Capítulo 3

El poder en el ciberespacio*

DOI: https://doi.org/10.25062/9786287602137.03

Steven Jones-Chaljub
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Citación APA: Jones-Chaljub, S. (2022). El poder en el ciberespacio. En Jones-Chaljub, S., *Conceptualización del ciberespacio humano* (pp. 53-78). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602137.03

Conceptualización del ciberespacio humano
ISBN impreso: 978-628-7602-14-4
ISBN digital: 978-628-7602-13-7
DOI: https://doi.org/10.25062/9786287602137

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2022

* Este libro presenta los resultados del proyecto de investigación "Fortalecimiento de las capacidades cibernéticas para Colombia" del grupo de investigación "Masa Crítica" de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por Minciencias y con código de registro COL0123247. Los puntos de vista pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

A lo largo de la historia, las mentes de muchos han sido cautivadas, al punto de la obsesión, por el irresistible deseo de entender, poseer o mantener el "poder". Les ha ocurrido a los puramente teóricos y académicos, así como a diversos personajes, icónicos y comunes, ilustres y nefastos, que se desenvolvieron en las múltiples esferas de la sociedad. Lo interesante es que dicha tendencia se mantiene hoy por hoy.

Todos, y con ello me refiero a la humanidad en general, tenemos cierto conocimiento tácito del poder. Podemos sentirlo, verlo y vivirlo con facilidad, pero cuando llevamos la experiencia al lenguaje y tratamos de profundizar en sus laberintos, nos perdemos en un mar de interrogantes.

En ese esfuerzo por acercarse al "poder" se han manifestado diversos planteamientos, desde numerosas áreas del conocimiento, que han permitido conformar un nutrido marco conceptual. En sociología y en ciencias políticas, Maquiavelo y Hobbes sentaron los cimientos del debate, el cual fue continuado, solo por mencionar a los más representativos, por Webber (como se cita en Wallimann et al., 1977), Dahl (1957), Bachrach y Baratz (1962), Lukes (2005), Gaventa (1980), Clegg y Giddens (como se cita en Sadan, 1997) y Foucault (1982). En el ámbito de seguridad y defensa, se destacan Sun Tzu ([1963], s. f.), Napoleón ([2018], s. f.), Von Clausewitz ([2007], s. f.), Mahan ([2018], s. f.), Douhet ([2013], s. f.), Jomini ([2008], s. f.), y Fuller (como se cita en Strenski, 1998).

A pesar de sus múltiples contribuciones, los trabajos de estos autores tienen un punto de convergencia que, inevitablemente, lleva a cuestionar la pertinencia de emplearlos textualmente para analizar al poder en el contexto del ciberespacio: todos ellos terminaron por reducir el poder a variables y estructuras que pertenecen o manifiestan en el "mundo material" o "real", lo cual choca directamente con el argumento de la flexibilidad teórica, soportado por las características desarrolladas en el segundo capítulo de este libro. Eso no significa que los

trabajos de los estudiosos clásicos quedan descartados, sino que deben emplearse a la luz de las circunstancias; es decir, tomar lo que sea útil y descartar lo que resulte inverosímil para ese entorno intangible.

Este tercer capítulo busca desarrollar la manera como el poder se manifiesta *en* el ciberespacio. El énfasis que se hace en la preposición no es al azar: indica que solo se tendrán en cuenta las interacciones interciberespaciales. La razón es sencilla. En dichas interacciones el ciberespacio funge como un entorno, con las particularidades que lo caracterizan, donde los actores y los sistemas se encuentran, se relacionan y se influencian mutuamente. En las interacciones extraciberespaciales, por el contrario, el entorno intangible se transforma en una simple herramienta más para la proyección de poder en el mundo material, lo que no contribuye al debate.

En el orden de ideas planteado, el capítulo se encuentra dividido en tres secciones. La primera de ellas comprende las premisas básicas teóricas que serán utilizadas para analizar el poder en el ciberespacio. La segunda desarrollará la forma como los actores influencian el comportamiento de otros a partir de un sistema de valores, si se toma en cuenta que el ciberespacio es, en esencia, y a pesar de su inmaterialidad, un entorno social. La última sección analiza la forma como los actores pueden configurar a otros el acceso al ciberespacio, al igual que la información que se encuentra disponible. De esta manera se responden ciertas preguntas fundamentales: quién, cómo, cuándo y dónde se puede o no hacer qué en el ciberespacio.

Las premisas del poder en el ciberespacio

Los estudios tradicionales del "poder" comienzan, por lo general, estableciendo como punto de partida la existencia de uno o varios sujetos, representados por las letras "A" y "B", que tienen la habilidad para interrelacionarse en un contexto particular, por múltiples razones. Dentro de este marco, se afirma que el "poder" se manifiesta cuando "A" consigue que "B" realice o no algo que este último no habría hecho de manera autónoma o voluntaria; es decir, sin la intervención de "A". La misma dinámica se manifiesta con diferentes nombres y condicionamientos: por ejemplo, en Lukes (2005), Gaventa (1980), Clegg y Giddens (como se cita en Sadan, 1997); pero la esencia es igual. Las diferencias entre los autores se desprenden de la naturaleza de los sujetos "A" y "B", la calidad y las consecuencias de su relación, el nivel de conciencia que ambas

partes tengan, las fuentes de donde emana el poder y las maneras como este último es empleado.

A la pregunta sobre cuál debería ser la aproximación teórica correcta para el ciberespacio, en la opinión propia del autor, la respuesta la brindan sus propias particularidades. El ciberespacio es un *entorno intangible creado desde componentes materiales y digitales que se constituyen en requisitos inamovibles para tener acceso; los usuarios pueden interactuar en y desde el ciberespacio solo si pueden ingresar a este*. Ello hace que el contexto donde se desarrollan las relaciones de poder se inclinen más hacia las *interciberespaciales* (usuario-usuario, usuario-sistema y sistema-sistema) que hacia las **extraciberespaciales**. En cualquier caso, debido a la desestatalización, los sujetos "A" y "B" se mueven en las categorías previamente mencionadas: individuos comunes, *insiders*, *script-noobs* o *script-kiddies*, *hackers* profesionales, *hacktivistas*, terroristas, insurgentes, crimen organizado, empresas y Estados.

La razón por la cual este libro acepta la proliferación de actores como premisa para analizar el poder es simple. Se ha demostrado que todos esos actores tienen la habilidad para relacionarse en el ciberespacio, y que al tener algún tipo de interés que los lleva a cooperar o competir entre ellos mismos, incluso por encima de sus diferentes naturalezas, tienen un incentivo para tratar de influenciar al otro. Ahora bien, esto es cierto cuando se tienen o no niveles elevados de conciencia sobre la relación de poder.

Si el poder es la habilidad para lograr que el otro haga o no algo, existe la posibilidad de que ese otro se resista. El éxito del empleo del poder implica que el otro, bajo esta lógica, debe percibir que resistirse es imposible, o que al intentarlo fracase. Cuanto esto último ocurre se habla de conflicto *directo* o *latente*. En ambos casos, los actores, quienes influencian y resisten, tienen un alto nivel de conciencia de la relación de poder; a esto se le denomina *poder directo* (Mager-Hois, 2010).

El poder directo está presente en la mayoría de los autores clásicos especializados en seguridad y defensa. Para dichos autores, a los Estados se les reconoce abiertamente como la principal fuente de inseguridad, lo cual los hace conscientes de su necesidad de proteger sus intereses a través del monopolio y el ejercicio del poder. Esa es una postura normal cuando se plantea el realismo puro como enfoque teórico.

Los actores pueden no ser conscientes de hallarse inmersos en una relación de poder, así como de la posición favorable o desfavorable que ocupan, por lo cual consideran su comportamiento algo natural y propio de la vida. Cuando algo

así ocurre se está ante un caso de *poder tácito*. En materia de seguridad y defensa, el poder tácito es transversal a la aparición de amenazas no estatales (por ejemplo, insurgencia y terrorismo), donde el objetivo es influenciar indirectamente a la población. De igual forma, el poder tácito hace parte activa de los estudios donde se analizan las estructuras sociales del poder, y la relación de estas con el individuo; a ese respecto, los de Michel Foucault son los más reconocidos.

Los niveles de conciencia en las relaciones de poder generan, entonces, una dualidad que debe ser tomada en cuenta en el contexto del ciberespacio: poder directo y poder tácito; sin embargo, dicha dualidad no se manifiesta de manera independiente, sino a través de las interrelaciones *interciberespaciales*. Al final de cuentas, el poder es una dinámica entre actores que es incapaz de existir abstraída de la relación que se gesta entre ellos.

Queda una cuestión final que debe ser respondida para completar las premisas de este capítulo, y la cual *cuestiona* el origen del poder. Respecto a si este realmente se adquiere y se pierde de formas particulares o si, por el contrario, es una variable perenne e innata de la condición humana, este libro acepta ambas posturas. En el ciberespacio, tal como se mostrará, existen medios de los cuales emana el poder, y dichos medios se pierden o se agotan en el tiempo. De igual forma, al ser el ciberespacio un entorno donde los seres humanos transfieren sus interacciones, muchas de las estructuras sociales del "mundo real" son, voluntaria o involuntariamente, replicadas (por ejemplo, valores, códigos de conducta, vigilantismo, etc.).

El poder comportamental en las interrelaciones interciberespaciales

La desestatalización, acompañada por la relativa desterritorialización, aparta al ciberespacio de la concepción hobbesiana del poder. Al difuminarse el rol del Estado y generarse los vacíos de soberanía propios de la relación con el territorio, se vuelve inviable el impulso unánime de toda la colectividad ciberespacial de transferir o ceder, en términos de Hobbes (como se cita en Buzan, 1983), los medios de poder a un leviatán para garantizar la seguridad en un entorno anárquico. En consecuencia, se genera una proliferación de actores que pueden fungir como intermediarios de la voluntad del Estado, así como competir o no con este en el desarrollo de gobernanza; estos serán denominados a partir de ahora como *actores reguladores*.

Los principales *actores reguladores* identificados son los Estados, las plataformas/sistemas, los escenarios cibernéticos, y las comunidades virtuales. Estos ejercen influencia sobre las interrelaciones de los usuarios del ciberespacio o, en otras palabras, delimitan lo que estos últimos pueden y no hacer, al igual que la forma como lo hacen. Esa habilidad es denominada por este libro como *poder comportamental*, y será el objeto de análisis de la presente sección. Este tipo de poder puede ser tácito o directo, dependiendo del nivel de conciencia que los actores mencionados, junto con el usuario final, tengan de la relación.

Entender a los *actores reguladores* y la manera como estos se comportan y ejercen poder comportamental requiere el desarrollo de cuatro conceptos sociológicos básicos: comunidad, membresía, sistemas de valores y autoridad. Estos son requeridos porque el ciberespacio, no obstante ser intangible, es un lugar donde ocurren interrelaciones que, al final, siguen siendo entre personas. Y las personas, en su comportamiento como criaturas sociales, extrapolan al ciberespacio, consciente o inconscientemente, *mecanismos de autorregulación existentes* en el "mundo real" (por ejemplo, administradores, aceptación de términos, resolución de controversias, vigilantismo, etc.) (Brainard, 2010; Fox & Roberts, 1999).

Las comunidades, desde la posición del comunitarianismo de Walzer (1983), son un conjunto de individuos que conviven e interactúan para el cumplimiento de un objetivo común. En estas, la membresía, entendida como la posibilidad de ser parte del grupo, se distribuye con el fin de asegurar que únicamente los iguales estén juntos. Los criterios de distribución de la membresía y la calidad de "igual" se desprenden de la alineación y la aceptación de un sistema de valores que constituyen la identidad de la comunidad. A eso se le conoce como la *autodeterminación de la comunidad* y, en teoría, sus miembros deberían estar prestos a defenderla.

El sistema de valores se compone de múltiples elementos: creencias, ritos, historias, memoria colectiva, normas y leyes, símbolos y comportamientos aceptados y condenados, entre otros. Dicho sistema se manifiesta a través de las instituciones de gobierno, religión y educación, al igual que en los medios de expresión escrita, oral y visual (por ejemplo, arte, leyes, literatura, canciones, etc.). Para que un sistema de valores sea útil para la comunidad, este debe ser claro y enseñado a sus miembros (Wray-Lake et al., 2014).

La desviación del sistema de valores —y por ende, el incumplimiento del contrato social— puede desencadenar distintas formas de castigo. Estos pueden

ser *privativos* (por ejemplo, el aislamiento), *físicos y psicológicos* (por ejemplo, la tortura y la muerte), *económicos* (por ejemplo, las multas y las compensaciones), *simbólicos* (por ejemplo, el señalamiento y la exigencia de disculpas públicas), e ir directamente contra la membresía (por ejemplo, la expulsión y el exilio). El propósito del castigo es forzar el cumplimiento —incumplir en sí mismo ya constituye algo— y suplir el daño que la acción genera en la comunidad o en algún otro miembro.

Aquel considerado la "autoridad" es quien se encarga de velar por el sistema de valores, así como de determinar y ejecutar el castigo correspondiente. La autoridad puede ser adquirida por mérito propio, como ocurre en las dictaduras, o ser designada a través de la elección popular. En cualquier caso, y no sin un límite en la mayoría de los casos, la autoridad controla los medios coerción, disuasión y persuasión. Por ejemplo, en las democracias sus miembros, entendidos como los nacionales, o población, ceden al gobierno el monopolio de la fuerza (por ejemplo, la policía), pero este tiene ciertas reglas que, por principio, debe respetar, y que se pierden completamente en los regímenes dictatoriales (por ejemplo, el uso de la policía para reprimir la oposición política).

Al trasponer estos cuatro conceptos sociológicos al contexto de *ciberespacio*, y suponiendo que se mantengan el comportamiento social que nos define como especie y el acceso tecnológico, todos los usuarios, desde los comunes hasta los considerados ilegales ante los ojos de la ley (por ejemplo, criminales, terroristas, etc.), hacen parte de o han tenido acceso a algún tipo de comunidad virtual. La comunidad virtual se erige como una asociación de usuarios, con o sin identidad diluida, que conviven e interactúan por o para un fin común en particular (Brainard, 2010; Fox & Roberts, 1999).

Las comunidades virtuales tienen, por lo general, una persona denominada "administrador", que tiene las funciones de: proteger el sistema de valores de la comunidad; otorgar y modificar accesos y privilegios, y aceptar, negar y despojar membresías. Dicho administrador puede o no ser el creador de la comunidad, y termina estableciendo qué interactúan los miembros dentro del marco del objetivo común que los define, y cómo lo hacen. Por ejemplo, el administrador de una comunidad existente en un foro o en un grupo de red social que tiene como fin compartir fotos de aves establece normas frente a la autoría de tales imágenes, y puede *bannear* (prohibir) —equivalente ello a despojar de la membresía— a los usuarios que se adjudiquen impropiamente créditos o que solo comparten fotografías de automóviles.

Las comunidades virtuales no existen en la nada: requieren un escenario cibernético delimitado que las soporte (por ejemplo, redes sociales, aplicación, intranet, videojuegos en línea, canales, foros, *boards*, *chans*, *chats*, etc.). El escenario cibernético es un conjunto de datos, parámetros, configuraciones, protocolos y demás que son designados para cumplir un fin determinado que implica el acceso de varios usuarios conectados en red (i.e. comunicarse, compartir imágenes, realizar transacciones, etc.). La accesibilidad se hace posible y fácil a través de la creación de interfaces gráficas y auditivas instintivas para los usuarios; adicionalmente, los componentes que dan vida a los escenarios cibernéticos se encuentran alojados en otras plataformas o sistemas de mayor envergadura, o dependen de ellos para su funcionamiento. Algunos escenarios famosos son Instagram, YouTube, WhatsApp, Facebook, Twitter y 4Chan. La *Dark Web* también tiene los suyos, pero son más difíciles de ubicar de forma permanente (por ejemplo, 8Chan). Una característica de los escenarios que debe tomarse en cuenta es su capacidad para dar forma a más de una comunidad virtual no excluyente; es decir, comunidades que brindan a los usuarios membresía de manera simultánea. Así, en el ejemplo del grupo de aves, los usuarios pueden ser miembros, de forma paralela, de otras comunidades dentro de Facebook.

Al igual que ocurre en las comunidades virtuales, los escenarios cibernéticos tienen sus propios sistemas de valores, los cuales dan a conocer, en la mayoría de los casos, en forma de "condiciones" de prestación del servicio. Estas condiciones aplican sobre todas las comunidades virtuales que utilizan el escenario cibernético para existir, al igual que los usuarios que se encuentran en cada una de ellas. En el caso YouTube, producto de Alphabet Inc., cuando alguien se dispone a crear una identidad o una cuenta, el escenario requiere al usuario remitirse a los siguientes términos:

> Al usar o ingresar al sitio de Internet de YouTube o cualquier producto, software, feed de datos y servicio de YouTube […] usted acuerda expresamente (1) estos términos y condiciones (en lo sucesivo los "Términos del Servicio"), (2) la política de privacidad de YouTube […]que declara expresamente conocer y aceptar en todos sus términos, y que se considera aquí íntegramente reproducida […] y (3) los Lineamientos de la Comunidad YouTube, […] que declara expresamente conocer y acepta en todos sus términos […] Si no estuviera de acuerdo con los Términos del Servicio, la política de privacidad de YouTube o los Lineamientos de la Comunidad YouTube, por favor no utilice el Servicio. (YouTube, s.f.)

En el ciberespacio muy pocos escenarios existen sin un "dueño"; la mayoría de estos son productos o servicios prestados, con o sin ánimo de lucro, por usuarios o empresas. Dichos "dueños" son, igualmente, *actores reguladores*, identificados con el nombre de plataforma/sistema en esta sección, que tienen sus propios sistemas de valores, los cuales proyectan hasta el usuario final. Facebook, por ejemplo, es una plataforma/sistema que tiene bajo su tutela diferentes escenarios cibernéticos, considerados por ellos productos o servicios, y sobre los cuales establecen los términos que se detallan a continuación.

Declaración de derechos y responsabilidades

> Esta Declaración de derechos y responsabilidades […] tiene su origen en los Principios de Facebook y contiene las condiciones de servicio que rigen nuestra relación con los usuarios y con todos aquellos que interactúan con Facebook, así como con las marcas, los productos y los servicios de Facebook, que se denominan "servicios de Facebook" o "servicios". Al utilizar o acceder a los servicios de Facebook, muestras tu conformidad con esta Declaración, que se actualiza periódicamente […] Puesto que Facebook ofrece una amplia gama de servicios, es posible que te pidamos que leas y aceptes condiciones complementarias aplicables a tu interacción con una aplicación, un producto o un servicio determinados. (Facebook, 2015)

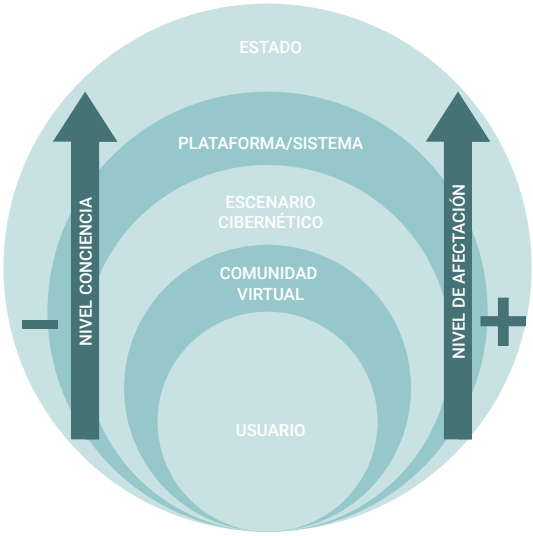
Facebook, como se evidencia en el fragmento anterior, contiene sus propios "principios" —elementos de un sistema de valores— que, espera, sean aceptados por todos, y que eventualmente acaban influenciando las interacciones de los usuarios. Los principios del sistema/plataforma son: 1) libertad para compartir y conectarse; 2) propiedad y control de la información; 3) flujo libre de información; 4) igualdad fundamental; 5) valor social; 6) plataformas y estándares abiertos; 7) servicio fundamental; 8) bienestar común, y 9) un mundo. Los sistemas/plataformas no son autónomos, pues sus actividades se hallan regidas por las reglamentaciones del territorio donde su infraestructura tecnológica se encuentra, así como por las del sitio donde prestan el servicio. Así lo establece Facebook cuando afirma en la introducción de sus principios que "la consecución de estos […] debería estar limitada únicamente por la ley, la tecnología y las normas sociales en continuo desarrollo" (Facebook, s. f.).

La manera como los *actores reguladores*, desde el Estado hasta la comunidad virtual, influencian las interrelaciones de los usuarios, o, en otras palabras, proyectan poder comportamental, se puede describir a la manera de un flujo en

cascada, como el que se muestra en la figura 1. Un evento ocurrido en Singapur en 2014 permite describir de mejor manera dicho flujo, al igual que la manera como este tipo de poder funciona.

Singapur es uno de los países con tejido social más complicados del mundo. En esta pequeña isla del Pacífico conviven miles de personas provenientes de múltiples países, al punto de que existen en su territorio cuatro idiomas oficiales (i.e. inglés, mandarín estándar, tamil y malayo) y diez religiones (i.e. hinduismo, zoroastrismo, judaísmo, budismo, taoísmo, jainismo, cristianismo, islam, sijismo y baha'i). En el pasado, el país sufrió revueltas religiosas y raciales; una de las más complejas fue la de 1964, denominada *Communal Riots*, que dejó varias docenas de muertos y heridos (Richard, 1984).

Figura 1. *Establecimiento de los flujos del poder comportamental, según los autores reguladores*



Fuente: elaboración propia.

Con el fin de evitar nuevas rupturas en la nación, el gobierno de Singapur estableció fuertes leyes contra cualquier manifestación de "discursos de odio", o *hate speech*, por medio de la *Sedition Act* (The Statutes of the Republic of Singapore, 2013). Las empresas de servicios cibernéticos que operan en la isla deben tener especial cuidado y ver por el cumplimiento de sus políticas frente a la temática. De igual forma, transfieren esas políticas a los productos que

ofrecen, y esperan que los usuarios acepten y cumplan, como clientes, ciertos compromisos. Un usuario que no admita dichos términos, simplemente, no podrá hacer uso del servicio (Price, 2002).

En junio de 2014, Google (plataforma o sistema) se vio obligado a remover el blog llamado *Blood Stained Singapore* (comunidad virtual), ofrecido por su producto Blogger (escenario cibernético), luego de que el gobierno singapurense emitió su "recomendación" al respecto. El blog tenía como propósito describir y demostrar disgusto, de manera no violenta, hacia la población filipina que habita la isla. Las autoridades locales consideraron que esa era la visión de un extremista que podría ser enjuiciado, junto con sus simpatizantes (usuarios), mientras algunos analistas vieron en ello un disgusto de la población frente a las políticas laborales (*The Independent*, 2014).

Los usuarios del ciberespacio en Singapur, y muy seguramente en otros países, vieron cómo los valores considerados correctos por un Estado fueron impuestos a un sistema o una plataforma de servicios cibernéticos. Así mismo, evidenciaron cómo estos se transformaron en políticas que los clientes tuvieron que aceptar para emplear sus productos y, eventualmente, poder interactuar. En tal sentido, los usuarios en Singapur que empleen los servicios de Google enfrentan la siguiente situación: aceptar los términos (i.e. no hacer expresiones de odio) para emplear el escenario que les permite constituir una comunidad virtual donde interactuar o, por el contrario, no hacerlo y verse obligados a buscar otro medio. (Siyuan & Chen-Wei, 2019).

El flujo de los *actores reguladores* tiene sus propias particularidades que deben distinguirse, y que el ejemplo de Singapur no desarrolla. En primera instancia, si bien la figura 1 muestra una relación jerárquica, el flujo no necesariamente es continuo; en otras palabras, la influencia puede provenir desde cualquiera de los niveles superiores al usuario, y no necesariamente tiene que pasar por todos los niveles para ser efectiva. Veamos a continuación algunos casos en los cuales esto se genera.

1. Flujo Directo Estado-Usuario

- En 2015, el ciudadano neozelandés Philip Blackwood fue sentenciado a dos años de cárcel y trabajos forzados en Myanmar por valerse de una imagen de Buda usando audífonos para promocionar un bar en su cuenta de Facebook. Aunque Facebook no consideraba esto una violación de sus "normas comunitarias o principios", para el país donde se

encontraba el usuario el acto fue tipificado como el delito de "irrespeto a la religión" (Associated Press & AFP, 2015).

- En 2017, dos ingleses fueron capturados en Tailandia por realizar *streaming* ilegales, con ánimo de lucro, de los partidos de la Champions League, a través de Cajas Kobi y de IPTV. Aunque el país asiático no es famoso por sus reglas hacia la propiedad intelectual —y eso no es diferente en sus prestadores de servicios cibernéticos—, la operación se hizo por la presión ejercida desde el gobierno británico. Prueba de dicha presión es que los individuos fueron eventualmente entregados a la embajada inglesa (*BBC News*, 2017).

2. Flujo directo plataforma/sistema-usuario

- Aunque los países tienen diferentes regulaciones frente a la protección de datos y de información personal, Alphabet Inc. —nuevo *holding* que contiene a Google— establece su propio criterio a los usuarios de cualquiera de sus servicios creando su propio conjunto de normas —componente de un sistema de valores—. En su sección de "Condiciones y privacidad" se lee textualmente:

  > Al subir, almacenar o recibir contenido o al enviarlo a nuestros Servicios o a través de ellos, concedes a Google […] una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas […] comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de proporcionar, promocionar y mejorar los Servicios y de desarrollar servicios nuevos. Esta licencia seguirá vigente incluso cuando dejes de usar nuestros Servicios. (Google, 2017)

- SERVNET es un sistema/plataforma de la *Dark Web* que tiene como función brindar *hosting* y encriptación, y diseñada principalmente para la Tor Network. Debido a su naturaleza, no es posible determinar a qué sistema legislativo se supedita SERVNET, pero establece una serie de normas para la prestación de su servicio a todos los escenarios cibernéticos y usuarios:

  > Network Security - You are not allowed to use this service for:
  >
  > » Spam, all forms of Email Abuse and Bulk Email related products
  >
  > » Background running programs (bots/daemons/monitors)

» Unauthorized monitoring of data or traffic on any network or system without express authorization.

» IP range scanning/port scanning/vulnerability scanning

» Unauthorized access to or use of data, systems or networks, including any attempt to scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization.

» The placement of material not deemed in good taste is not permitted such as CP - customer is held fully responsible for any misuse of account regardless of whoever published the content.

» Distributed Denial of Service (DDoS) - No resources and servers may be used to perform any form of DDoS/DoS attacks. (Sevnet, s. f.)

3. Flujo directo escenario cibernético-usuario:

- Wordpress.org es una de las plataformas disponibles para el almacenamiento y el desarrollo de blogs. Aunque cada blog es una comunidad virtual independiente, Wordpress.org establece una serie de reglas que deben ser tomadas en cuenta, y las cuales no hacen referencia a ningún Estado en particular. Algunas hacen referencia a conceptos técnicos para el uso del correcto del servicio, mientras otras establecen una lista de contenido que no es permitido: *spam*, pornografía, publicar información personal, publicidad, violaciones a la propiedad intelectual…
- GALAXY 3 es una red social de la *Dark Web* que tiene como propósito conectar usuarios que quieran interactuar de manera anónima. Es soportada por el sistema/plataforma Elgg (elgg.org), pero no es posible determinar algún lugar geográfico que la vincule a leyes específicas —no tendría sentido si el propósito es tener anonimato en la *web*—. Aun así, GALAXY 3 establece las siguientes reglas para, como afirma, evitar que esta se convierta en un mercado situado en el foco de atención de las diversas agencias gubernamentales y de las fuerzas policiales, así como para evitar que se convierta en el blanco de tales agencias:

  1. No images of children. Including 3D or cartoon. Use your common sense, if in doubt ask before you post. DO NOT ask for these things either, you will be banned […] 2. No public commercial trade. We don't want Galaxy3 turning into a market place targeted by Government agencies […] 3. No pornographic

> content and / or gore in public areas. Legal (18+) pornography / erotica and gore are allowed in closed groups [...] 4. Images and avatars are considered public content, so rule 1. and rule 3. apply [...] 5. No doxing or posting anything that may endanger someone [...] 6. Do not solicit members into committing a crime. This includes, but not limited to, hacking and carding requests [...] 7. Do not advertise criminal internet resources (clearnet or hidden) [...] 8. Be respectful. Galaxy is a respectful community, allowing Freedom of Speech. Harassment will get you banned [...] 9. Do not spam [...] 10. Do not scam [...] 11. Do not advertise extremist / terrorist material [...] 12. No public sex ads. This is not a dating site. (Galaxy 3, s. f.)

4. Flujo directo comunidad virtual-usuario

- Actualmente existe una proliferación de grupos cerrados en Facebook que se diseñan con diversos propósitos: por ejemplo, compartir una pasión, tranzar bienes o servicios y establecer redes de apoyo. Dichos grupos, generalmente, tienen un administrador que establece las reglas de interacción y determina qué es o no realizable en la comunidad. Dichas reglas no necesariamente son un reflejo de Facebook o de las leyes de los Estados. Así, es común ver cosas como: "prohibido ofrecimientos por inbox", "publicaciones con fotos reales", etc.
- LOLIFOX es una comunidad de la *Dark Web* que permite crear *imageboards* —una especie de foro que opera, principalmente, haciendo uso de imágenes—. LOLIFOX establece una serie de reglas aplicables para todos los usuarios que hacen uso de sus *boards*. No es posible establecer una línea directa de influencia de otros *actores regulares*, por lo cual es posible suponer que las siguientes reglas son propias del administrador de LOLIFOX:

  > (1) Do not post child pornography or questionable 3DCG/3DPG/human dolls sexual depictions of children or child abus e[...] (2) Do not post wipe, spam, bypassing spam sheet, damage to the site and calls for it [...] (3) Bypassing the ban can lead to an increase in the ban period and removal of all posts [...] (4) The user is personally responsible for the materials posted on the site and for compliance with the laws of the country in which it is located. (Lolifox, s. f.)

- DEVIL'S SKY-MARKT es un mercado en la *Dark Web* que funciona con *bitcoins*, y en el cual es posible hallar diferentes drogas (por ejemplo, cocaína, LSD, marihuana, heroína) y servicios de *malware* y *hackeo*, así como elementos falsificados (por ejemplo, dinero, tarjetas de crédito, pasaportes, etc.).

A pesar de tener una naturaleza ilegal, el administrador demarca los bienes prohibidos que se vayan a tranzar: servicios de asesinato, venenos, armas de destrucción masiva, pornografía infantil o armas de fuego, y acciones que atenten contra la integridad de personas (i.e. *red romos*). De igual manera, establece unos comportamientos prohibidos para los usuarios, como, por ejemplo, subirse personalmente la calificación, o *rating*.

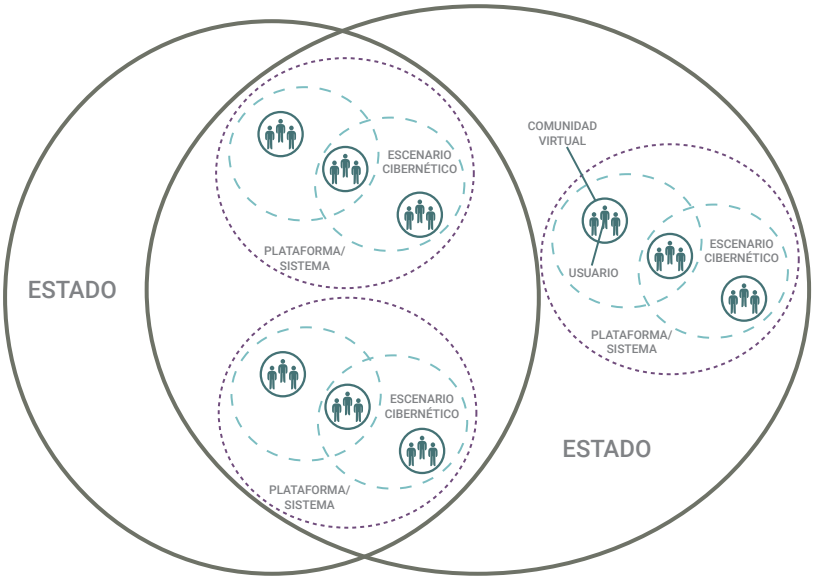
Las demás características del flujo de los *actores reguladores* que es necesario describir responden a los niveles de conciencia y de influencia, como se muestra en la figura 1. Centrado en la posición de los usuarios finales, la conciencia que estos tienen del poder comportamental que ejercen los *actores reguladores* sobre sus habilidades para realizar interacciones interciberespaciales tiene una tendencia a decrecer a medida que dichos usuarios se acercan más al Estado; no obstante, no puede afirmarse lo mismo de la relación entre *actores reguladores*. Los casos estudiados evidencian que estos, por lo general, conocen los sistemas de valores de quienes que se encuentran en un lugar superior en la jerarquía, lo cual explica por qué crean descargos de responsabilidad —en inglés, *disclaimer*—.

Es necesario profundizar en la explicación de la tendencia frente a la conciencia en el flujo de los actores reguladores. Aun así, la sociología nos brinda una pista: Foucault (1982) incita a pensar que identificamos con mayor facilidad los sistemas de valores de las estructuras con las cuales tenemos una interacción directa (por ejemplo, familia, colegio, amigos, clubes etc.), y tendemos a desconocer las que son más subjetivas; de ahí que sean pocas las personas que conocen las leyes que gobiernan al ciberespacio en cada país donde se encuentran, y menos aún, las que leen y cumplen los términos de un sistema/plataforma.

La característica final del flujo de los *actores reguladores* tiene que ver con el nivel de influencia o, en otras palabras, la magnitud de poder comportamental que son capaces de transmitir a otros actores y usuarios finales. El Estado es el actor que ejerce mayor influencia, y esta se va diluyendo para los otros actores en la medida en que se acercan al usuario final en la jerarquía descrita en la figura 1. De esa manera, y debido a la *desterritorialización*, los Estados solo podrán influenciar a quienes se encuentren en su territorio, salvo que haya alguna herramienta que brinde capacidades transnacionales. Así mismo, una plataforma/sistema solo podrá influenciar los escenarios cibernéticos bajo su control directo; los escenarios cibernéticos y a sus comunidades, y estas últimas, a sus miembros.

Existe, entonces, un límite a la influencia del poder comportamental que se manifiesta a modo de una frontera imaginaria, como se muestra en la figura 2. A pesar de ello, se debe tener presente que la manifestación simultánea de múltiples *actores reguladores* no implica que sus sistemas de valores sean excluyentes: por el contrario, pueden fácilmente darse los casos en los que estos se complementen, o en los que un *actor regulador* define cuál es el sistema que tiene mayor preponderancia. De igual forma, los actores pueden optar por esquemas de coinfluencia, a través de mecanismos de cooperación o entendimiento (i.e. *joint-ventures*, tratados, etc.).

Figura 2. *Distribución de la influencia de los actores reguladores en el marco del poder comportamental.*



Fuente: elaboración propia.

Facebook, en sus condiciones de servicio, hace la salvedad de que, debido a la existencia de múltiples productos, los cuales se comportan como escenarios cibernéticos delimitados, hay términos complementarios que pueden llegar a entrar en conflicto con su "Declaración de Condiciones (DDR)". Por tal razón, el sistema/plataforma afirma lo siguiente:

> Puesto que Facebook ofrece una amplia gama de servicios, es posible que te pidamos que leas y aceptes condiciones complementarias aplicables a tu interacción con una aplicación, un producto o un servicio determinados. En caso de que esas condiciones complementarias entren en conflicto con esta DDR, las condiciones complementarias asociadas con la aplicación, el producto o el servicio prevalecerán en lo referente al uso de tales aplicaciones, productos o servicios en caso de conflicto. (Facebook, 2015)

Los Estados utilizan comúnmente los medios ofrecidos por las organizaciones internacionales para entablar mecanismos de cooperación. Los compromisos adquiridos o demostrados en los documentos de dichas organizaciones no contravienen, por ser un principio fundacional de estas, la soberanía de ninguno de sus miembros. En tal sentido, los sistemas de valores de los Estados coexisten paralelamente para lograr cierto grado de coinfluencia en el ciberespacio o, en otras palabras, proyectar de manera conjunta poder comportamental.

En el contexto del ciberespacio, la Organización de los Estados Americanos (OEA) tiene varios documentos que sirven para demostrar la afirmación anterior. Estos son: 1) *Declaración sobre Seguridad en las Américas de 2003; 2) Seguridad Multidimensional* (OEA/Ser.K/XXXVIII/ CES/dec.1/03 rev. 1); 3) *Adopción de una Estrategia Inter-americana para combatir las Amenazas a la Ciberseguridad* (AG/RES. 2004/XXXIV-O/04), y 4) *Declaración para el Fortalecimiento de la Ciberseguridad en las Américas* (OEA/Ser.L/X.2.12/ 7 March, 2012 CICTE/ DEC.1/12 rev. 1).

La *Declaración de Seguridad de las Américas*, de 2003, reconoce los incidentes en la seguridad cibernética como una amenaza no tradicional a los Estados. En la mencionada declaración los miembros se comprometen a enfrentar las manifestaciones de terrorismo y delincuencia en el ciberespacio, así como a desarrollar e implementar una estrategia integral de la OEA sobre seguridad cibernética. La estrategia diseñada (AG/RES. 2004/XXXIV-O/04) urge, entre otros elementos, a que los Estados participantes establezcan e identifiquen los *Computer Security Incident Response Teams* (CSIRT). Tales compromisos se reafirman en la *Declaración para el Fortalecimiento de la Ciberseguridad*, de 2012.

Se debe tener presente que el poder comportamental no se circunscribe únicamente a las interacciones interciberespaciales persona-persona, sino que también cobija aquellas entre persona-sistema y sistema-sistema, lo cual significa que los estímulos, automatizados o no, tienen unos limitantes. Por ejemplo,

por más que un usuario quiera vulnerar un escenario delimitado, estos tendrán políticas que expresan directamente el comportamiento como indeseado. De forma similar, los sistemas de valores restringen las respuestas recíprocas a los estímulos de un actor. En otras palabras, un miembro de una comunidad virtual no debería esperar que otro responda inmediatamente de forma contraria a las reglas internas, incluso si es incitado.

Debe hacerse una última observación frente al poder comportamental, y es sobre la capacidad de los actores para resistir la influencia. Existen múltiples técnicas para hacerlo —esto será la temática del próximo capítulo, pero, dicho de forma superficial, es posible tomando la decisión de migrar, crear o destruir los escenarios donde se realizan las interrelaciones interciberespaciales—; sin embargo, al igual que como ocurre con el resto del modelo, cuanto más cerca se esté del Estado, tanto más difícil será. Por ejemplo, un usuario cansado de la forma como un administrador lleva la dinámica en un grupo de Facebook puede optar por salirse para buscar o crear uno nuevo y, de esa forma, hacer que la influencia del administrador desaparezca; no obstante, cambiarse de red social es más difícil, y aún más lo será encontrar un escenario cibernético que no se halle controlado por alguna de las grandes compañías de tecnología (por ejemplo, Facebook, Apple, Microsoft, Amazon, eBay o Alphabet).

En la *Dark Web*, la dinámica descrita se manifiesta de una forma muy similar, salvo por el comportamiento del Estado. Debido a los productos y los servicios ilegales que allí se transan —se debe mencionar que no todo lo que allí se transa o se hace es necesariamente ilegal—, los Estados son bastante agresivos en buscar el cumplimiento de sus sistemas de valores por parte de los demás *actores reguladores* y usuarios. Ello termina reflejándose en una mayor destinación de recursos para el ejercicio de la autoridad y en castigos más fuertes.

En términos de la concepción básica del "poder"-relación de "A" y "B", el poder comportamental se traduce de la siguiente manera: un *actor regulador* ("A") puede lograr que otro *actor regulador* de menor jerarquía, o usuario final ("B"), realice o no algo en el ciberespacio que guarda estrecha relación con un sistema de valores predefinido. Para ello, el sistema es acompañado de mecanismos de castigo y autoridad que pueden afectar, entre otros, la membresía. En cualquier caso, el poder comportamental de "A" sobre "B" termina influyendo las interacciones de "B", así como las respuestas recíprocas de terceros a sus estímulos.

El poder funcional en las interacciones interciberespaciales

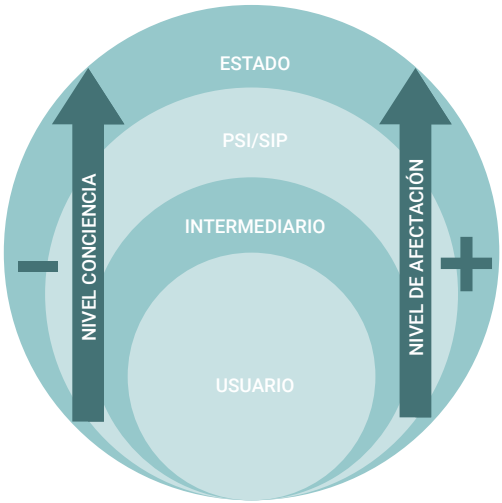
El ciberespacio depende de unos componentes materiales y tecnológicos para existir como un entorno intangible donde los usuarios pueden interrelacionarse (por ejemplo, redes, computadores, servidores, cableado, etc.). Quienes controlan y vulneran estos elementos tienen la facultad para determinar quiénes pueden interactuar y por cuánto tiempo, así como los resultados de algunas interacciones. La facultad descrita es denominada por este libro *poder funcional* y, al igual como ocurre con el comportamental, tiene una serie de *actores reguladores* con su respectivo flujo de influencia y su respectivo nivel conciencia. Dichos actores son: Estados, proveedores de servicio de internet (PSI/) e intermediarios.

En el capítulo segundo se desarrolló la manera como los Estados ejercen soberanía sobre el componente físico del ciberespacio que se encuentra en sus territorios, según se ve en la figura 3. En dicho capítulo se sugirió que los Estados, como lo evidenciaba el caso del "Gran Firewall de China", tienen la facultad de limitar acceso al ciberespacio y controlar su contenido para todos los usuarios que se hallen sujetos al sistema jurídico nacional. La misma idea fue ampliada en el poder comportamental, y ahora es necesario retomarla para entender el poder funcional.

En la mayoría de los países existen normatividades que reafirman el absoluto dominio del Estado sobre todo lo que tiene que ver con las telecomunicaciones en el interior de sus fronteras. Y como la mayoría de estos no tienen la capacidad o los recursos para satisfacer autárquicamente la necesidad, también establecen los procedimientos y las contraprestaciones para ceder a empresas privadas la prestación del servicio. De esa forma, la primera manifestación del poder funcional es la potestad del Estado para determinar quiénes pueden brindar acceso al ciberespacio, así como las reglas generales para hacerlo; en otras palabras, para seleccionar los actores reguladores en el nivel PSI, tal cual se muestra en la figura 3.

En Colombia se estableció la Ley 1341 de 2009, por la cual se definen los principios y los conceptos sobre la sociedad de la información y organizaciones de las TIC. En su artículo 10, se habilita de forma general la provisión de redes y servicios de telecomunicaciones, el cual se reconoce como un servicio público, bajo la titularidad del Estado, a terceros que quieran hacerlo a cambio de una contraprestación periódica. Ello se ve complementado por el Decreto 1078 de 2015, que obliga a todos los posibles interesados a tener un *Registro TIC* para facilitar el control estatal.

Figura 3. *Establecimiento de los flujos del poder funcional, según los autores reguladores*



Fuente: elaboración propia.

La segunda manifestación del poder funcional desde el Estado es la prohibición expresa de acceso a internet en ciertos lugares y nichos poblacionales. Canadá, por ejemplo, prohíbe el uso de internet en sus cárceles provinciales y federales para los prisioneros. Estados Unidos, por el contrario, tiene un sistema altamente monitoreado que permite un acceso restringido a sus presidiarios a correos electrónicos (i.e. *Trust Fund Limited Inmate Computer System*), así como internet para fines de educación y reintegración.

La tercera manifestación del poder funcional del Estado es, como en el caso de China, su habilidad para manipular y denegar cierta información a los usuarios del ciberespacio a partir de consideraciones en sus sistemas de valores. Esto último, en los términos del primer capítulo, significa que los estímulos de los usuarios solo tendrán las respuestas recíprocas esperadas, no por ellos, sino por un tercero aparentemente exógeno a la interacción (por ejemplo, búsquedas de Taiwán en China). Esta última manifestación pone sobre la mesa, y de manera evidente, la relación que hay entre ambos tipos de poder.

El poder funcional y el poder comportamental son independientes, pero se hallan estrechamente relacionados. El primer tipo de poder afecta directamente al ciberespacio como entorno, y tácitamente, a los *actores reguladores* y usuarios finales. El segundo tipo, por el contrario, afecta particularmente a los actores

y usuarios, sin que ello implique algún tipo de influencia sobre el ciberespacio. Aun así, el poder funcional se alimenta del sistema de valores central del comportamental para justificar su aplicación; es decir, para encontrar un argumento que permita dictar los términos de conectividad al ciberespacio y el acceso a información. Miremos una analogía que nos permita entender esto mejor:

Imaginemos un bar exclusivo que brinda el lugar perfecto para interactuar. En la entrada de este se encuentra un individuo del personal encargado de brindar seguridad, así como de permitir y cobrar el ingreso a otras personas. Supongamos que al personal de seguridad se le han dado unos criterios para controlar la admisión: solo mayores de edad, uso de traje formal, 50 dólares por persona y hasta las 2:00 a. m. Adicionalmente, y una vez dentro, se espera que los clientes tengan un comportamiento enmarcado dentro de las reglas fijadas por la administración.

El personal de seguridad está empleando poder funcional cuando configura la naturaleza del bar, y cuando determina quiénes pueden entrar o no, así como el tiempo de permanencia. Quienes se encuentran afuera solo podrán interactuar con los demás clientes si superan, a través del cumplimiento de los requisitos de ingreso, la infraestructura física que conforma al bar, y que funge como barrera (i.e. paredes, ventanas y puertas). Una vez adentro, el sistema de valores del establecimiento entra en acción ejerciendo poder comportamental sobre todos los presentes, y configurando lo que se puede o no se puede hacer, al igual que las formas para ello. Las personas que no acepten o violen el sistema de valores podrán ser expulsadas del lugar.

En la analogía, el entorno donde las personas se encuentran interactuando, lo que entendemos abstractamente como "bar", es el ciberespacio. La mesa, las paredes, los asientos, la barra, la música, los aromas y los demás componentes que hacen posible la concepción de un "bar" equivalen a la infraestructura física y digital del ciberespacio. Las reglas impuestas por la administración a sus clientes son similares a los sistemas de valores que proyectan los *actores regulares*; en este caso, una comunidad virtual. Y la función que cumple el personal de determinar el ingreso y la permanencia de los clientes es, como veremos a continuación, análoga a la de un proveedor del servicio de internet.

Ahora bien, supongamos que a la puerta del bar llega alguien que cumple con los criterios de ingreso, pero viene en estado de embriaguez. El personal de seguridad puede optar por restringirle a dicha persona el acceso al establecimiento argumentando que tiene la capacidad potencial para violentar las reglas

de comportamiento fijadas por la administración. En tal sentido, el poder funcional se alimenta del sistema de valores del poder comportamental. Un equivalente en el ciberespacio es cuando China bloquea las búsquedas en internet relacionadas con Tiananmen porque contradicen la lectura oficial de los hechos y, por ende, pueden poner en peligro la unidad de la nación.

No solo los Estados ejercen poder funcional en el ciberespacio: todos los que tengan privilegios y control sobre la infraestructura física y su configuración podrán hacerlo. Los PSI, de hecho, ejercen tal tipo de poder sobre sus usuarios. Al controlar los servidores de conexión, ellos determinan quiénes pueden acceder al ciberespacio, su velocidad de conectividad y el tiempo disponible.

Supongamos que un usuario quiere ver todas las temporadas disponibles de la serie de moda en su computador, vía *streaming*. Para ello, el usuario contrató por un mes con un PSI una suscripción prepagada a internet que le brinda 1MB de velocidad real; sin embargo, debido a la longitud y el número de capítulos, requeriría al menos dos meses para satisfacer completamente su interés. Al comenzar el proceso de *streaming*, el usuario se da cuenta de que la velocidad de su servicio detiene constantemente la reproducción, y hace casi imposible disfrutar la serie.

En términos del poder funcional e interacciones en el ciberespacio, la situación hipotética del *streaming*, bastante común de por sí, se traduce de la siguiente forma: el individuo hace un estímulo al sistema que almacena la serie, del cual obtiene la respuesta recíproca esperada, pues evidencia cómo el video carga en su computador; no obstante, el ancho de banda que el PSI le permite tener (i.e. 1 MB) constriñe el nivel de respuesta del sistema, y eso lleva a que el interés del individuo se vea afectado. Así, las condiciones del PSI, las cuales representan sus posturas económicas como prestador del servicio, establecen unas condiciones —en tiempo y modo— que enmarcan el ciberespacio donde nuestro individuo pretende interactuar.

Otra manifestación del poder funcional que permite ilustrar cómo un actor diferente del Estado delimita al ciberespacio para otros, desde el contenido y la información, ocurre cuando tenemos conexión de cortesía en algún establecimiento. Cuando llegamos a un lugar comercial o público, y hacemos uso de su Wifi, es común someterse a un cronómetro que indica el uso gratuito de conexión, diferentes procesos de registro y autenticación, *banners* de propaganda y un sistema de control parental. Dichos elementos influencian enormemente las formas como interactuamos, al igual que las razones para hacerlo.

Seguramente, muchos de nosotros hemos utilizado el Wifi de un aeropuerto donde se nos indica que tenemos "30 minutos gratis de internet", pero pocos hemos analizado lo que sucede bajo el lente del poder. Lo primero que ocurre es que aceptamos develar nuestra identidad, y, por la premura del tiempo, asumir un ritmo acelerado. Subsecuentemente, nos vemos forzados a ver contenidos que no esperamos o no deseamos (por ejemplo, propagandas), porque es una exigencia para completar el proceso de conexión. Y, finalmente, una vez logrado el acceso, debemos ajustar lo que podemos hacer al sistema de filtro de la red. Así, sucede que muchas veces terminamos llenos de *e-mail* promocionales, pese a no haber podido lograr nuestro cometido durante esos valiosos 30 minutos.

En el poder funcional, el flujo de influencia y el nivel de conciencia se comportan de manera similar a como sucede en el poder comportamental. Así, el nivel de afectación o de influencia puede ir desde un individuo en particular hasta toda una comunidad; el tamaño dependerá del nivel de control que un actor tenga sobre la infraestructura y la configuración del ciberespacio. De igual forma, es muy raro que un usuario final tenga completo conocimiento de las medidas tomadas por un Estado o PSI, y de la manera como estas influyen en sus interacciones interciberespaciales.

Ahora bien, el poder funcional, a diferencia del comportamental, es más susceptible a la intervención de actores exógenos que no hacen parte del flujo como *actor regulador* que se ilustró en la figura 3. Por ejemplo, un *hacker* o un Estado pueden fácilmente vulnerar la accesibilidad, los componentes físicos y digitales y el contenido del ciberespacio en otro territorio, y así afectar directamente las interacciones interciberespaciales; sin embargo, raro sería que estos pudiesen influenciar el sistema de valores, y en consecuencia, tácitamente, el comportamiento de los usuarios finales.

La resistencia del poder funcional dependerá de si el *actor regulador* hace parte del flujo descrito, como se ve en la figura 3, o de si, por el contrario, es un tercero exógeno a la relación de influencia. En el primer caso, en la relación usuario-intermediario, el poder se agota cuando el usuario decide encontrar otra fuente de conexión, y el intermediario, no prestar el servicio; sin embargo, hacer lo mismo respecto a un PSI es más difícil y tomará más tiempo, pues en ello intervienen variables como la oferta existente, las políticas de la compañía y los recursos financieros del usuario para cambiar el servicio. Finalmente, si el Estado es el que está condicionando al ciberespacio, superar su influencia es, para alguien sin conocimiento técnico avanzado, algo imposible.

Cuando la fuente del poder funcional es un actor exógeno, la resistencia a la influencia se transfiere al dominio de la ciberseguridad o ciberdefensa. En tales casos, el objetivo es evitar, por los medios y las técnicas necesarios, que ese actor controle los términos de conexión y de contenido disponible. En este campo es posible hablar de la triada de la seguridad de la información (i.e. disponibilidad, confidencialidad e integridad), al igual que de conceptos relacionados con el servicio (i.e. accesibilidad, redundancia, resiliencia, entre otros).

En términos de la concepción básica del "poder"-relación de "A" y "B", el poder funcional se traduce de la siguiente manera: un actor regulador ("A") puede lograr que otro actor regulador de menor jerarquía, o usuario final ("B"), tenga o no acceso al ciberespacio, o visualice cierta información. En tal sentido, el actor "A" configura el tipo del ciberespacio al que "B" puede acceder, así como las formas y los modos para hacerlo. Para ello, "A" depende del control que pueda ejercer sobre la infraestructura tecnológica y física del entorno intangible, así como de los argumentos que le permitan crear los sistemas de valores. El poder funcional de "A" sobre "B" termina influyendo en las interacciones de "B", en el sentido de que determina cuándo pueden realizarse, así como las respuestas recíprocas de terceros a sus estímulos.

Lecciones

- La aparición de *actores reguladores* desvirtúa la concepción del ciberespacio como un lugar donde reina la anarquía. A decir verdad, existen múltiples sistemas de valores jerarquizados que coexisten, y constituyen así un intrincado conjunto de criterios que influencian directamente la manera como los usuarios realizan interacciones interciberespaciales, al igual que las respuestas recíprocas y los estímulos llevados a cabo.
- El poder comportamental constituye la manera como los actores reguladores proyectan sus sistemas de valores en el ciberespacio, en un fenómeno que se comporta como un flujo descendente. El sistema de valores delimita qué, cómo y dónde los actores reguladores, según la jerarquía y los usuarios, pueden "*HACER*" en el ciberespacio.
- Los actores reguladores identificados para el poder comportamental son, en orden descendente: 1) el Estado, centro del sistema social moderno; 2) las plataformas/sistemas, proveedores de los escenarios cibernéticos delimitados donde ocurren las interacciones; 3) los escenarios

cibernéticos delimitados, o servicios cibernéticos que permiten la interacción, y que contienen más de una comunidad virtual; 4) la comunidad virtual, o asociación de usuarios, con o sin identidad diluida, que conviven e interactúan por o para un fin común en particular.

- El poder funcional es la habilidad de un actor para dictar los términos de conectividad al ciberespacio, así como el acceso a información; incluso, si es en detrimento de otros. Este determina, entonces, cuándo los usuarios pueden *usar* el ciberespacio y, por ende, interrelacionarse. Así mismo, influencian lo que estos pueden **encontrar** en el dominio intangible, de modo que fungen como una especie de modelador.
- Al igual que como ocurre con el poder comportamental, el funcional también tiene una serie de *actores reguladores* que se comportan jerárquicamente. Estos son, en orden descendente: 1) El Estado, centro del sistema social moderno, y quien controla los derechos de conexión en un territorio determinado; 2) los PSI, encargados de la distribución del servicio de internet desde el *backbone* hasta el usuario final, y 3) el intermediario, o prestador de servicio a internet temporal para el usuario final.
- El poder funcional y el poder comportamental existen entre todos los tipos de actores mencionados en capítulos anteriores. La forma como se manifiestan puede ser distinta, pero se hallan igualmente presentes entre la legalidad y la ilegalidad.
- En ambos tipos de poder, el comportamental y el funcional, el nivel de influencia será más fuerte cuanto más cerca del Estado se halle la fuente. De igual forma, y de manera inversa, el nivel de conciencia decrecerá mientras más lejos se halle la fuente del usuario final. Cuando el nivel de conciencia es alto, es posible hablar de un poder comportamental o funcional de naturaleza directa, y cuando la relación se invierte, se está ante un carácter tácito.
- El cumplimiento de la influencia que emana de ambos tipos de poder viene acompañado de mecanismos de autoridad y de castigo. Estos serán tanto más drásticos —entendido ello como capaces de afectar la integridad física o jurídica de un actor regulador o usuario final— cuanto más alto sea el nivel de influencia.
- Existen diferencias fundamentales entre los poderes comportamentales y los funcionales. En primer lugar, el funcional es más susceptible de sufrir injerencias de terceros actores exógenos a la relación de poder

visualizada en el flujo. Cuando ello ocurre, estamos ante un incidente de ciberseguridad o ciberdefensa. Y en segundo lugar, la desterritorialización y la dilución de la identidad pueden servir para superar la influencia del Estado en cuanto a lo comportamental, pero no en cuanto a lo funcional. No todos los actores tienen los medios ni los conocimientos para controlar su conexión sin estar sujetos a la jurisdicción territorial de un Estado, lo cual es mucho más complejo para quienes se mueven entre la ilegalidad.

Referencias

Ackerman, S. (2015). US Central Command Twitter account hacked to read 'I love you Isis'. *The Guardian*.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. I*nternational Journal of Drug Policy, 35*, 7-15. https://doi.org/10.1016/j.drugpo.2016.04.020

Assaf, A., & Moshnikov, D. (2020). Contesting sovereignty in cyberspace. *Int. Cybersecur. Law Review. 1*, 115-124.

Associated Press, & AFP. (2015). *Bar manager gets more than TWO YEARS hard labour in Myanmar for putting headphones on Buddha in online drinks ad*. https://tinyurl.com/bde9ew88

Ayers, C. E. (2016). *Rethinking sovereignty in the context of cyberspace*. Center for Strategic Leadership, United States Army War College. https://www.hsdl.org/?view&did=802916

Bachrach, P., & Baratz, M. S. (1962). Two faces of power. *The American Political Science Review, 56*(4), 947-952.

Bakken, D. E., Rarameswaran, R., Blough, D. M., Franz, A. A., & Palmer, T. J. (2004). Data obfuscation: anonymity and desensitization of usable data sets. *IEEE Security and Privacy, 2*(6), 34-41.

Balcells, L. (2011). Continuation of politics by two means: Direct and indirect violence in civil war. *The Journal of Conflict Resolution, 55*(3), 397-422. http://www.jstor.org/stable/23049892

Barlow, J. P. (2009). Declaración de independencia del ciberespacio (1996). *Periférica Internacional. Revista Para el Análisis de la Cultura y el Territorio, 1*(10), 241-242.

Beevor, A. (2009). *D-Day: The battle for Normandy*. Viking.

BBC News. (2017). Two Britons arrested in Thailand over football streaming. https://www.bbc.com/news/technology-39947622.

Bergman, M. (2001). *The Deep Web: Surfacing hidden value*. Bright Planet: Deep Content.

Blocked on Weibo. (s.f.). https://blockedonweibo.tumblr.com/tagged/list.

Bonaparte, N. (2018). *Napoleon the art of war & power: Slip-cased edition*. Arcturus Publishing Ltd. (Obra original sin fecha conocida).

Brainard, L. A. (2010) Cyber-communities. En H. K. Anheier, S. Toepler (Eds.), *International Encyclopedia of Civil Society*. Springer. https://doi.org/10.1007/978-0-387-93996-4_43

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law and Criminology (1973), 97*(2), 379-475.

Brock, J. L. (2000). *Critical infrastructure protection "ILOVEYOU": Computer Virus Highlights Need for Improved Alert and Coordination Capabilities (GAO/T-AIMD-00-181*. United States General Accounting Office.

Bronk, C., Monk, C., & Villaseñor, J. (2012). The dark side of cyber finance survival. *Journal Survival Global Politics and Strategy 54*(2), 129-142. doi:10.1080/00396338.2012.672794

Burgess, M. (2016). *Chinese hacker jailed after stealing 'cutting-edge' military secrets*. https://www.wired.co.uk/article/chinese-hack-us-military-su-bin

Buzan, B. (1983). *People, states, and fear: The national security problem in international relations*. Wheatsheaf Books Ltd.

Clemente, D. (2011). International security: Cyber security as a wicked problem. *The World Today, 67*(10), 15-17.

Command, U. A. T. a. D. (2005). *Cyber operations and cyber terrorism*. Handbook No. 1.02. Leavenworth, KS.

Corbin, C. (2017). Pro-ISIS hackers release 'kill list' with 8,786 targets in US and UK. *Fox News*.

Dahl, R. A. (1957). The concept of power. *Behavioral Science, 2*(3), 201-215. doi:10.1002/bs.3830020303

Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2017). Battlefield cyberspace: Exploitation of hyperconnectivity and internet of things. En M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.), *Developing next-generation countermeasures for homeland security threat prevention* (pp. 204-235). IGI Global. http://doi:10.4018/978-1-5225-0703-1.ch010

Dittus, M., Wright, J., & Graham, M. (2018). Platform criminalism: The 'Last-Mile' geography of the darknet market supply chain. Paper presented at the *Proceedings of the 2018 World Wide Web Conference*. Lyon, France.

Douhet, G. (2013). *Command of the air*. Books Express Publishing. (Obra original publicada en fecha desconocida).

Dowding, K. (2006). Three-dimensional power: A discussion of Steven Lukes' power: A Radical View. *Political Studies Review, 4*.

Economy, E. (2018). The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*.

El Tiempo. (2008). Informe de Interpol sobre computador de 'Raúl Reyes' calentó la cumbre de Lima. https://tinyurl.com/ynsnkhk2

Facebook. (2015). *Declaración de derechos y responsabilidades* [video]. https://tinyurl.com/2p95jzc2

Facebook. (s.f.). *Principios de Facebook*. https://www.facebook.com/principles.php.

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32. Stuxnet Dossier*. Symantec Security Response.

Fuerzas Militares de Colombia. (1997). *Manual de estrategia*. Bogotá.

Foch, M. (2007). *The principles of war*. Kessinger Publishing, LLC. (Obra original publicada en 1903).

Follath, E., & Stark, H. (2009). *The story of 'Operation Orchard': How Israel destroyed Syria's Al Kibar nuclear reactor*. https://tinyurl.com/35axjzkh

Foucault, M. (1982). The subject and power. *Critical Inquiry, 8*(4), 777-795.

Fox, N., & Roberts, C. (1999). Gps in Cyberspace: The Sociology of a 'Virtual Community.' *The Sociological Review, 47*(4), 643–671. https://doi.org/10.1111/1467-954X.00190

Fuller, J. (1926). *The foundations of the science of war*. Hutchinson & CO.

Gady, F.-S. (2015). *New Snowden documents reveal Chinese behind F-35 Hack*. https://tinyurl.com/mpp2k4sk

Galaxy 3. (s.f.). *Terms*. http://galaxy3m2mn5iqtn.onion/terms

Gaventa, J. (1980). *Power and powerlessness*. University of Illinois Press.

Gilman, N., Goldhammer, J., & Weber, S. (2013). Deviant globalization. En M. Miklaucic & J. Brewer (Eds.), *Convergence: Illicit networks and national security in the age of globalization* (pp. 3-15). National Defense University Press.

Golinger, E. (2011). La guerra cibernética. En N. D. Ferreyra, *Periodistas sin miedo 1* (pp. 89-94). https://tinyurl.com/yw23mstn

Google. (2017). *Condiciones de servicio de Google*. https://policies.google.com/terms?hl=es.

Handel, M. (1991). *Sun Tzu and Clausewitz: The art of war and on war compared*. Strategic Studies Institute U.S. Army War College.

Hanzhang, T. (2000). *Sun Tzu art of war: The modern Chinese interpretation*. Sterling Publishing Co., Inc.

Heinrich, M. (2009). *IAEA finds graphite, further uranium at Syria site*. https://tinyurl.com/47hx8br4

Hua, J., & Bapna, S. (2015). Industrial cyber espionage. *Journal of Management Systems, 25*(3), 67-18.

Huffingtonpost. (2011). Operation Delego: Dreamboard child sex ring bust nets 72 arrests in U.S., Canada, France, Germany. *The Huffingtonpost Canada*.

Jomini, A.-H. (2008). *The art of war*. Wilder Publications. (Obra original publicada en fecha desconocida).

Lee, J. (2013). Cyber kleptomaniacs: Why China steals our secrets. *World Affairs, 176*(3), 73-79.

Lendvay, R. L. (2016). *Shadows of stuxnet: Recommendations for U.S. Policy on critical infrastructure cyber defense derived from the stuxnet attack*. Naval Postgraduate School.

Lewis, J. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic and International Studies.

Liaropoulos, A. (2013). Exercising state sovereignty in cyberspace: An international cyber-order under construction? *Journal of Information Warfare, 12*(2), 19-26.

Lolifox. (s.f.). *Rules*. http://lisach7joohmqk3a.onion/.

Lukes, S. (2005). *Power: A radical view* (2nd Edition). Palgrave MacMillan.

Mager-Hois, E. A. (2010). Ideología y poder. *Revista Multidisciplina, 5*(1), 46-60.

Mahan, A. (2018). *The influence of sea power upon history, 1660-1783* (Classic Reprint). Forgotten Books. (Obra original publicada en fecha desconocida).

Mann, E., & Endersby, G. (2002). *Thinking effects effects-based methodology for joint operations. Cadre paper n.°15: College of Aerospace Doctrine, Research and Education*. Air University

Maurer, T., & Morgus, R. (2014). *Compilation of existing cybersecurity and information security related definitions*. https://tinyurl.com/3seuwwyf

Mcdonald, T., & Mills, R. (2010). *An application of deception in cyberspace: Operating system obfuscation*. Paper presented at the International Conference on Information Warfare and Security At: Dayton OH

Miyamoto, M. ([2014], s.f.). *El libro de los cinco anillos*. Santiago de Chile: EDAF. (Obra original publicada en fecha desconocida)

Moscaritolo, A. (2010). *Analysts pick apart "huge" Mariposa botnet*. Itnews.com.au.

Mueller, P., & Yadegari, B. (2012). *The stuxnet worm*. University of Arizona.

National Cybersecurity and Communications Integration Center (NCCIC). (2014). *Combating the insider threat*. Department of Homeland Security.

NortonLifeLock. (2017). *What is the difference between black, white and grey hat hackers?* Norton. https://tinyurl.com/bdd59mkv

NSPCC. (s.f.). *Grooming: What it is, signs and how to protect children*. https://tinyurl.com/32x7npma

Ogun, M. N. (2015). *Terrorist use of cyberspace and cyber terrorism: New challenges and responses* (Vol.42). Delft University Press.

Panda Security. (2013). *Los virus más famosos de la historia: ILoveYou*. https://tinyurl.com/yc58mpph

Paquet-Clouston, M., Décary-Hétu, D., & Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy, 54*, 87-98. https://doi.org/10.1016/j.drugpo.2018.01.003

Parks, R., & Duggan, D. (2011). Principles of cyberwarfare. *IEEE Security and Privacy Magazine, 9*(5), 30-35.

Pricewaterhouse Coopers. (2018). *The scale and impact of industrial espionage and theft of trade secrets through cyber*. European Comission. https://tinyurl.com/yc4c3kwv

Pérez, B., Musolesi, M., & Stringhini, G. (2018), *You are your metadata: Identification and obfuscation of social media users using metadata information*. Paper presented at the Twelfth International AAAI Conference on Web and Social Media.

Price, M. E. (2002). *Media and sovereignty: The global information revolution and its challenge to state power*. The MIT Press.

Rabinovich, A. (2005). *The Yom Kippur war: The epic encounter that transformed the Middle East United States*. Schocken.

Revista Semana. (2008). "Los archivos de los computadores de 'Raúl Reyes' no han sido manipulados": Interpol. https://tinyurl.com/2uuxxsj2

Richard, L. C. (1984). *Conflict and violence in Singapore and Malaysia 1945-1983*. G. Brash.

Sadan, E. (1997). *Empowerment and community planning: Theory and practice of people-focused social solution*. Hakibbutz Hameuchad Publishers.

Schneider, F., & Williams, C. C. (2013). *The shadow economy*. Institute of Economic Affairs (IEA).

Sevnet. (s.f.). *Terms of service*. http://servnetshsztndci.onion/terms-of-service.

Shamsi, A., Zeadally, S., Sheikh1.F, & Flowers, A. (2016). Attribution in cyberspace: techniques and legal implications. *Security Comm. Networks*, 9:2886-2900. doi: 10.1002/sec.1485

Shimomura, T. (1996). *Takedown: The pursuit and capture of Kevin Mitnick, America's Most wanted computer outlaw - By the man who did it*. Voice. First edition.

Singer, P. A. (2013). *Cybersecurity and cyberwar: what everyone need to know*. Oxford University Press.

Siyuan, C., & Chen-Wei, C. (2019). *Singapore's latest efforts at regulating online hate Speech: a perspective from international law and international practices*. Research Collection School of Law, Singapore Management University. https://ink.library.smu.edu.sg/sol_research/2921

Soghoian, C. (2012). Surveillance and security lessons from the petraeus scandal. *ACLU. ORG*. https://tinyurl.com/257tm5tr

Springer, P. (2015). *Cyber warfare: A reference handbook*. ABC-CLIO, LLC.

Strenski, I. (1998). Religion, power, and final Foucault. J*ournal of the American Academy of Religion, 66*(2), 345-367.

Sun Tzu. (1963). *The art of war*, S. B. Griffith (Ed.). Oxford University Press. (Obra original publicada en fecha desconocida).

The Independent (2014). Why Filipinos have become the punching bag. https://tinyurl.com/2p84uwc2

The Statutes of the Republic of Singapore. (2013). *Sedition Act* (Chapter 275). https://sso.agc.gov.sg/Act/SA1948?ProvIds=pr1-#pr1-

UK Ministry of Defense. (2014). *Joint doctrine publication 0-01 (JDP 0-01)*. (5 ed.). Forms and Publications Section.

US Army. (1984). *The soviet army: Operations and tactics (FM 100-2-1)*. Headquarters. Department of the Army.

US Army. (1993). *U.S. army field manual: Operations (FM 100-5)*. Headquarters Department of the Army.

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy, 25*(2), 183-189. https://doi.org/10.1016/j.drugpo.2013.10.009

Von Clausewitz, C. (2007). *On war*. M. Howard, P. Paret, & B. Heuser (Eds.). Oxford University Press. (Obra original publicada en fecha desconocida).

Wallimann, I., Tatsis, N. C., & Zito, G. V. (1977). On Max Weber's definition of power. *The Australian and New Zealand Journal of Sociology, 13*(3), 231-235. doi:10.1177/144078337701300308

Walzer, M. (1983). *Spheres of justice: A defense of pluralism & equity*. Basil Blackwell.

Winter, P. (2012). *The great firewall of China: How it blocks tor and why it is hard to pinpoint*. USENIX - The Advanced Computing Systems Association.

Wolfsfeld, G., Segev, E., & Sheafer, T. (2012). Social media and the Arab Spring: Politics Comes First. *The International Journal of Press/Politics, 18*(2), 115-137.

Wray-Lake, L., Christens, B. D., & Flanagan, C. A. (2014). Community values. En A. C. Michalos (Ed.), Encyclopedia of Quality of Life and Well-Being Research. Springer. https://doi.org/10.1007/978-94-007-0753-5_482

Yagoda, B. (2014). A short history of "Hack". *The Newyorker*. https://tinyurl.com/4ktnhcb5

YouTube. (s. f.). *Términos del servicio*. https://tinyurl.com/28rt8ykv

Yuan, G. (2013). *Las 36 estratagemas chinas. La sabiduría de Oriente para Occidente*. EDAF.

Zedong, M. (2007 [1937]). *On guerrilla warfare*. S. B. Griffith (Ed.). BN Publishing.