Los desafíos a la soberanía de los Estados nación en tiempos de internet
Challenges to Nation States Sovereignty in the Age of Internet

Autor: Lic. Dianet Doimeadios Guerrero[1]
Noviembre de 2020.

Resumen: La expansión de internet durante las últimas décadas, hasta ser imprescindible en la vida personal, política, social y económica de la humanidad, ha planteado desafíos en términos de soberanía y jurisprudencia a los Estados nación, en un mundo interconectado y de interdependencias financieras y económicas, con actores múltiples (Estados, corporaciones multinacionales, imperios mediáticos, grupos de poder y estructuras supranacionales) y problemas cada vez más globalizados en términos de cambio climático, seguridad nacional, instituciones multilaterales en tensión y flujos de información asimétricos. El espacio virtual que es internet, visto como libre, "prepolítico", democrático y ajeno a toda regulación, es contrariamente vehículo de control para intereses que se sirven de la ausencia de un marco jurídico coherente, sistémico y universal, y amenazan la libertad individual y la soberanía de los Estados nación.

Palabras clave: Internet, soberanía, Estado, ley, derecho internacional, redes sociales, campañas políticas, datos, democracia, comunicación, información, era digital, comunicación política, ciberespacio, regulación, poder, seguridad

Abstract: *The Internet has along the past decades grown essential in personal and social, political and economic life of mankind. The growing impact of the cyberspace and ICTs has increasingly challenged nation states in terms of sovereignty and law-making, in an interconnected world with countries more and more economically and financially interdependent, multiple actors operating on cyberspace (States, multinational corporations, media empires, power groups and supranational structures) and where problems related to the climate change, national security, a multilateral system under stress and asymmetric information flows are globalized. The Internet, seen as a pre-political, democratic and non-regulated space, is being*

[1] Maestrante del Instituto Superior de Relaciones Internacionales "Raúl Roa García".

used by political and economic powers to manipulate trends and control citizens amidst the lack of a clear and binding legal framework, thus threatening both individual freedoms and the sovereignty of nation states.

Keywords: *Internet, sovereignty, nation estate, law, international law, social network, political campaign, data, democracy, communication, information, digital era, political communication, cyberspace, regulation, power, security*

–Si toda la información que damos a Google nos la hubiera pedido algún Gobierno, ya habría sido denunciado ante todos los tribunales internacionales.
Y, sin embargo, se la cedemos graciosamente a Amazon, Twitter, Google, Facebook y sus adláteres.
–¿Y ellos la convierten en billones?
–¡Y en PODER!
Evgeny Morozov (2013)

INTRODUCCIÓN

El siglo XX nos legó internet. Pareciera que su advenimiento e incesante evolución pretende tornar la geografía planetaria en un espacio sin fronteras, aunque los viejos mapas digan otra cosa. La red, sistema nervioso central de la comunicación y la información, la investigación, la economía y la política actuales, extiende los límites de los Estados nación y les plantea no pocos desafíos a la hora de ejercer su soberanía en una era globalizada en la que actúan en el ciberespacio –terreno de competencia y de crecientes conflictos– no solo Estados sino también corporaciones multinacionales, grupos de poder con agendas políticas y económicas, poderes supranacionales y ciudadanos, actores estatales y no estatales.

Internet es el corazón de un sistema supranacional, el ciberespacio, donde se generan situaciones y conflictos que tradicionalmente estaban bajo la órbita de acción del Estado y ahora dependen de números IP, nombres de dominios, cables transatlánticos, fincas de servidores, *big data*, conexiones satelitales y una retórica de la neutralidad que nos vende un sueño: andamos por la ruta del progreso.

Sin barreras divisorias ni reglas –una visión que han implantado los poderes que dominan las redes, que las muestran como un espacio democrático y plenamente horizontal, con las mismas oportunidades y *fair play* por igual para todos–, esta concepción, muy acorde con las ideas

neoliberales, minimiza el papel de los Estados nacionales en la regulación de los asuntos globales, desprecia su capacidad para tener máxima autoridad sobre su territorio y población y, sobre todo, para ser independientes en las relaciones exteriores.

Al promediar la segunda década del siglo XXI, los Estados fomentan el despliegue de internet, pero no van a la par en términos de su regulación. En teoría, la estructura legal no se adapta a la celeridad de los cambios tecnológicos.

La tecnología y servicios que sustentan en gran parte la evolución de la llamada sociedad de la información son prácticamente ajenos a los propios Estados, y usualmente residen en las decisiones de actores internacionales trasnacionales que redefinen los conceptos usualmente aceptados de libertad, control y ejercicio de la soberanía.

Es posible afirmar que el grueso de la literatura que se ha ocupado del tema de la explotación del ciberespacio asegura que la internet constituye una amenaza para el concepto mismo de soberanía considerada, en palabras de Walter Wriston, como “el poder de una nación para impedir que otros interfieran en sus asuntos internos” (Aoki, 1998).

Otra postura al respecto, en palabras de Henry Perritt (2004), establece que internet tiene la capacidad para fortalecer el ejercicio del gobierno a escala nacional y global, consolidando así la soberanía en lugar de destruirla. No existe una única línea de pensamiento.

Desde diferentes perspectivas y en muchos aspectos, puede inferirse que el concepto de soberanía está siendo vulnerado. Reflexionemos entonces, en un marco crítico y analítico, sobre este atributo del Estado, con el objetivo de desarrollar distintos puntos sobre la problemática de la soberanía en internet.

DESARROLLO/ La soberanía frente a las asimetrías y la desregulación en el ciberespacio

Soberanía no es un concepto unívoco, sus múltiples acepciones dependen del objeto de análisis. Etimológicamente, la palabra proviene del Latín (*super* y *omnia*, poder que está sobre todo, y que no admite superior a él).

Desde Aristóteles o Santo Tomás de Aquino hasta los teóricos contemporáneos, las definiciones de Estado y de soberanía han evolucionado como categoría filosófica y de la teoría política. Norberto Bobbio (1994) resume que el concepto político-jurídico del término “sirve para indicar el poder de mando en última instancia en una sociedad política y, por consiguiente, para diferenciar a esta de otras asociaciones humanas, en cuya organización no existe tal poder

supremo, exclusivo y no derivado". Así, la idea de poder supremo define a la soberanía y su presencia es inherente a la aparición del Estado.

El profesor e investigador cubano Leyde E. Rodríguez Hernández (2017) define el Estado como la "organización política de una comunidad humana sobre un territorio determinado que, por tanto, posee población y territorio. Desde el siglo XVII, el atributo jurídico político de la soberanía". Y a esta última la designa como la "máxima autoridad sobre la población y el territorio, y la independencia en las relaciones exteriores", un concepto que servirá de eje para este análisis.

Atributos de la soberanía

Para el Estado, el ejercicio de su soberanía está asociado con el uso del poder sobre su base territorial y poblacional, y con el equilibrio y balance de ese poder en su interacción con otros Estados, atributos constitutivos de la noción de Estado nación surgido en Westfalia. En síntesis, tradicionalmente se consideran atributos esenciales de la soberanía del Estado el territorio, la población y la independencia en su política exterior.

Internacionalmente, un Estado será soberano en tanto ejerza su capacidad decisional en el contexto de un marco jurídico de coordinación (derecho internacional público), y mantenga derechos básicos del atributo de la soberanía como el *ius legationen* y el *ius tratatum* (Arbuet, 2016). Frente al derecho internacional público, los Estados son nominalmente soberanos e iguales, aunque no pueden ejercer este atributo si carecen de poder real para lograrlo. Entre otras variables, el dinámico desarrollo de las nuevas tecnologías ha influido en esta capacidad de los Estados y acentuado el desfase entre la teoría y la práctica.

Con el fin del esquema bipolar de los años noventa se inaugura un nuevo orden internacional que, a merced de la revolución tecnológica, aún no ha logrado definirse. A pesar de ello, existe una fuerte tendencia a conceptualizarlo como el "sistema de la comunicación", debido a la asociación de sus transformaciones con la dinámica de los cambios tecnológicos. La complejidad de este sistema se profundiza con la incursión de nuevos actores internacionales, que hacen tambalear el tradicional rol del Estado como actor de primer orden.

Esta etapa se caracteriza no solo por la envergadura de los cambios políticos, sino también por los tecnológicos y la forma en que países occidentales, en primera línea Estados Unidos –mediante el uso hegemónico de la tecnología, las redes sociales y el ejercicio del poder blando–, crearon y crean situaciones ficticias de descontento popular aupados por la Agencia Central

de Inteligencia (CIA) y otros organismos de inteligencia y seguridad. Acciones que se enraizaron en nuestras sociedades provocando cambios en toda su estructura, desde el desarrollo de movimientos revolucionarios, las llamadas “revoluciones de colores” y la Primavera árabe, hasta la caída de gobernantes, como consecuencia de los llamados *Panamá Papers* o las *fake news*, cortinas de humo de la injerencia mediática más organizada.

¿Quién detenta el poder en el ciberespacio?

Internet surge originariamente como una red subsidiada por fondos del Gobierno estadounidense para proporcionarse un sistema fiable de mantenimiento e intercambio de información frente a un posible atentado nuclear, post-Segunda Guerra Mundial.

Visto desde este supuesto fáctico, no cabría duda alguna ante la afirmación del carácter público de internet, entendiendo como “público” la esfera de la actividad estatal. Sin embargo, la teoría libertaria o liberal de internet sostiene que es privada y “prepolítica”, y que desde esta red se fortalece el sentido liberal de las relaciones interpersonales. De esta forma, se nos plantea la interrogante acerca de quién tiene la última palabra frente a cualquier conflicto que pueda suscitarse entre cibernautas.

Al cierre de 2017, de las 10 marcas más valorizadas del mercado, ocho tenían que ver con internet y las nuevas tecnologías, todas estadounidenses. De las 10 compañías que controlan la red, por el número de usuarios que registran, seis son de Estados Unidos, con más de 3 200 millones de ciudadanos conectados; las otras cuatro, chinas. En el mapa que evidencia el dominio del ciberespacio por las empresas de internet, Google y Facebook ocupan el continente americano, la Antártida, Europa, Medio Oriente, África Norte, el sudeste asiático y Oceanía; solo se libra Rusia porque la multinacional Yandex opera el motor de búsqueda de ese país, con una cuota del 65%, como también lo hace Baidu en China (Hannes Grassegger y Krogerus, 2017).

La topografía de la red es reflejo del escenario geopolítico actual, en el que existe un actor hegemónico, Estados Unidos, contendiente con dos potencias emergentes, China y Rusia, las cuales han desarrollado una tecnología propia en defensa de su soberanía en el ciberespacio, pero que solo compite con la estadounidense en su propio territorio.

Los “dueños de las redes” están trayendo una nueva e intensa concentración comunicativa y cultural mucho más global que la de las industrias culturales transnacionales o nacionales. En la actualidad hay pocas instituciones públicas en un nivel nacional o global que puedan enfrentar

estas cuestiones. No existe Estado nación que pueda remodelar esa red por sí solo, aun cuando ejecute normativas locales de protección antimonopólicas e impecables políticas de sostenibilidad en el orden social, ecológico, económico y tecnológico. Todavía menos puede construir una alternativa viable estando desconectado de la llamada "sociedad informacional", cuya sombra –intangible, pero no por ello menos real– alcanza incluso a quienes están fuera de internet.

Según datos de la Unión Internacional de Telecomunicaciones (2018), América Latina es la región más dependiente de los Estados Unidos en términos de tráfico de internet. Más del 90% de la información electrónica de la región pasa por algún nodo administrado directa o indirectamente por EE.UU., fundamentalmente por el llamado "NAP de las Américas", en Miami, y se calcula que entre 80 y 70% de los datos que intercambian internamente los países latinoamericanos también van a ciudades estadounidenses, donde se ubican 10 de los 13 servidores raíces que conforman el código maestro de la internet.

¿Se puede hablar de soberanía y sostenibilidad si la mayoría de las comunicaciones, en vez de acercar a nuestros países, los alejan? ¿Qué autoridad o autonomía tenemos si nuestras comunicaciones pasan por el escrutinio de los puntos de control y espionaje en Estados Unidos, a los que incluso pagamos ciberpeaje por ello? ¿Hay independencia cuando las estrategias de un país al final acatan la voluntad de las empresas de internet, que básicamente venden al mejor postor nuestros contenidos, con un considerable derroche de recursos y energía?

Evidentemente, el concepto tradicional de soberanía está siendo retado y vulnerado, porque la autoridad es ejercida en internet desde un solo polo, que justifica su postura de usurpación con el principio de la "neutralidad en la red", defendido y detractado por las grandes corporaciones, concepto construido a la medida de los intereses de quienes lo generan. Cabe preguntarse en qué contribuye este principio, que dista mucho del verdadero significado de neutralidad, con la democratización de su uso.

Ejes de la soberanía: internet y territorio

Inicialmente, el ciberespacio era considerado por algunos como un ámbito totalmente separado del mundo físico, sin fronteras ni reglas. Esta concepción, muy acorde con las ideas neoliberales que minimizan el papel de los Estados nacionales en la regulación de los asuntos globales, fue denominada ciberlibertarianismo, y se fundamenta en "una colección de ideas que enlaza al extático entusiasmo por las formas de vida mediadas por la electrónica con ideas libertarias

radicales, de extrema derecha, respecto de las propias definiciones de la libertad, la vida social, la economía y la política en los años venideros" (Winner, 2000).

Sin embargo, con el paso del tiempo se impuso el hecho real de que la infraestructura de comunicaciones y computación está ubicada en el mundo físico y sujeta a la jurisdicción territorial de los Estados (Lambach, 2018). De ahí que, al ser quebrantada la legalidad en la red, las leyes sean aplicadas sobre el territorio de un Estado.

La aplicación de la ley en internet ha sido uno de los temas que más ha atraído la atención de los juristas en lo que va del siglo XXI. La tradicional aplicación de las leyes ligadas a un territorio delimitado por fronteras claras, se ve amenazada por la estructura transfronteriza de internet. Los problemas de la aplicación territorial de leyes deben ser atendidos por soluciones pensadas para otra realidad, representando desafíos constantes para el intérprete y aplicador el derecho. Ley aplicable y jurisdicción competente son dos cuestiones a atender en cada caso que se presenta.

Un ejemplo práctico: aunque la Constitución de la República de Cuba (2019) establece en el inciso m) del Capítulo II *Relaciones Internacionales*, del Título I *Fundamentos Políticos* de la nueva Constitución de la República, que:

> m) ratifica su compromiso en la construcción de una sociedad de la información y el conocimiento centrada en la persona, integradora y orientada al desarrollo sostenible, en la que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento en la mejora de su calidad de vida; y defiende la cooperación de todos los Estados y la democratización del ciberespacio, así como condena su uso y el del espectro radioeléctrico con fines contrarios a lo anterior, incluidas la subversión y la desestabilización de naciones soberanas;

Y aunque el país llegara a promulgar una ley que reglamentara las normas sobre la publicidad política o sobre la no realización de actos de propaganda proselitista en los medios de difusión escrita, radial o televisiva, ¿podría realmente regular la publicidad nociva a través de internet?

Internet es un canal de información más, a través del cual se amplía el alcance de los medios de difusión, por lo que *a priori* parecería estar incluido en la prohibición. Sin embargo, resulta imposible ejercer actos de control por parte del Estado, dado que los medios o servidores donde se publica la propaganda proselitista pueden estar ubicados en cualquier lugar del mundo. Se podría rastrear desde qué IP se realizó la publicación, y comprobar si fue hecha desde Cuba, pero una vez que la propaganda está en línea es improbable que se pueda controlar la

duplicación del contenido en redes sociales y otros medios, especialmente cuando se utilizan CDN o P2P, que desacoplan la prestación del servicio con cierta IP. En este caso, ¿puede probarse que el Estado cubano pierde soberanía?

Para un Estado es improbable alcanzar un compromiso global de respeto a su norma interna, aun en el marco de Naciones Unidas, aunque de hecho podría iniciarse un camino a través del derecho internacional en pos de generar acuerdos con un alcance regional. Pero, ¿esto no significaría limitar el derecho de expresión de otros? Fácilmente, otro Estado podría llegar a argumentar un intento de violación del principio de no intervención en los asuntos internos, recogido en el Artículo 2, párrafo 7, de la Carta de las Naciones Unidas.

En el ciberespacio, ámbito artificial creado por medios informáticos, a diferencia de lo que ocurre en el territorio físico de un país, no hay aduanas; se “importa” contenido y se “exporta” de forma asimétrica, sin control. La comunidad de internet se ha pronunciado en contra de cualquier control o bloqueo por parte de los Estados, pronunciándose por la autorregulación.

No existen tratados internacionales que regulen el uso del ciberespacio, tal como los hay sobre otros ámbitos transfronterizos como el mar o el espacio exterior. Sin embargo, en el marco de las Naciones Unidas se han adoptado documentos que, aunque no son vinculantes, establecen algunos principios importantes.

Por ejemplo, en 2003, durante la Cumbre Mundial sobre la Sociedad de la Información, se acordó que “la autoridad de política en materia de política pública relacionada con internet es un derecho soberano de los Estados. Ellos tienen derechos y responsabilidades en las cuestiones de política pública internacional relacionadas con internet”.

Una década más tarde, en su informe de 2013, el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional expresó que:

> El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías.
>
> La soberanía de los Estados y las normas y principios internacionales que de ella emanan son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías que se halle en su territorio.

El alcance y la forma en que se ejerce esta soberanía constituyen una decisión política de cada Estado, que debe definir cómo aplicar las nociones territoriales de soberanía y de derecho internacional al ciberespacio con respecto a las actividades de personas y de objetos (Tsagourias, 2018).

En Latinoamérica, Bolivia ha sido pionero en la intención de regular dentro del derecho internacional privado, mediante un proyecto de ley en el que la víctima podría elegir el derecho que entienda más beneficioso para la reparación por daños resultantes de un ilícito informático, pudiendo optar por el derecho de su lugar de domicilio, el del lugar donde se producen los efectos del ilícito, o bien del lugar donde se generó el ilícito (Santos Belandro, 2013). En el caso de que Alicia viva en el país *A*, se comunique con Bernardo, que vive en el país *B*, y utilicen un servidor *S* que está físicamente en el país *C*, ¿cuál jurisdicción se aplicaría?

No hay una respuesta uniforme para todas las situaciones. En tanto, en un escenario de mayor complejidad, donde en lugar de un servidor se utiliza una tecnología de replicación geográfica a escala global, en la que no se conoce el lugar específico desde donde se provee el servicio, un servicio “en la nube”, ¿cuál es la jurisdicción de la nube?

En el mismo camino, aparece la idea de construcción de una *lex retialis* o ley de la red, como un derecho de carácter global-universal que acompañe el desarrollo de la sociedad de la información. Cabe preguntarse cuán dúctil debería ser este esquema regulatorio, para ser eficiente y acompase el dinamismo que caracteriza a las tecnologías que dan estructura a este nueva sociedad. En suma, con la *lex retialis* se intentaría dar al mismo tiempo una respuesta a la gestión de internet y un marco legal requeridos por la nueva sociedad.

Una de las principales funciones de un Estado, vinculada al ejercicio de la fuerza, es la de vigilancia. Sus límites están en el derecho de los ciudadanos y en la ley que impera en su territorio. Desde fines del siglo pasado, cuando se privatiza el uso de internet, este rol pasa a ser compartido con nuevos actores.

Para hacer frente a algunos de los problemas mencionados con respecto a la localización de la información a través de las redes transfronterizas, algunos Estados han manifestado la intención de colocar el contenido en servidores establecidos dentro de su territorio nacional. En agosto de 2015, Rusia aprobó su Ley de Localización de Datos, por la cual se exige que los datos de ciudadanos rusos –hayan sido estos recogidos a través de internet o no– se mantengan dentro del territorio de la Federación.

En la región latinoamericana, durante 2013 se discutió en Brasil la inclusión de un artículo dentro de su Marco Civil que obligaba a las compañías que manejaran datos personales de ciudadanos brasileños a mantener sus servidores y centros de datos dentro de sus fronteras. Finalmente, y quizás a raíz de las revelaciones de Edward Snowden en 2014, se aprobó la Ley 12965/14, Marco Civil da Internet. Su articulado sobre neutralidad, privacidad y libertad de expresión en línea convirtieron a Brasil en modelo en cuanto a legislación progresista para internet. Aunque su contenido fue muy debatido, en mayo de 2016 la presidenta Dilma Rousseff firmó el Decreto 8771 reglamentario de la Ley Marco Civil de Internet, que se refiere a la aplicación práctica de la ley.

En Uruguay, el Decreto 92 del 7 de abril de 2014 estableció las políticas de seguridad de la información para organismos del Estado uruguayo. En él se incluyeron normas referidas a las condiciones locativas de los centros de datos, así como a los nombres de dominio a utilizar por parte de los organismos. Aun así, el Gobierno usa cuentas de Twitter y hospeda su información utilizando servicios de Google.

En agosto pasado, Alemania puso en marcha la Agencia para la Innovación en Ciberseguridad, con un presupuesto de 350 millones de euros hasta 2030 y encargada de su seguridad informática para “la protección de sus ciudadanos, la administración y la economía en el ciberespacio”, que supone un “paso importante hacia la soberanía digital” del país, señalaron los ministerios de Defensa e Interior.

Este mismo verano fue presentado GAIA-X, una iniciativa público-privada liderada por Alemania y Francia con la que Europa busca unificar sus soluciones en la nube y mantener la soberanía de los datos de los países europeos. Se trata de asegurar un ecosistema o federación de nube propio para empresas y ciudadanos, bajo un marco normativo común que regulará la soberanía y disponibilidad de los datos, la interoperabilidad, la portabilidad, la transparencia y la participación justa.

Abundan ejemplos demostrativos de las dificultades a las que se enfrentan los Estados para hacer valer sus normas en el ciberespacio.

Un caso por antonomasia ocurrió recientemente, cuando un tribunal de la ciudad de París, Francia, se declaró competente en una demanda civil instaurada contra Facebook (Lidgett, 2016) por atentar contra la libertad de expresión. Más allá del análisis de fondo de la cuestión en litigio, relativa al derecho mencionado, a los efectos de este análisis resulta paradigmática la dificultad de establecer soluciones claras y unánimes a la hora de juzgar actos cometidos a

través de medios telemáticos. El demandante solicitó en Francia la reparación de los daños ocasionados tras haber visto suspendida su cuenta de la red social por haber publicado la obra *El origen del mundo*, de Courbet.

La defensa instaurada por la empresa norteamericana se basó en la falta de competencia del tribunal francés por existir una cláusula en los términos y condiciones de Facebook aceptados por el actor, en la cual se establece que cualquier cuestión litigiosa deberá resolverse ante la justicia del estado de California.

Algunos bloques de integración regionales también se han preocupado en alguna medida por avanzar en la construcción de soberanía tecnológica. Por ejemplo, lo ha hecho el Mercosur, impulsando el Grupo de Trabajo sobre Gobernanza, Privacidad y Seguridad de la Información e Infraestructura Tecnológica, mientras que Unasur ha emprendido el Anillo Óptico de Interconexión e Integración TIC.

Por su parte, varios Estados han elaborado estrategias para la defensa de su ciberespacio, las que incluyen el marco legal correspondiente.

Teniendo en cuenta que el ciberespacio se ha convertido en los últimos años en un ámbito de mucha importancia para el desarrollo económico, político y cultural, y que cada vez es usado con mayor frecuencia e intensidad para fines que atentan contra la seguridad del país, se debió aprovechar la actualización de la Constitución para establecer la soberanía del Estado cubano sobre el ciberespacio nacional. Porque la alternativa a que el Estado cubano ejerza su soberanía sobre el ciberespacio nacional sería permitir que otros Estados puedan ejercer hegemonía sobre el mismo.

Ese espacio virtual donde pululan las *fake news, bots y trolls*, los ciberataques, el ciberespionaje o manipulaciones masivas como la de Cambridge Analytica para la campaña de Donald Trump, difícilmente haya sido imaginado por John Perry Barlow, fundador de la Electronic Frontier Foundation (EFF), cuando en 1996 presentó en Davos su “Declaración de Independencia del Ciberespacio”, en la que criticaba las interferencias de los poderes políticos en el mundo de internet, defendía la idea de un ciberespacio soberano y afirmaba que “el espacio social global que estamos construyendo es independiente por naturaleza de las tiranías que estáis buscando imponernos. (…) Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros”.

Internet, usuarios reales y falsos y tendencias fabricadas

Cada día hay más casos de manipulaciones políticas y sociales sobre una población determinada utilizando internet como un terreno fértil para las campañas y la confrontación, en muchas ocasiones manipulando e influenciando la percepción de la realidad de los ciudadanos a través de contenidos personalizados.

Las plataformas tecnológicas se están convirtiendo en extractoras de nuestros datos, como lo demostró públicamente el escándalo de la compañía de *big data* Cambridge Analytica: el uso de datos personales, de más de 50 millones de perfiles de Facebook (sin consentimiento), para extraer patrones de comportamiento y personalidad, inundar a los usuarios con mensajes personalizados que influyeran en su intención de voto e incluso para delinear elementos de la estrategia de la campaña de Trump en 2016 a partir de modelos estadísticos con base en los datos personales extraídos de la red social, procesados por algoritmos y modelados estadísticamente.

A partir de algoritmos que han probado que con 100 *likes* de una persona en Facebook se puede predecir su orientación sexual, sus opiniones religiosas y políticas, su nivel de inteligencia y de felicidad; que con 250 *likes* se puede adivinar el resultado de un test de personalidad mejor que como lo haría la pareja del individuo, y que con unos pocos *likes* adicionales se puede saber más de una persona que ella misma, la compañía Cambridge Analytica –que antes intervino en la campaña Leave.EU para el Brexit en el Reino Unido– construyó un perfil psicométrico personal para cada adulto de EE.UU., a través de bases de datos comerciales y análisis de redes sociales. Esta herramienta le permitió a los expertos de la campaña de Donald Trump monitorear los datos de 220 millones de estadounidenses y ajustar los mensajes exactamente a los intereses y gustos particulares de cada individuo, proporcionando así el margen clave para la victoria del republicano (Hannes Grassegger y Krogerus, 2017).

En el otro lado del continente, Venezuela ha librado duras batallas de ciberguerra. La oposición venezolana, financiada desde los Estados Unidos, ha utilizado los medios digitales para difundir propaganda negra. La nación bolivariana es uno de los países con mayor penetración de internet en América Latina, con el 68% de usuarios conectados a la red y con móviles en el 94% de los hogares, según datos de la Comisión Nacional de Telecomunicaciones (Conatel).

Durante el primer semestre de 2017, cientos de páginas y grupos públicos y privados en Facebook, y millones de mensajes en Twitter, Instagram y WhatsApp divulgaron propaganda negra y llamados a la desobediencia civil. Los personajes de los videojuegos tomaron las calles para hacerse cargo de los daños colaterales de la guerra de cuarta generación. Dueños de

medios privados financiaron las principales campañas en internet y las empresas tecnológicas que las hicieron posible, en alianza con multimillonarios emigrados y fundaciones en EE.UU.

Varias investigaciones del sitio alternativo red58.org (2017) demostraron el uso de robots para generar estados emocionales adversos al Gobierno de Nicolás Maduro. Se contrataron *data brokers* para realizar *marketing* político, con un extraordinario nivel de efectividad. ¿Y cuál volvió a ser el sujeto de la manipulación?: la población venezolana.

Poco a poco, las grandes empresas están adquiriendo la posibilidad de entrar en terrenos a los que antes no tenían la posibilidad de acceder. Solo ellas están en capacidad de saber más de nosotros que nosotros mismos. Lo más preocupante es que tal situación revela lo fácil que está siendo convertir a las democracias liberales en dictaduras de la información dispuestas a encerrar a cada ciudadano en una burbuja observable, parametrado y previsible.

La política se ha convertido en tecnopolítica: en la Guerra del Golfo y en la de Irak –como en otras durante las últimas tres décadas– Estados Unidos empleó un cóctel propagandístico: desde panfletos y ondas de radio hasta sitios web, transmisiones televisivas desde aviones, campañas de prensa para influir tanto a los iraquíes como al público de los países occidentales y a la opinión mundial, montajes como el del rescate de la soldado Lynch, en una operación de propaganda elaborada por la firma de relaciones públicas Rendon Group. Ahora se emplean el *big data* y el *data mining*, el *microtargeting*, la minería o la compra de datos personales y su procesamiento algorítmico para influir en la ciudadanía; *bots* (cuentas falsas activas por programas que generan comportamientos y mensajes automáticos y preestablecidos) y *trolls* (usuarios con cuentas apócrifas) para propagar mensajes políticos o establecer y expandir tendencias de opinión específicas en redes sociales. Del análisis demográfico para definir tendencias, las campañas políticas están pasando a lo psicométrico y a la publicidad personalizada con la huella digital de las personas como materia prima. Y no importan las fronteras.

Se observa como tendencia que los partidos políticos son empresas que compiten en un mercado de votantes y que capitalizan en las urnas, de acuerdo con el poder de procesamiento de la información, como hemos visto en la campaña de Donald Trump.

Desde tiempos inmemoriales, la autoridad política ha estado estructurada de manera que, hacia dentro, unos pocos han gobernado a otros muchos mientras que, hacia fuera, el sistema internacional se ha organizado de forma jerárquica con un pequeño centro de poder y una gran periferia. En los dos casos, la dominación se ha basado en la superior capacidad tecnológica

que permita dominar a las masas, y, a través de ellas, dominar a los Estados. ¿Por qué iban a ser las cosas diferentes ahora en “el imperio de la vigilancia”?, como llama a este fenómeno contemporáneo Ignacio Ramonet (2016).

La universalización del uso de internet tiene efectos contrapuestos de gran envergadura a nivel social. Internet ha permeado todas las actividades humanas, desde la cultura, la religión y la política a la vida personal, entre otras, dando paso a la ya mencionada cibercultura, donde coexisten dos visiones enfrentadas sobre su uso: de un lado, la que tienen sobre la red las grandes empresas; del otro, los Estados.

En 2016, el *Diccionario de Oxford* colocaba el término *post-truth* como palabra del año. Poco después, ingresaba en la vigésimo tercera edición del *Diccionario de la lengua española* como “distorsión deliberada de una realidad, que manipula creencias y emociones con el fin de influir en la opinión pública y en actitudes sociales”. Es el signo contradictorio de una época en que, al contrario de la horizontalidad que en teoría debería facilitar, internet se ha convertido en vehículo verticalista de *fake news* y espionaje y manipulación digital de usuarios por parte de grupos de poder, retando a instituciones democráticas y cuerpos jurídicos.

Los conceptos de neutralidad limitan lo que los Gobiernos hacen en la red, la cual es a la vez desarrollada, gestionada y explotada como resultado de actividades corporativas. Si no se tiene el debido cuidado en defender el acceso a internet, y a la vez irlo regulando, puede confundirse con un amparo a ciertos monopolios/oligopolios *de facto* que se dan en el ciberespacio. La internet como un espacio supranacional y desregulado, abierto y supuestamente inclusivo y democrático como una “tierra de nadie” para el beneficio de quienes tienen el poder de ocupar ese espacio y usarlo para servir a sus intereses.

Si los Gobiernos impulsan la conectividad de su población de forma ciega, están casi directamente ampliando el mercado potencial de trasnacionales con fines de lucro o aliadas por contratos o comisiones oscuros con Gobiernos o grupos políticos, perdiendo poder y, con él, soberanía.

CONCLUSIONES/ Control para democratizar: legislando para todos

Desregulada y bajo el mito que esgrime la transparencia y la democracia como argumentos que hacen ver como ataques autoritarios o retardatarios los intentos de poner orden en el espacio digital (aunque cada día es más claro que la “desregulación” como factor de “democracia” es un espejismo que intenta enmascarar el verdadero control y las asimetrías de poder en la red),

la internet representa en el escenario actual una amenaza para la soberanía de los Estados, pero limitar de plano el acceso a este ámbito y su uso no los hará más independientes.

Urge democratizar la red: que los datos de los ciudadanos (que han devenido activos de mercado) sean propiedad colectiva y no de empresas transnacionales, con lo cual serían útiles para construir un proyecto de interés común que tome en cuenta las necesidades y las responsabilidades de la ciudadanía para afrontar los retos que encaran las sociedades y la humanidad en su conjunto. En caso contrario, seremos sujetos de un sistema internacional donde un ínfimo número de empresas no solo controlarían todos los servicios, sino el destino del ciberespacio de los Estados nación.

El avance de internet, sus servicios y las tecnologías de la información ha sido tan abrumador que el sistema jurídico fue incapaz de acompañarlo, tanto en lo nacional como en lo internacional. Se impone la adopción de un código de conductas para el uso y la explotación de la red de redes –en los niveles global y nacional, articulados–, que debe ser seguido tanto por los Estados como por las empresas transnacionales que manejan los servicios de internet. Para ello es necesaria la creación de normas de derecho internacional público que sean de obligatorio cumplimiento.

La transnacionalidad se ha jerarquizado frente al Estado, que se ha visto superado en algunas de sus competencias dentro de sus fronteras. Aunque esta coyuntura no refleja un pronosticable fenecimiento del Estado, la territorialidad ha de ser uno de los aspectos más complejos a analizar, ya que el desarrollo de la red de redes cuestiona su vigencia como elemento esencial en una definición actual del concepto soberanía.

Los expertos coinciden en que se hace necesaria una reformulación de este concepto, en función de acompasar las transformaciones impuestas por la incesante evolución de internet. En tanto, aparece el concepto de espacio –así como se aplica para altamar o la Antártida–, como alternativa para abordar el alcance de la noción de soberanía en el ciberespacio, por lo que debería ahondarse en el estudio y desarrollo de una *lex retialis* o ley de la red.

La vulneración de la soberanía en tiempos de internet es aún insuficiente y está lejos de un consenso y de conclusiones claras en los debates profesionales y de los programas de los movimientos progresistas en América Latina. Faltan programas para intervenir en las políticas públicas y para generar líneas de acción definidas que ayuden a construir un modelo verdaderamente soberano de la información en el continente. No existen una estrategia sistémica ni un marco jurídico homogéneo y fiable que minimice el control estadounidense, o

que asegure que el tráfico en la red se intercambie entre países vecinos, fomente el uso de tecnologías que garanticen la confidencialidad de las comunicaciones, preserve los recursos humanos en la región y suprima los obstáculos a la comercialización de instrumentos y servicios digitales avanzados que esta produce.

La integración Sur-Sur en temas de soberanía tecnológica e informática es una alternativa y una posibilidad de poder para los pequeños Estados que no cuentan por separado con el capital financiero para competir en el universo digital.

El Alba-TCP podría involucrarse en el esfuerzo de impulsar redes de observatorios que, además de ofrecer indicadores básicos y alertas sobre la colonización del ciberespacio, permitan recuperar y socializar las buenas prácticas de uso de estas tecnologías y las acciones de resistencia en la región, a partir de la comprensión de que el éxito o el fracaso frente a estas desigualdades dependen de decisiones políticas que serán más efectivas con la integración.

Bibliografía

Aoki, Keith. (1998). Soberanías múltiples y superpuestas: liberalismo, doctrina libertaria, soberanía nacional, propiedad intelectual “global” e Internet. Indiana Journal of Global Legal Studies, (5), 443.

Arbuet Vignali, H. (2016). La soberanía jurídica, la democracia y el derecho internacional en la posmodernidad. Estudio del CURI. Recuperado de http://curi.org.uy/archivos/Estudio%20del%20CURI%205%20Arbuet%20Vignali%20rev6.pdf

Asamblea Nacional del Poder Popular. (2019). Constitución de la República de Cuba. Recuperado de http://www.parlamentocubano.cu/wp-content/uploads/Tabloide-Constituci%C3%B3n.pdf

Congreso de la República del Perú. (2011). Ley que declara como derecho fundamental el acceso gratuito a internet y de necesidad pública y de preferente interés nacional la masificación de los servicios de telecomunicaciones de banda ancha y modifica los alcances del fondo de inversión en telecomunicaciones (FITEL). Recuperado de http://www2.congreso.gob.pe/Sicr/RelatAgenda/proapro.nsf/ProyectosAprobadosPortal/33F1A27C33F9CF97052578890009C80C/$FILE/4255FITEL.pdf

Cumbre Mundial sobre la Sociedad de la Información. (2003). Informe Final de la Fase de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información. Recuperado de https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0009!R1!PDF-s.pdf

Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones. (2013). Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Recuperado de http://undocs.org/es/A/68/98

Hannes Grassegger, V., y Krogerus, M. (2017). Yo no construí la bomba, sólo demostré que existía. Cubadebate. Recuperado de http://www.cubadebate.cu/especiales/2017/02/19/yo-no-construi-la-bomba-solo-demostre-que-existia/#.W-pi11v9TIU

I. R. P. Coalition. (2015). Carta de derechos humanos y principios para Internet. Recuperado de http://internetrightsandprinciples.org/site/wp-content/uploads/2015/03/IRPC_spanish_1stedition_final.pdf

Lambach, D. (2018). The Territorialization of Cyberspace. Conference: Tagung der DVPW-Themengruppe Internet und Politik, Heidelber. Recuperado de http://www.ub.edu/prometheus21/articulos/obsciberprome/winner.pdf

Lidgett, A. (2016). France facebook lawsuit update: Paris court rules over social media removal of painting depicting vagina. Recuperado de http://www.ibtimes.com/france-facebook-lawsuit-update-paris-court-rules-over-socialmedia-removal-painting-2305741

Perrit, H. H. (2004). Internet, ¿una amenaza para la soberanía?. Reflexiones sobre el papel de Internet en el fortalecimiento del gobierno a escala nacional y global. Buenos Aires: Heliasta.

¿Por qué Venezuela salió victoriosa en la más reciente guerra de cuarta generación?. (2017). *red58.org*. Recuperado de https://red58.org/por-qu%C3%A9-venezuela-sali%C3%B3-victoriosa-en-la-m%C3%A1s-reciente-guerra-de-cuarta-generaci%C3%B3n-ef5a524e88d7

Rabinad, M. G. (2008). La soberanía del ciberespacio. Lecciones y Ensayos, (85),85–107. Recuperado de http://www.derecho.uba.ar/publicaciones/lye/revistas/85/05-ensayo-maria-gimena-rabinad.pdf

Ramonet, I. (2016). El imperio de la vigilancia. La Habana, Cuba: Editorial José Martí.

Rodríguez Hernández, L. (2017). Un siglo de Teoría de las Relaciones Internacionales. La Habana, Cuba: Editorial Universitaria Félix Varela.

Santos Belandro, R. B. (2013). Territorio, frontera, soberanía y espacios: Cuatro conceptos que tensionan al derecho internacional privado. Revista de Derecho Público, (43), 75-110.

Suprema Corte de Justicia de Uruguay. (2016). Sentencia Nº 253, 22 de agosto, 2016. Ministro Redactor: Doctor Jorge O. Chediak González. Recuperado de

http://www.poderjudicial.gub.uy/images/resoluciones/2016/sent_scj_22-08-16_inconst_ley19307_medios_audiovisuales.pdf

Tsagourias, N. (2018). Law, Borders and the Territorialisation of Cyberspace. Indonesian Journal of International Law. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213511

Winner, L. (2000). Los Mitos Ciberlibertarios y sus Prospectos para la Comunidad. Contexto educativo: revista digital de investigación y nuevas tecnologías, (4).