que se tenga por libertad es esencial para determinar si el accionar estatal en el ciberespacio constituye o no una violación a la libertad de las personas. Asimismo, permitirá evaluar las situaciones en que el Estado puede afectar legítimamente la libertad y la privacidad de las personas. A eso se agrega el origen y el tipo de información manejada y de la severidad de la amenaza.

26 Ibidem, Loc. Cit.
27 Ibidem, p. 37.
28 Ibidem, p. 40.
29 Ibidem, p. 41.
30 Ibidem, pp. 41-42.
31 Friedrich Hayek, *Los fundamentos de la libertad*, Buenos Aires: Centro de Estudios sobre la Libertad, 1982, pp. 32-38.

Libertad en el ciberespacio

El ciberespacio tiene por característica una "realidad dual" en cuanto lo público y lo privado. A diferencia de la realidad física, en el ciberespacio es difícil distinguir entre lo abierto y lo cerrado y privado y lo público; están separados por una fina membrana. Esto se debe en parte a la coexistencia de distintos tipos de actores, pero principalmente a la dualidad público/privada de sus componentes, en especial la información ahí almacenada.

Las distintas herramientas disponibles en el ciberespacio se caracterizan por una dualidad público/privada: la membrana es tan fina que es posible pasar de un ámbito a otro en un *click*. Retomando el ejemplo de las redes sociales, Twitter permite emitir comentarios públicos, abiertos a todos, pero a su vez permite enviar mensajes privados entre dos o más usuarios. Algo similar sucede con Facebook. Es sumamente fácil para los usuarios el generar, almacenar y administrar información tanto pública como privada incluso empleando una misma herramienta —que tiene barreras de entrada prácticamente inexistentes—. Este fenómeno no se agota en las redes sociales, en las que la privacidad/publicidad de la información dependerá mayoritariamente de la configuración de privacidad que haga el usuario. La información disponible en el ciberespacio puede encontrarse abierta o cerrada y protegida por medio de encriptación según un código determinado. Existen otras porciones de información que se encuentran protegidas mediante un acceso restringido según usuarios y sus claves de seguridad correspondientes, requiriendo un inicio de sesión previo —el sistema bancario, por ejemplo—. Los últimos dos casos corresponden a fuentes de información privada y cerrada, ya que para acceder a dicha información se necesitan ciertos pasos que van más allá de la mera navegación. En cambio, la información de libre acceso —fuentes abiertas y públicas— no requiere de mayor esfuerzo. Existen sectores del ciberespacio en que la delimitación entre el espacio de información cerrada y privada vs. el espacio de información abierta y pública es sumamente clara —por ejemplo, el sistema bancario, en el que existen numerosas barreras de acceso, protegiendo así las cuentas—, pero también existen ciertas áreas en las que esta línea es, cuando menos, difusa.

Las barreras de acceso mencionadas han sido superadas en incontables ocasiones. Individuos, organizaciones e incluso Estados, haciendo un uso irrestricto e indebido de su libertad, realizan intromisiones en los espacios de libertad y de privacidad de otros. El robo de información con *software* malicioso —*malware*— es una de las formas de atravesar esta barrera. Una vez que el ladrón de información obtiene los datos requeridos para el inicio de sesión en algún portal de acceso restringido, es posible para este llegar a sectores protegidos, cerrada y privada.

Los individuos no son las únicas víctimas de este tipo de prácticas; los sistemas de información de empresas e incluso de organismos estatales, entre otros, han sufrido el robo de información altamente importante desde sus sectores y redes de información protegidas. Estas prácticas, al requerir procedimientos que van mucho más allá de la navegación de buena fe, constituyen violaciones a la libertad y a la privacidad de las personas, sea quien sea el intruso. Estos terceros, que se inmiscuyen en los asuntos cerrados y privados de otros, llevan a cabo violaciones a la privacidad y limitaciones a la libertad, aprovechando indebidamente su propia libertad. En respuesta a estas violaciones, al Estado le es posible establecer limitaciones y/o consideraciones para evitarlas, apuntando así a la defensa de la privacidad y de la libertad de las personas en el ciberespacio, así como buscando garantizar su ciberseguridad.

Para analizar la relación del accionar estatal en el ciberespacio con la libertad de las personas se utilizará el Principio del Daño de John Stuart Mill. Él analizó la naturaleza y los límites del poder que puede ser legítimamente ejercido sobre los individuos.[32] Ante la posibilidad de abusos de poder y prácticas tiránicas por parte de los gobernantes, se refirió a las situaciones en las que es válido establecer limitaciones a la libertad de las personas, lo que se tradujo en el Principio del Daño. Este principio teórico podría inspirar las normativas legales de un Estado en torno a la limitación del accionar de los individuos en el ciberespacio, bajo ciertos supuestos. Según el Principio del Daño, el único argumento válido para limitar la libertad de uno o más individuos en una sociedad es el evitar un daño a sus miembros.[33] Desde el minuto en que cualquier actividad de uno o más miembros de una sociedad suponga un eventual daño a sí mismos, a los demás o al Estado, esa conducta puede ser prohibida, limitando de manera legítima la libertad de quien desease llevarla a cabo. Se pone el bien de la colectividad por sobre las preferencias, gustos, deseos e intereses individuales[34], privilegiando el bienestar derivado de la inexistencia de actos dañinos en una sociedad determinada. La libertad, según este principio teórico, puede y debe ser limitada, pero únicamente en circunstancias extraordinarias y cumpliendo a cabalidad los supuestos ya mencionados.

Esta lógica es aplicable tanto para el margen de acción individual como para el de los demás actores —incluyendo al Estado— en el ciberespacio. Los espacios de libertad de los que gozan los actores del ciberespacio pueden ser ocupados según

32 Mill, op cit., p. 3.
33 Ibidem, pp. 13-14.
34 Ibidem, p. 14.

su libre albedrío, siempre y cuando sus acciones no supongan un daño para sí mismos ni para el resto de la sociedad, ni una violación a los espacios de libertad y a la privacidad de los demás actores. Al realizar actos en desmedro de la libertad de los demás o persiguiendo fines contrarios a esta[35], como inmiscuirse en la información privada de otros individuos, de empresas o del Estado, se están llevando a cabo acciones que dañan a los actores invadidos. Si se invoca el Principio del Daño, el Estado podría encontrarse habilitado para imponer de manera legítima, límites a la libertad de acción de quienes realicen estas acciones dañinas. Esta posibilidad teórica de limitar la libertad de los actores puede traducirse en la generación de mecanismos legales que penalicen estos actos. Esta es la lógica que sigue el Estado en lo que respecta a la lucha contra la ciberdelincuencia y los ciberdelitos. Al enfrentarse a conductas que dañan a los miembros de una sociedad —por ejemplo, el robo de información— tanto en el plano individual, en el colectivo, en el organizacional e incluso en el estatal, el Estado reacciona mediante su institucionalidad punitiva para sancionarlos y para prevenir el surgimiento de futuros actos delictuales en este ámbito.

En el marco de las operaciones de ciberinteligencia, el Estado busca la prevención de las situaciones descritas, operando *ex ante*. Es necesario para el Estado discernir entre aquellos actos que eventualmente podrían significar un daño para la sociedad y aquellos que no. Ello debe ser llevado a cabo con una responsable utilización de la función de ciberinteligencia, siempre respetando los márgenes impuestos por la libertad y la privacidad y adecuándose al marco jurídico imperante. Tanto la recopilación como la confección de informes son hechas con la intención de prepararse para un daño del que eventualmente se podría ser objeto. Con ello se busca inicialmente evitar ser víctima de ese daño y, de ser inevitable, se busca estar en un mejor pie para resistir sus embates y para reaccionar por medio de las distintas herramientas estatales. El problema en el marco de las operaciones de ciberinteligencia radica en torno al tipo de información a la que se accede. Muchas veces esta información es privada y se encuentra ubicada en el espacio de libertad del que las personas gozan en el ciberespacio, siendo por lo mismo cerrada en su acceso. Una intromisión injustificada por parte del Estado en dicha información constituye evidentemente una violación a la libertad y a la privacidad de las personas y es por lo mismo reprochable. Es más, en dichas situaciones el Estado incurriría en la contradicción de encontrarse produciendo un daño a los mismos individuos que busca proteger. ¿Qué sucede cuando dicha información está siendo recopilada para evitar un daño a la sociedad o al Estado?

35 Molina, op cit., p. 40.

¿Podría este argumento darle validez y legitimidad a una intromisión estatal en los espacios de privacidad y de libertad de los que gozan los individuos en el ciberespacio?

Si aplicamos el Principio del Daño, las operaciones de ciberinteligencia únicamente podrían acceder a información privada y cerrada cuando su utilización suponga un daño a la sociedad y al Estado. De no ser así, el propio Estado sería el que estaría incurriendo en una conducta que significa un daño para los individuos, en la forma de una violación a su privacidad y a su libertad. Para ser capaz de discriminar respecto de la cualidad de la información en cuestión, el Estado debe realizar un monitoreo previo de esta, evaluando si aplica o no el Principio del Daño. Una especie de sobrevuelo de la información abierta y pública disponible en el ciberespacio que conduzca a conclusiones acerca de la información cerrada y privada —sin inmiscuirse en esta— y de los actores que almacenan y manejan dicha información. De esta manera se busca determinar, con la mínima intromisión posible en los espacios de privacidad de las personas, si dicha información podría presentar o no un eventual daño a la sociedad, a los individuos que la componen o al Estado. En caso que la línea que delimita los márgenes del sobrevuelo quede mal establecida, el Estado podría accidentalmente —o adrede— entrometerse en aquellas áreas que debieran únicamente ser revisadas en caso de aplicarse el Principio del Daño. Si el Estado se inmiscuye anticipadamente en esos espacios de privacidad y de libertad, está asumiendo de manera infundada que la utilización de dicha información es potencialmente dañina; el mismo Estado, con esta violación de la privacidad y la libertad de los individuos, estaría causando un daño. En situaciones extraordinarias en que la evaluación previa entregue resultados que demuestren de manera fundada que la información en cuestión podría significar un daño, el Estado estaría habilitado para acceder a esta, entrometiéndose en los espacios de libertad y de privacidad, dentro del marco de una investigación en curso y respetando irrestrictamente el ordenamiento jurídico.

El marco legal recién mencionado, generado a partir del análisis y la reacción estatal en virtud del Principio del Daño, debiera referirse expresamente a aquellas áreas del ciberespacio en las que el Estado no puede interferir, sectores que regidos por la libertad individual no pueden ser permeados. La única causa que podría extraordinariamente justificar intervenir en dichos espacios de libertad es, como ya se dijo, una certeza por parte del Estado acerca de que la información ahí manejada supone un daño en potencia. Esta certeza debe generarse a partir del ya mencionado sondeo superficial, que corresponde a una evaluación de aquellos espacios de libre acceso, que contienen información pública y abierta, sin entrar en aquellos espacios en que reina la información privada/cerrada de las personas. Una vez hecho este sondeo y generada esta certeza, es posible para el Estado recurrir

—a modo de ejemplo— al aparato judicial y requerir permisos para inmiscuirse de manera legítima en la información privada y personal de los individuos. De no ser así, se están llevando a cabo enormes violaciones a la libertad y a la privacidad de las personas. Basta con imaginar los escándalos que se generarían si un Estado llevase a cabo escuchas telefónicas arbitrarias y no autorizadas o intercepción e intervención de la correspondencia de alguien. Si estos actos generan rechazo tras su sola mención, ¿por qué no se da igual trato a la privacidad de los individuos en el ciberespacio? ¿Qué diferencia existe entre una conversación telefónica, una carta, un correo electrónico y un mensaje privado en una red social en cuanto al componente de privacidad y de libertad que revisten para los individuos que participan de estos actos comunicacionales? La reacción civil a los casos Wikileaks y Snowden demostró que la tolerancia a este tipo de intromisiones es baja, similar a la que existe en torno a la inviolabilidad de la correspondencia. Los espacios de libertad y privacidad los que gozamos como individuos en el ciberespacio deben ser tratados como tal, con el mismo respeto que se da a los demás medios de comunicación empleados en el ámbito privado de las personas.

En caso que el Estado se inmiscuya sin el respaldo de 1) el Principio del Daño —en lo teórico— y 2) la normativa legal existente que ampare y habilite su intervención en los espacios de privacidad y libertad, estaría incurriendo en conductas que atentan contra la libertad y la privacidad de los individuos y que generan un daño a estos. De ser así, el Estado en cuestión puede quedar expuesto a situaciones similares a los casos Wikileaks y Snowden, casos en que la pugna entre la seguridad del Estado y la libertad fue ganada —en la opinión pública—por la libertad. Ante una ciudadanía con una baja tolerancia a violaciones a su libertad y a su privacidad por parte del Estado, este último debe ser precavido al realizar operaciones de ciberinteligencia, ya que de lo contrario podría generar un descontento y una desconfianza generalizadas a nivel ciudadano.

Conclusiones

El antiguo debate entre libertad y autoridad revive con fuerza en el ciberespacio. Las distintas concepciones de libertad permiten indagar acerca de los elementos que en distintos momentos la compusieron. Este razonamiento, que se extrapola desde el plano físico de libertad individual hacia el espacio de libertad del que las personas gozan en el ciberespacio, apunta mayoritariamente hacia una intervención estatal reducida a su más mínima expresión, al predominio del libre albedrío de las personas y al respeto irrestricto de su libertad y privacidad en esta dimensión.

El rechazo a intentos de regulación y control estatal del ciberespacio manifiesta una postura mayoritaria en la sociedad: el ciberespacio debe estar exento de dominación y de cualquier intervención injustificada por parte del Estado, asegurando así la libertad y la privacidad de los individuos. Mientras dicha libertad sea ejercida como tal, la regulación, monitoreo y vigilancia estatal del ciberespacio debiese estar estrictamente limitada a los sondeos y al monitoreo de la información abierta y pública. Pero en caso que dicha libertad sea ejercida para llevar a cabo acciones potencialmente dañinas, es válido invocar el Principio del Daño y la normativa existente para legítimamente limitar la libertad de quienes realicen dichos actos. El requisito de legitimidad recién mencionado es una condición necesaria para el accionar del Estado en el ciberespacio mediante la ciberinteligencia. Este no puede abusar de dicha función, ni mucho menos realizar incursiones en la información personal y las comunicaciones privadas y cerradas de los individuos en el ciberespacio sin la justificación y la autorización correspondientes. Ambos requisitos son ineludibles.

Así se buscaría la ciberseguridad al mismo tiempo que se estaría respetando la libertad y la privacidad de los actores. Únicamente en aquellos casos extremos y fundados, en que el accionar de ciertos actores sea un daño potencial, resulta válido limitar la libertad de los individuos en el ciberespacio. Salvo estas situaciones extraordinarias, la libertad y la privacidad de los individuos en el ciberespacio debieran ser respetadas irrestrictamente por todos aquellos que conviven en esta dimensión, siendo ambos elementos las piedras angulares que coadyuvaron al desarrollo del ciberespacio y a la proliferación de su uso en los distintos ámbitos de la vida individual, de la sociedad y del Estado.

Bibliografía

Abbagnano, Nicola, *Diccionario de filosofía*, México: FCE, 1987.

Baggio, Antonio María et al., "Seminario "Libertad, Igualdad, ¿Fraternidad?", *Revista de Ciencia Política*, nº 27, vol. 1, 2007, pp. 133-157.

Berlin, Isaiah, *Libertad y necesidad en la historia*, Madrid: Ediciones de la Revista de Occidente, 1974.

Betz, David. & Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, London: International Institute for Strategic Studies, 2011.

Bobbio, Norberto, *Liberalismo y democracia,* México: FCE, 1989.

Clarke, Richard. y Robert Knake, *Guerra en la red: los nuevos campos de batalla*, Barcelona: Editorial Planeta, 2011.

Godoy, Oscar, "Selección de textos políticos de Benjamin Constant", *Estudios Públicos*, vol. 59, invierno, 1995, pp. 51-68.

Ferrater Mora, José, *Diccionario de filosofía,* Madrid: Alianza Editorial, 1980.

Frías, José, *Nuestra guerra y nuestra paz (una estrategia para la paz)*, España: Servicio de Publicaciones del EME, 1984.

Hayek, Friedrich, *Los fundamentos de la libertad*, Buenos Aires: Centro de Estudios sobre la Libertad, 1982.

Holzmann, Guillermo, "La función del sistema nacional de inteligencia en un estado democrático", *Política*, vol. 35, 1997 pp. 97-130.

Lambeth, Benjamin, "Airpower, Spacepower and Cyberpower", en Charles Lutes y Peter Hays (eds), *Toward a Theory of Spacepower, Selected Essays*, Washington: National Defence University Press, 2011, pp. 155-178.

Lejarza, Eguskiñe, "Ciberguerra, los escenarios de confrontación", Instituto Español de Estudios Estratégicos nº 14 (febrero 2014), (en línea) [Fecha de consulta 10 de junio de 2015] http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

Mill, John Stuart, *On Liberty*, New York: Bantam Classics, 2008.

Molina, José María, "Cyberdilemma", Instituto Español de Estudios Estratégicos nº 115 (noviembre 2013), (en línea) [Fecha de consulta 10.06.2015] http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO115-2013_Cyberdilemma_JM.MolinaMateos.pdf

Pettit, Philip, *Republicanismo. Una teoría sobre la libertad y el gobierno*, Barcelona: Editorial Paidós, 1999.

Platt, Washington, *Producción de inteligencia estratégica*, Buenos Aires: Editorial Struhart & Cía, 1983.

Rexton, Paul, "Cómo analizar la guerra en Wi-fi. De ciberguerra a Wikiguerra: la lucha por el ciberespacio", *Military Review*, vol. 69, nº 5, 2014, pp. 30-36.

Sánchez de Rojas, Emilio, "¿Ciber…qué? La ciberseguridad", *Ejército*, vol. 837, 2010, pp. 136-143.

Stewart, John, "El campo de batalla digital futuro: Guerra C2 e Inteligencia – el concepto estadounidense", *Tecnología Militar*, vol. 23, nº 1, 2001, pp. 10-12.

Tikk, Eneken, "Ten Rules for Cyber Security", *Survival*, vol. 53, núm. 3, 2011, pp. 119-132.

Torres, Manuel, "Los dilemas estratégicos de la ciberguerra", *Ejército*, 2011, vol. 839, marzo, pp. 14-19.

Vacca, W. Alexander, "Military Culture and Cyber Security", *Survival*, vol. 53, nº 6, 2012, pp. 159-176.