Ciberdefensa y el ciclo evolutivo del ciberespacio

Oscar Niss / compilador

UNDEF libros

Universidad de la Defensa Nacional
Ciberdefensa y el ciclo evolutivo del ciberespacio ; Compilación de Oscar Niss. - 1a ed. - Ciudad Autónoma de Buenos Aires : Universidad de la Defensa Nacional, 2023.
132 p. ; 21 x 15 cm.

ISBN 978-987-82847-7-4

1. Ciberespacio. I. Niss, Oscar, comp.
CDD 005

Coordinación editorial: Martín H. Bertone
Diseño de tapa: Ana Lebioso
Diseño de interior: María Cordini
Diagramación de interior: Silvana Ferraro
Corrección: Zoe Ledesma

ISBN 978-987-82847-7-4

Impreso en Multigraphic Servicios Gráficos
Belgrano 520, C1091AAS. Buenos Aires.
en el mes de agosto de 2023.

Hecho el depósito que indica la ley 11.723
Impreso en Argentina.

Índice

Introducción

El libro que el lector tiene en sus manos recoge ponencias, ideas y debates surgidos en el ciclo sobre ciberdefensa organizado por el Centro de Estudios Estratégicos para la Defensa "Manuel Belgrano" (CEEPADE).

En las últimas décadas hemos asistido a un nuevo punto de inflexión en la línea del cambio civilizatorio: el tráfico de la información se volvió muchísimo más rápido que el de las personas. El desarrollo y la complejidad de las vías de comunicación electrónica, de la informática y la tecnología digital posibilitaron el surgimiento de un "ciberespacio" en el cual millones de usuarios se conectan permanentemente, y donde múltiples prestaciones y servicios se utilizan. Esto hace cómoda la vida cotidiana, reconfigura pautas de socialización e intercambio y construye nuevas dimensiones de representación cultural.

Puede ser un ejercicio interesante pensar cómo, en un siglo y medio, sucedieron una serie de saltos de globalización estructurados por el despliegue de paradigmas tecnológicos en transporte y comunicaciones, y analizar la relación de esos despliegues y paradigmas con las concepciones ideológicas predominantes. Tanto el surgimiento del ferrocarril como el del telégrafo, el teléfono, la radio y la televisión se dieron en un marco de pensamiento de fuerte impronta colectiva. La idea del Estado nacional, así como visiones finalistas –la fe en el progreso, los ideales igualitaristas, las ideologías totalitarias– se dieron en simultáneo con el despliegue de aquellas tecnologías. Habría que pensar cuánto ha sido causa y cuánto efecto, pero las ideas de centralidad, de poder total, de núcleo organizador, de canal claro y jerarquizado de emisión, fueron una pauta habitual y de sentido común.

El despliegue de la informática distribuida, de Internet y la era digital, en cambio, se dio en simultáneo con fin de la Guerra Fría, la postulación de una idea ingenua de globalización democrática y neutra, el surgimiento del posmodernismo, la promoción de ideologías del desencanto y de lógicas fragmentarias, además de la difusión de concepciones individualistas y consumistas. Cabe evaluar también aquí el juego de causa y efecto.

Tras la etapa inicial de entusiasmo, surgieron indicios y evidencia sobre los problemas que puede acarrear volverse dependiente de la red. Virus informáticos y estafas cimentaron la percepción de amenazas a la disponi-

bilidad, integridad y confidencialidad de la información que cada usuario pone en el ciberespacio, o de los riesgos a los que se expone cuando toma un servicio de la red, a la hora de adoptar o utilizar estas herramientas tecnológicas.

En este sentido, el derecho siempre va detrás de los hechos, y tras una década larga se empezó a dar un marco para la prevención de amenazas y ataques para robar o alterar información, que pueden tener motivaciones criminales, atacar a distintas víctimas individuales y poner en riesgo datos personales y privados de los ciudadanos. La seguridad de información fue generando conceptos, entornos y procedimientos de buenas prácticas. Se empezó a hablar, un poco más lentamente, de la dimensión militar y de los riesgos para la soberanía de los Estados. Además del crimen individual y de la amenaza a los derechos personales, podían darse ataques masivos, planificados y extendidos, dirigidos globalmente contra el cuerpo nacional.

Un caso señero de operación de guerra cibernética fue la infección de las centrífugas iraníes con el virus *stuxnet*, para retrasar aquel programa nuclear. Otro caso emblemático fue el ataque masivo de denegación de servicios en Estonia, cuyo análisis devino en la elaboración del "Manual Tallin", una suerte de extensión oficiosa de las reglas del derecho de guerra realizada por la OTAN.

Cuando nuestro país completaba el primer ciclo de planeamiento de capacidades militares, distintos países habían empezado a hablar de la ciberdefensa, desarrollando doctrina, organización, medidas preventivas y respuestas de índole o dimensión militar relativas a la seguridad cibernética. Así lo encararon también nuestras Fuerzas Armadas, y durante una década y media tuvieron una gran evolución y aprendizaje, inmersas en el contexto cambiante de las condiciones del ciberespacio, que se abordan en este libro desde distintas ópticas.

Cuando en 2014 se conformaron la Dirección y el Comando Conjunto de Ciberdefensa, en el mundo había un intento de abrir el debate sobre quién gobierna Internet y cómo. Las revelaciones de Assange, el caso Snowden, el hackeo de las cuentas de la presidencia de Brasil y el robo de la información de Petrobras fueron de altísimo impacto. Sin embargo, la literatura predominante y el sentido común consagrado eran renuentes a abordar la perspectiva soberana, mientras admitían, sí, que debía prevenirse el riesgo individual en la red. Una década después, el marco mundial del debate ha evolucionado y ya es difícil objetar la necesidad de un abordaje de perspectiva estatal y soberana.

Cómo se gobierna internet, cómo se despliegan y administran las redes de telecomunicaciones por las que discurren los datos, cuál es la dinámica

de investigación, desarrollo y comercialización de *hardware* y *software* y cuánto la dependencia tecnológica o comercial condiciona los grados de soberanía ciberespacial son interrogantes inevitables. Asegurarse el funcionamiento de cuotas o porciones del ciberespacio pasa a ser una necesidad para los Estados si quieren mantener los niveles de funcionamiento adecuados y satisfacer los requerimientos y aspiraciones de sus ciudadanos, que cada vez lo perciben más como una herramienta indispensable de la vida cotidiana.

La geopolítica tiñe de manera evidente la puja por el 5G, y casos como el *software* espía israelita *Pegasus*, o las acciones de interferencia y manipulación electoral de la empresa inglesa Cambridge Analytica en terceros países, entre ellos el nuestro, sinceraron el debate sobre la asepsia y neutralidad del ciberespacio. El ciclo organizado por el CEEPADE, cuyos debates y reflexiones se recogen en este volumen, resulta, por lo tanto, más que necesario y pertinente.

Sergio A. Rossi
Secretario de Estrategia y Asuntos Militares

Un marco para pensar políticas sobre el ciberespacio y la ciberdefensa

OSCAR NISS

Las acciones y operaciones en el ciberespacio están precedidas por el despliegue de una tecnología cambiante, puesta en producción apresurada y voluntariosamente.[1] En este sentido, debería otorgársele mayor rigurosidad al principio organizacional que dicta que todo elemento operacional debe estar enmarcado en un plan estratégico. Y esto sin duda pone a prueba las capacidades de las organizaciones que pretenden hacer más seguro el uso de este nuevo ambiente operacional.

A raíz de ese despliegue y de la irrupción de nuevas tecnologías vinculadas a la información y las comunicaciones es que aumenta la superficie de ataque[2] en el ciberespacio. En efecto, las vulnerabilidades en los dispositivos tecnológicos están estrechamente relacionadas con la aceleración de los procesos productivos que se dan entre el desarrollo del prototipo y su difusión en los mercados. El estímulo por la demanda de nuevos servicios hace que, en muchas ocasiones, sino en todas, los productos que se ofrecen en el mercado tengan altos grados de vulnerabilidad incorporados, casi convirtiéndose en uno de sus atributos.

En ese sentido, la velocidad de difusión[3] también ha crecido, especialmente en los últimos diez años, dado el notable acortamiento del ciclo de vida de los productos como consecuencia del constante y creciente flujo de innovación tecnológica. Estos y otros factores, como los presupuestarios y las divergentes visiones a largo plazo, hacen que a menudo las estra-

1 Es una práctica habitual que productos y servicios informáticos se comercialicen sin los debidos procesos de ensayos de seguridad en su diseño, lo que provoca el uso de tecnología vulnerable, con los riesgos que eso conlleva.

2 Magnitud de dispositivos tecnológicos vulnerables que están conectados a la Internet o en redes privadas.

3 La difusión de un nuevo producto se define como el proceso durante el cual la novedad se va propagando en la sociedad y es aceptada por los consumidores.

tegias queden de lado u obsoletas, legitimando lo táctico y operacional, llevando así a las organizaciones o a los Estados hacia un laberinto donde es necesario asumir o ignorar los riesgos inherentes, lejos de los residuales.[4]

Es debido a esto, en parte, que usar marcos referenciales[5] y pensar los escenarios posibles son de los principales desafíos en el momento del planeamiento estratégico de una política en el ciberespacio y en particular para su defensa. En ese sentido, el Ciclo Evolutivo del Ciberespacio propone las ideas centrales de un marco referencial de nivel estratégico, que contribuya en el diseño de políticas para el ambiente cibernético.

El Ciclo Evolutivo del Ciberespacio

Como todo ciclo, el punto inicial podría ser cualquiera de sus estadios. No obstante, lo que debe tenerse en cuenta para la elaboración de una estrategia, o bien para una gestión integral del ciberespacio con características soberanas, es que existen distintos componentes que contribuyen a un todo, cada uno de ellos con su propia estrategia para tratar sistémicamente, con una entrada y con un producido.

En ese sentido, el Ciclo del Ciberespacio propone un marco de trabajo compuesto por cinco burbujas, como ilustra la Figura 1: construcción de sentido, soberanía, normativa, industria, paradigmas. Cada una de estas burbujas del ciclo tiene sus *stakeholders*,[6] con sus intereses y objetivos, en ocasiones contrapuestos entre ellos. Otra complejidad que se agrega a este ciclo es que las partes pueden ser del sector privado o estatal, con políticas, a veces en ambos casos, atravesadas por cuestiones geopolíticas. Consideremos que hoy el ciberespacio atraviesa todas las actividades de un Estado y de la sociedad, desde el comercio, la educación, la comunicación y hasta las acciones bélicas.

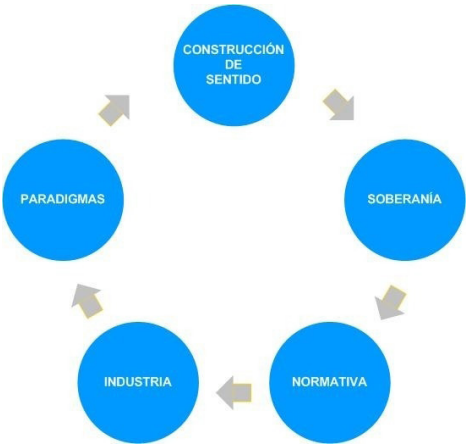
---

4 Los riesgos inherentes son aquellos que están presentes en un sistema o proceso desde su diseño o implementación inicial, mientras que los riesgos residuales son aquellos que permanecen después de haber implementado medidas de control y mitigación para reducir el impacto o su probabilidad de ocurrencia.

5 Los marcos referenciales para el diseño de una estrategia son enfoques estructurados que proporcionan un marco conceptual para el diseño y la implementación de políticas, planes y prácticas relacionados con una temática determinada. Estos marcos proporcionan una guía para identificar, evaluar y proyectar acciones.

6 Partes interesadas que ejercerán acciones que influencien las decisiones.

Figura 1: componentes del marco - Ciclo del Ciberespacio



Así, desde la perspectiva estatal, aunque el ciclo sea constante, es preciso saber dónde se está parado en un determinado momento, en qué burbuja, ya que este dato contribuiría a una evolución conveniente para los intereses de una nación. El dónde estamos requiere de un análisis minucioso, que puede contemplar actores estatales, privados e incluso académicos con el fin de elaborar un diagnóstico de posición certera en el ciclo. Esto no implica desatender las otras burbujas, sino saber dónde poner el foco para centralizar la energía y recursos disponibles.

Construcción de sentido

Sin duda el ciberespacio, siendo el escenario sobre el cual se despliegan políticas y acciones de la ciberdefensa, contiene diversas definiciones que surgen a partir de esta idea, aún amorfa y carente de sentido consensuado. Así lo describe la Junta Interamericana de Defensa (JID):

> *Muchos términos relacionados con el dominio* Ciber *y el propio término y concepto "ciber" son actualmente controvertidos. No existe un único glosario de definiciones ni una taxonomía globalmente aceptada y como consecuencia, la mayoría de estudios relacionados con el ciberespacio y sus aplicaciones se ven en la obligación de incluir sus*

> *propios listados de definiciones. Esta falta de consenso global de todo lo relacionado con el dominio ciber trae como consecuencia importantes disfunciones. (JID, 2020, p. 11)*

En ese sentido, existen disfunciones provocadas por los distintos enfoques derivados de disímiles concepciones acerca del dominio ciber.[7] Es muy normal ver esas disfunciones reflejadas en las estructuras del gobierno con incumbencias en lo cibernético.

Volviendo al título que nos ocupa, según Beccaria "la construcción de sentido que surge del diálogo entre quien produce una imagen/texto y quien la reconoce a través de una práctica hermenéutica, pone en relieve el carácter permanentemente abierto que le confiere a la obra el intérpete" (2013, p. 2). Esto tiene una implicancia literal en el caso de algo tan abstracto como el ciberespacio. De esta forma, la producción del concepto asociado, consecuente de esa rutina de diálogo, nunca es producto de una situación azarosa, sino de una intención de su creador. Esa intención, que dista de una teoría conspirativa, puede ser por conservar intereses económicos o políticos, en ambos casos desbordados por tensiones geopolíticas.

¿Y cuáles son los problemas con el concepto de ciberespacio? Según la JID son cuatro los inconvenientes, que adaptamos a nuestro planteo:

I. Falta una percepción global común, lo que trae aparejado distintas visiones y enfoques en el análisis necesario para el diseño de las políticas.
II. Difícil comprensión del dominio ciber. La información confusa –y a veces contradictoria– existente acerca de todo lo relacionado con el dominio ciber dificulta la labor de los decisores, tomándose en ocasiones resoluciones inadecuadas para las necesidades.
III. Estructuras organizativas diferentes. Las distintas percepciones y enfoques cibernéticos traen como consecuencia distintos tipos de organizaciones estatales, complicando la acción estatal y la cooperación internacional.
IV. Conflicto de responsabilidades. Diferentes definiciones y taxonomías derivan en conflictos en la asignación de tareas hacia dentro de una administración.

7 Una de las controversias más importantes en las discusiones de los grupos de trabajo sobre la temática en la ONU, que tensiona el debate, es sobre las características soberanas de este dominio.

Por todo esto, es normal ver organizaciones estatales con funciones difusas y a veces solapadas en sus incumbencias cibernéticas.[8] Esto nos lleva a la discusión de origen y primordial para cualquier diseño de políticas públicas: el resguardo de la soberanía.

Soberanía

La construcción de sentido sobre este nuevo espacio de operaciones, dado su pretendido carácter virtual, interpela el concepto de soberanía nacional tradicionalmente vinculado a lo territorial. Sin duda el ciberespacio, tomando muchas de las definiciones plasmadas en distintos tratados entre naciones, tiene en sus capas inferiores un componente tecnológico duro, dispuesto sobre una superficie territorial física en la mayoría de los casos. Esto es la tecnología que le da soporte a la comunicación, al almacenamiento y al procesamiento de datos. Estamos hablando aquí del componente físico del ciberespacio: antenas de comunicación, fibra óptica, centros de datos y otros, que están dentro de territorios soberanos.

Si ese conjunto de datos que componen un paquete de información puede estar distribuido en distintos servidores, y a su vez estos distribuidos en distintos asientos territoriales, todos integrados por tecnología de *software*, que también puede estar distribuida, entendemos que este conjunto de componentes tecnológicos o datos binarios está necesariamente asentado en dispositivos apoyados en algún territorio, sobre el que alguna nación ejerce sus derechos soberanos.

Es preciso entonces conceptualizar adecuadamente la idea de ciberespacio considerando que no es un espacio independiente de los otros ámbitos espaciales como la tierra, el mar y el aire. Tampoco es soberano *per se*, sino que es una infraestructura sobre la que se ejerce soberanía, como tantas otras. Su naturaleza escindida y compleja no lo exime de la pertenencia. El ciberespacio, entonces, concebido como entidad abstracta y disociada del mundo físico es consecuencia de la construcción de sentido. Así es que las prácticas discursivas que subyacen a esta lógica –la del ciberespacio como entidad abstracta– han establecido formas particulares de

8 Por ejemplo, en nuestro país distintos ministerios tienen incumbencias en temas cibernéticos: Ministerio de Seguridad, de Defensa, de Justicia, de Relaciones Exteriores y Jefatura de Gabinete de Ministros. Las misiones y funciones no están del todo claras y se solapan.

representación del mundo, logrando quebrar varias veces la lógica del pensamiento técnico.

En ese sentido, el aspecto del ciberespacio en su anclaje territorial debe ser ponderado incluso desde una perspectiva geográfica, donde "se podría experimentar cierto tipo de preocupación, al presenciar la gran cantidad de opiniones que desde diferentes sectores mencionan la falta de relevancia que puede tener el espacio geográfico en el contexto de las actuales tecnologías digitales" (Buzai, 2013, p. 3).

Aun en la pretensión de desarrollar cartografías enmarcadas en lo que hoy se llama cibergeografía, puede apreciarse tanto en los mapas topológicos como los de despliegue que el ciberespacio lejos está de ser igualitario:

> *Al analizar detalladamente el mapa obtenido, la simple visión de la configuración espacial de las conexiones realizadas muestra inmediatamente que la red igualitaria para todos sus usuarios es un mito. El ciberespacio presenta sitios claramente jerarquizados y la ubicación de Buenos Aires en el extremo inferior del* cibermapa *es netamente periférica. (Buzai, 2013, p. 8)*

Es evidente que la discusión sobre el despliegue territorial y físico del ciberespacio es la fundamentación para la consideración soberana de este, que deriva hacia la construcción normativa para este nuevo ambiente. Así lo consideran incluso las distintas naciones en el seno de la Organización de las Naciones Unidas, concordando que la soberanía aplica al conjunto de las Tecnologías de la Información y la Comunicación (TIC) o al componente físico del ciberespacio.

Normativa

A partir del entendimiento soberano de las TIC, es necesario un marco normativo legal que otorgue legitimidad a la instrumentación de ulteriores políticas en este tensionado ambiente. Particularmente, que contemple las acciones de los diferentes actores estatales con incumbencia en el ciberespacio, como Defensa, Seguridad, Justicia y Cancillería, entre otros, que requieren la construcción de un marco legal que las ampare, delimite e instruya, considerando los derechos y deberes normados por la Constitución, los tratados internacionales y las leyes vigentes.

No solo las normativas se debaten en el ámbito nacional, sino que hay otras dos esferas de discusión y de aplicación del derecho, que son la internacional y la regional, donde es menester participar de manera activa. Organizaciones como la ONU –con sus grupos de trabajo sobre derecho internacional aplicado al ciberespacio–, la Organización de Estados Americanos, la Junta Interamericana de Defensa, el Foro Iberoamericano de Ciberdefensa y el Convenio de Budapest, entre otros, se encargan de debatir y poner en consideración los aspectos de soberanía, paz y seguridad en el ciberespacio.

Nuestro país, por su parte, tiene normas como la Ley Argentina Digital, que se expresa claramente sobre el aspecto soberano:

> *Las disposiciones de la presente ley tienen como finalidad garantizar el derecho humano a las comunicaciones y a las telecomunicaciones, reconocer a las Tecnologías de la Información y las Comunicaciones (TIC) como un factor preponderante en la independencia tecnológica y productiva de nuestra Nación, promover el rol del Estado como planificador, incentivando la función social que dichas tecnologías poseen, como así también la competencia y la generación de empleo mediante el establecimiento de pautas claras y transparentes que favorezcan el desarrollo sustentable del sector, procurando la accesibilidad y asequibilidad de las tecnologías de la información y las comunicaciones para el pueblo. (Ley 27.078/2014)*

Aun así, es muy frecuente encontrar normas que se contraponen a otras, sobre todo cuando abordan cuestiones novedosas, como el caso de las TIC. Esto puede observase en la Estrategia Nacional de Ciberseguridad en su primera versión, publicada durante la gestión del gobierno del ex presidente Mauricio Macri, cuando plantea:

> *… las cuestiones vinculadas con el ejercicio de la soberanía. Este último concepto en particular, entendido como el ejercicio supremo del poder del Estado, está necesariamente vinculado a lo territorial. Sin embargo, Internet representa un dominio global e intangible y un flujo infinito de datos sobre el cual no se ejerce dominio ni soberanía. (Poder Ejecutivo Nacional, 2019)*

La necesidad de un plexo normativo coherente y actualizado, en vista de los acuerdos internacionales, es la base del desarrollo de políticas públicas para esta dimensión. De hecho, en la reciente y segunda versión de la

Estrategia Nacional de Ciberseguridad, puesta para consulta pública en diciembre de 2022, durante la gestión del presidente Alberto Fernández, se incorporan los conceptos de soberanía en el ciberespacio y respeto a los derechos humanos, en línea tanto con las normas internas como con las resoluciones de la ONU.

Adicionalmente, en el ámbito nacional se deben impulsar determinados cumplimientos, como el alojamiento de datos sensibles en servidores y *datacenters* con anclaje físico en el país, al igual que los servicios de nombre de dominio (DNS, por sus siglas en inglés) y políticas precisas respecto de la protección de las infraestructuras críticas de las tecnologías de la información y de las de la operación (IT y OT respectivamente, por sus siglas en inglés), requiriendo estándares de seguridad pertinentes.

Industria

Este estadio es consecuente a las decisiones normativas que, además de delimitar obligaciones, deben propiciar políticas, como por ejemplo impulsar la industria nacional de la ciberdefensa,[9] ya que es el elemento operacional de las Fuerzas Armadas que debe asegurar la soberanía en el ciberespacio. En ese sentido, es necesario tener control sobre la tecnología empleada para el desarrollo de una capacidad de defensa adecuada en este ambiente. Por otro lado, debe estar normada la calidad o seguridad de la tecnología que se dispone en el mercado, tanto para uso comercial como militar, lo cual implica trabajar sobre la cadena de suministros.

En particular el desarrollo tecnológico para la defensa es necesario para ser consecuentes con el objetivo de brindar un resguardo soberano a la porción nacional del ciberespacio. Desde el punto de vista tecnológico, la defensa del ciberespacio está compuesta por diferentes elementos, donde al menos uno de ellos debe ser de origen nacional a fin de permitir, como se dijo, que los elementos operacionales tengan control de las herramientas empleadas.

Como lo expresaba Jorge Sábato, la soberanía tecnológica:

> *…trata del manejo propio de la tecnología que más nos conviene, nacional o no. Por supuesto que si no hay un fuerte contenido de*

9 Defensa del espacio cibernético ligado a la soberanía.

> *elementos propios, esos paquetes pueden no estar bajo nuestro control: si el paquete tiene todos los elementos importados, sencillamente nos encontramos bajo el dominio del dueño del paquete. (Gallardo, 2005, p. 90)*

Asimismo, para el desarrollo de esta industria se debe pensar en políticas públicas de promoción de tecnologías dedicadas a la ciberseguridad y ciberdefensa. El potencial mercado debiera actuar como aliciente para la inversión tanto privada como estatal. No olvidemos que de la inversión en investigación y desarrollo (I+D) surgen las innovaciones y los nuevos paradigmas, que no son otra cosa que parte de los procesos del ciclo que proponemos.

Un párrafo aparte debe ser dedicado a la formación de profesionales. El talento humano es el activo más importante de cualquier pretensión tecnológica. La promoción desde el Estado de políticas públicas educativas, con apoyo e incentivo a la creación y matriculación en estas ciencias, es uno de los renglones necesarios para el desarrollo industrial de las tecnologías aplicadas al despliegue y defensa del ciberespacio.

Paradigmas

Indudablemente la inversión y la acción conjunta del Estado y la industria es lo que posibilita la aparición los nuevos paradigmas, a partir del resultado de sus procesos de investigación, innovación en productos y creación de servicios. Una de las maneras de anticiparse a estos paradigmas es situarse a diez *años vista* y pensar qué se debió haber hecho en el pasado para llegar hoy a un escenario tecnológico que sirviera a la sociedad en su conjunto. Pensar, además, cómo se debe organizar el ambiente del ciberespacio de interés para la nación, cómo se debe defender, qué inquieta y cómo afecta a las funciones inherentes del Estado, abre el camino para ensayar distintas estrategias con la anticipación necesaria.

En ese sentido la internet de las cosas (IoT, por sus siglas en inglés), *big data* y *cloud computing* son todas tecnologías que pueden llegar a ser disruptivas, afectando la administración y el uso adecuado del ciberespacio, tanto para la sociedad como para el Estado, y sin embargo no constituir un cambio de paradigma. En cambio, hay que prestar especial atención a la inteligencia artificial (IA) y *machine learning* (ML), además del escenario cuántico y al la internet cuántica, que sí puede constituirlo.

Los cambios de paradigma por definición presentan el desafío de desarrollar nuevos conceptos, nuevas imágenes para esas cosas que no estaban definidas. Sin duda es en ese momento que aparecen las tensiones, ya que esos cambios, en general, son de enorme magnitud, aunque no pueda apreciarse en el momento. Debe considerarse que un cambio de paradigma manifestado en nueva tecnología suele ser conocido en sociedad una vez que su desarrollo adquiere un cierto grado de evolución para la industria estratégica de un país, sea esta de defensa, de impacto en la economía o en la comunicación social. Ejemplo de eso es la Internet, cuyo derrotero comenzó en las Fuerzas Armadas de Estados Unidos de América, para luego de un par de décadas pasar al ambiente universitario y recién otras décadas después transformarse en este ambiente ciberespacial explotado por todos los interesados.

Sin duda, los cambios de paradigma impactan regularmente en una posterior construcción de sentido que contiene al concepto, comenzando así nuevamente este ciclo constante de desarrollo de tecnología contenida en el ciberespacio.

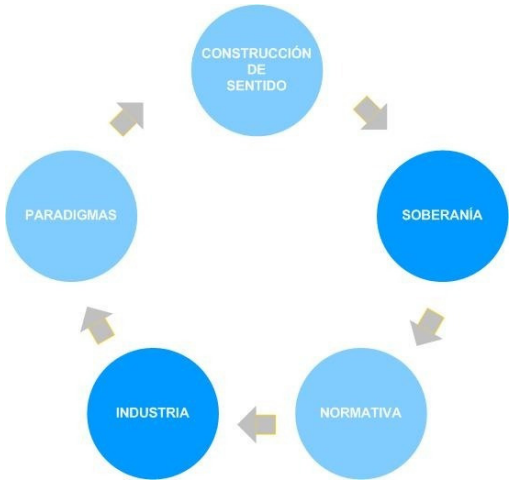
Conclusión

La compleja administración del ambiente ciberespacial debe ser abordada con políticas públicas desde diferentes dimensiones, pero con una mirada holística. El Ciclo Evolutivo del Ciberespacio pretende ser una herramienta que nos permita pensar la problemática del ciberespacio abordando temas tan abstractos como la construcción de sentido, lo normativo o incluso lo *duro* como la tecnología. Nos permite distinguir cada una de las burbujas interconectadas para el diseño de un desarrollo hacia el interior de cada una de ellas y nos permite medirlas, para invertir de manera inteligente los recursos disponibles.

En este marco del Ciclo Evolutivo del Ciberespacio hay dos burbujas que tienen especial importancia. Una de ellas es la de soberanía y la otra es la de industria, como puede verse en la Figura 2. La política y las políticas públicas deben atender el aspecto soberano y de desarrollo de la industria nacional.

A lo largo de este libro repasaremos cada una de las etapas del marco propuesto, con textos extraídos del ciclo de charlas realizado en la Universidad de la Defensa Nacional, junto con el Observatorio de Defensa y la Subsecretaría de Ciberdefensa, durante octubre y noviembre de 2021,

Figura 2: Componentes del marco – procesos esenciales



titulado "Ciberdefensa: el Ciclo Evolutivo del Ciberespacio", donde los disertantes abordaron cada uno de las procesos del ciclo. Valga como propuesta para pensar estrategias y políticas para el ambiente cibernético y la libre disponibilidad del ciberespacio, para los intereses de la nación, la ciberseguridad y la ciberdefensa.

Referencias

Beccaria, L. N. (2013). *El lenguaje y la construcción de sentido.* Buenos Aires: UNLP.

Buzai, G. D. (2012). El Ciberespacio desde la Geografía. Nuevos espacios de vigilancia y control. *Meridiano - Revista de Geografía*, *1*: 265-278. Disponible en: <http://www.revistameridiano.org/n1/13/>.

Gallardo, O. S. (2005). *Jorge A. Sabato y el desarrollo tecnológico necesario y posible*. Córdoba: El Emporio Ediciones.

Junta Interamericana de Defensa (2020). Guía de Ciberdefensa. Recuperado de: https://www.jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf

Poder Ejecutivo Nacional (2019). *Estrategia Nacional de Ciberseguridad*. Recuperado de: https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf

Tecnologías digitales, Internet y cambios de paradigma

ARIEL VERCELLI

Sabemos que tenemos que desarrollar políticas nacionales, mejorar ciertos niveles industriales y alcanzar regulaciones acordes a los tiempos que corren y orientarlas a la defensa de los intereses de la patria. Estos son todos asuntos absolutamente necesarios y que nos tomamos en serio, pero que muchas veces no sabemos bien cómo abordarlos. Por ello, entiendo necesario establecer diálogos, mirar en perspectiva nuestros problemas y analizar cómo hacemos para resolverlos.

Con mi intervención no pretendo dar una solución. No la tengo. Pero sí quiero compartir con ustedes los caminos para encontrarlas. Porque, ciertamente, se trata de caminos que se hacen al andar, de caminos que hay que transitar colectivamente. Nos enfrentamos a una situación de alta complejidad. Es un escenario donde no hay buenos ni malos, sino que hay intereses permanentes. Este punto es clave. Hay que entender que algunos desarrollos en China o algunos posicionamientos estadounidenses se vienen sosteniendo durante muchas décadas, lo mismo ocurre con los rusos. La idea de esta exposición es que nosotros podamos mirarnos al espejo y analizar bien qué estamos haciendo. Nada de todo lo que voy a contarles es inmediato. Diría, mejor, que les vengo a plantear preguntas, a mostrarles posibles caminos para recorrer y a ofrecerles referencias para profundizar.

¿Cuál es el problema? Estamos frente a una situación compleja, cambiante, y en la cual aún no nos terminamos de dar cuenta de qué es lo que ocurre con el ciberespacio. Si bien analizamos estas cuatro, cinco o seis esferas del ciberespacio (y tal vez habría que agregar algunas más), algo se nos está escapando de la situación problemática en general. Oscar Niss lo describe bien, nos enfrentamos a situaciones problemáticas que son circulares y que se presentan como redes. Y cuando trabajamos sobre soberanía nacional, también estamos trabajando sobre industria, cambio tecnológico, normativas, etc. Estamos trabajando en todo eso y, en simultáneo, en

varias cosas más, como cuestiones ideológicas o sobre la construcción de sentido. Y, claro, la complejidad está en que nosotros necesitamos una solución integral sobre el ciberespacio en la República Argentina.

Puntualmente, en esta charla me voy a abocar a analizar qué está pasando en la actualidad entre las tecnologías digitales, Internet (el ciberespacio) y los cambios de paradigmas que se observan (o los que no observamos). Estos, por otra parte, implican a cada paso otros cambios en el escenario global. De hecho, cada vez que se cambian cuestiones normativas, industriales o de otro tipo, también se van produciendo distintos escenarios en las otras esferas en las que estamos trabajando. De esto se trata la complejidad que antes mencionamos.

Por ello, y es muy importante enfatizar este punto, si nosotros somos buenos solo en algunas de estas esferas (como, por ejemplo, los europeos, que son muy buenos planteando regulaciones), estas capacidades no nos van a alcanzar para resolver el problema general. Digamos que, para resolver lo que Oscar Niss nos está invitando a pensar, que es cómo cambian y se articulan estos ciclos evolutivos del ciberespacio (cómo pensarlos, sus cuestiones ideológicas, la creación de sentido, las políticas, las regulaciones), vamos a necesitar ser muchas y muchos analizando el fenómeno. No importa si somos plenamente coincidentes. Importa que en algún momento podamos dialogar e identificar qué situación estamos atravesando.

Hace años que estamos acostumbrados a que los cambios tecnológicos (y de paradigma) provengan de otros lugares. Por ejemplo, si consideramos las industrias tecnológicas de los Estados Unidos o de China, rápidamente observamos que son realmente arrasadoras. Si uno mira la industria estadounidense, a partir del Silicon Valley, ve algo exponencial. Es imposible que Argentina u otros países de América Latina puedan competir de forma directa sin establecer políticas de largo plazo. Digamos, además, que tampoco nos alcanzan las cuestiones sustitutivas. Basta con mirar un poco la historia de la informática nacional: Argentina contó con buenas iniciativas, pero rodaron un poco y se quedaron a mitad de camino.[1]

En concreto, para esta presentación me gustaría invitarlos a reflexionar sobre un cambio de mirada que se está dando en el mundo tecnológico. Se trata de un cambio que, como mencionábamos, es a la vez tecnológico e ideológico, y está atravesado por cuestiones jurídico-políticas e industriales.

1 Al respecto se puede revisar el texto de Bianculli y Vercelli (2022).

¿Cómo estamos acostumbrados a ver y considerar el desarrollo tecnológico e industrial de otros países? Por lo general (perdón por las generalizaciones) a nosotros nos llega una idea de industria tecnológica, de artefactos industriales y de empresas privadas altamente eficientes y con servicios muy concretos (entre otras: Facebook, Google, Netflix, Intel, AMD u otras chinas, como Tencent o Huawei, o rusas o europeas). Es decir, estamos acostumbrados a ver estas empresas como si fueran parte de una esfera privada y como si estuvieran perfectamente alineadas con una lógica de mercado –y de competencia– en cada uno de sus países. Estas empresas se nos presentan ("se nos venden"), dentro de una lógica de mercado global, como si solo dependieran de la genialidad de sus dueños y accionistas, o de la visión y eficiencia de otras empresas que invierten en ellas. Se nos representan, todavía, como si fueran ascéticas, puras, eficientes, innovadoras y desligadas de los Estados.

¿Por qué digo esto? A partir de las denuncias y de las filtraciones de Julian Assange (2013; 2014) y, sobre todo, las de Edward Snowden,[2] allá por el 2013, pudimos advertir que muchas de las más grandes empresas y plataformas tecnológicas no eran algo distinto de la esfera pública-estatal, y que se mantenían indiferenciadas de las acciones y políticas de los diferentes gobiernos en EE. UU. ¿Dónde habrán quedado conceptos como la neutralidad de la red, la no intervención estatal en la regulación de Internet, la idea de un ciberespacio autogestivo o la autorregulación corporativa? Muchas de estas temáticas, centrales durante décadas y con un claro posicionamiento ideológico, hoy se podrían describir como parte de las mitologías a través de las cuales aprendimos a mirar el ciberespacio.

Con el tiempo, Internet se expandió y todos, rápida o lentamente, advertimos que el ciberespacio estaba montado sobre infraestructuras, que tenía una capa física y que había allí cuestiones vinculadas a la defensa, al derecho, a la soberanía, etc. Sin embargo, a pesar de estos aprendizajes, todavía hoy muchas y muchos siguen pensando que estas grandes corporaciones tecnológicas y de Internet solo pertenecen al sector privado y están perfectamente separadas de los Estados. ¿Es posible seguir sosteniendo esta separación? ¿Cuántas de las grandes plataformas de In-

2 Edward Snowden es un experto en tecnologías de información estadounidense asilado en Rusia, que trabajó para la CIA (Agencia Central de Inteligencia, por sus siglas en inglés), la DIA (Agencia de Inteligencia en Defensa, ídem), la empresa Dell y la firma Booz Allen Hamilton (trabajando para la National Security Agency, en Hawaii). En 2013 filtró 2013 a los medios masivos de comunicación miles de documentos clasificados sobre la vigilancia masiva de la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) de EE.UU. Al respecto se pueden revisar el libro de Glenn Greenwald (2014) y el documental de Laura Poitras (2014).

ternet están efectivamente separadas de los Estados donde crecieron y se les dió (o da) protección? Yo diría que ninguna. Es obvio que tienen una especie de ropaje para la competencia en mercados internacionales, porque obviamente no descartan ganar todo el dinero que puedan. Sin embargo, más allá del dinero, también hay otros intereses detrás del diseño de sus servicios y tecnologías, que están orientados por intereses geopolíticos de los Estados.

Cuando se observa el accionar de estas empresas puertas adentro de sus Estados (por ejemplo, cómo operan al interior de Estados Unidos, Rusia, China) es muy difícil observarlas atravesadas por el ascetismo liberal-neoliberal. Se trata, en su gran mayoría, de corporaciones monopólicas, que han crecido gracias a los contactos gubernamentales y estatales, que se nutren de gigantescos contratos con el Estado y, claramente, se mantienen gracias a regímenes de excepción y privilegios (muy pocas veces son sancionadas administrativa o judicialmente). Incluso, en sus países de origen, la mayoría de las veces se las considera y protege como parte de la cultura nacional.[3]

La modernidad política estableció separaciones tajantes entre el Estado y el mercado. Sin embargo, para este tipo de empresas nunca queda tan clara la separación. Para algunos esta indiferenciación entre lo público y lo privado puede ser algo evidente y para otros una gran herejía. Ahora, si se mira cómo operan empresas como Facebook (ahora Meta) o Alphabet (en el caso de Google), o cómo opera la misma Huawei en China, es evidente que se hayan estrechamente unidas e indiferenciadas de las políticas estatales (de EE. UU. y China respectivamente). Las revelaciones de Edward Snowden nos permitieron ver que, en realidad, las empresas estadounidenses denunciadas eran parte del Estado, con pleno acceso en tiempo real a todo lo que circulaba por sus servidores a nivel nacional e internacional. Las filtraciones permitieron observar cómo estas empresas formaban parte de las infraestructuras críticas del gobierno estadounidense.

Me acuerdo perfectamente de que las filtraciones no me dejaron tan sorprendido, porque ya venía investigando el tema y escribiendo algunas

3 Más allá de los ejemplos estadounidenses, chinos o rusos, en 2004, invitado por la Agencia Coreana para las Oportunidades Digitales (KADO, por sus siglas en inglés), escribí en Seúl un artículo denominado "Corea y la ubicuidad de la información: U-Corea" (Vercelli, 2004). Una de las cosas que más me sorprendió de los laboriosos coreanos fue que ofrecían su tecnología como una parte esencial y constitutiva de su cultura milenaria. Incluso, muchas de sus corporaciones tecnológicas (Hyundai, LG o Samsung) también mantienen una indiferenciación entre intereses públicos y privados.

columnas de opinión relacionadas.[4] Sin embargo, para el momento era un tema novedoso, que no se veía tan claro. Una década después asumimos como normal que Mark Zuckerberg fuera al Senado estadounidense por el caso Facebook Inc. / Cambridge Analytica y que solo se le hubieran hecho preguntas formales, "de cotillón", que no le preguntaran nada complejo y le permitieran contestar cualquier cosa sin recibir sanciones. La justicia estadounidense tampoco hace absolutamente nada sobre el poder omnímodo que tienen estas corporaciones sobre la población. En el caso europeo también es parecido, aunque buscan restringir las corporaciones extrajeras a la Unión Europea.

Así, al interior de cada uno de estos países (tomemos Estados Unidos, la Unión Europea, Rusia y China como para tener un esquema) muchas de las cosas que vemos en la prensa no son ciertas. Cada vez que estalla un escándalo, sólo se dan algunos movimientos formales (accesorios, periféricos) pero no termina pasando nada. Resulta obvio que mucho de lo que estamos leyendo sobre el mundillo tecnológico es mentira, está vacío o es meramente formal. Este es uno de los motivos por los cuales no ocurren las soluciones del derecho internacional.

Algo similar se da con el calentamiento global. Simple y sencillamente, no hay consenso para construir y adoptar las soluciones. En estos momentos, aunque tal vez cambie en el futuro (para mejor o para peor), el escenario tecnológico es de enfrentamientos. Por ello, resulta necesario tanto advertir estos cambios como ajustar nuestras miradas.

Ahora bien, insisto en este punto, aunque no quede tan claro que estas empresas en Estados Unidos o en China sean empresas del ámbito privado y estén perfectamente separadas de la esfera estatal: ¿para qué sirve el ropaje externo que le dan a nivel internacional a esta división entre las empresas privadas y los Estados? Bueno, digamos que a nivel internacional, detrás del diseño de ciertas tecnologías, es posible identificar diversos intereses: comerciales, de posicionamientos geopolíticos y de control de las poblaciones, entre otros. Miremos lo que ocurre en la actualidad, por ejemplo, con Internet de las cosas, con los desarrollo de microchips o la puja entre Estados Unidos y China por las tecnologías 5G (quinta genera-

4 El 28 de noviembre de 2011, antes de las filtraciones de Snowden en 2013, el escándalo de Carrier IQ mostró como los teléfonos móviles (HTC), bajo sistema operativo Android (Google Inc.) traían instalados de fábrica un rootkit (*software* espía) que registraba y enviaba furtivamente todo tipo de información a la empresa Carrier IQ en Silicon Valley. Al respecto, en la sección de tecnologías de *Télam*, escribí seis columnas siguiendo el caso (Vercelli, 2012b; 2012c; 2012d; 2012e; 2012f; 2012g).

ción de telefonía móvil). Desde 2019 los estadounidenses aplican sanciones económicas, bloqueos comerciales y prohibiciones para la tecnología 5G de Huawei y de otras empresas chinas, buscando que estas no sean habilitadas en su territorio y también queden excluidas de los territorios de sus socios estratégicos en términos de inteligencia (australianos, ingleses, etc.).[5]

Las prohibiciones y bloqueos de los EE. UU. sobre las tecnologías chinas, o sobre las empresas rusas, buscan delimitar alianzas tecnológicas. El planteo que hacen los estadounidenses es: "si querés comprar y usar mis tecnologías (determinados chips, computadoras, etc.), entonces no podés comprar otras, no podés comprarles a otros". Parecen afirmar, sin grises: "o estás dentro de mi sistema tecnológico o estás fuera. Y si estás afuera no sos mi enemigo, pero casi. Decime de qué lado de las nuevas fronteras tecnológicas estás y dónde te paras y después vemos cómo seguimos otras conversaciones comerciales y políticas" (entre otras, las deudas con organismos internacionales). Y la presión es real y concreta. Ni Argentina ni otros países de la región se pueden quedar sin tecnologías, sin chips, sin hacer funcionar algunos de sus servicios más elementales. Por ello, el concepto de soberanía tecnológica resulta clave para entender como se relacionan las diferentes esferas del ciberespacio.

Nos encontramos en una especie de cambio de paradigma, de transición, donde reconocemos que algunas empresas a nivel internacional usan sus servicios (algunos gratuitos y otros baratos) como parte de una negociación más compleja, que involucra los intereses públicos-estatales de las principales potencias. Este escenario internacional se torna evidente al observar las pujas tecnológicas. Hoy la casuística es abundante, sobre todo si analizamos EE. UU., China, Rusia o la Unión Europea. Surge, entonces, una pregunta central y urgente: ¿qué hacemos o qué deberíamos hacer en la Argentina frente a estos cambios, tanto tecnológicos como jurídico-políticos? ¿Qué modelo de desarrollo tecnológico-industrial podríamos utilizar sabiendo que, como venimos analizando, las empresas privadas funcionan en tándem con la esfera público-estatal?

En Argentina, lamentablemente, ciertas alternancias gubernamentales han perjudicado al Estado, con gobiernos que contrajeron deuda de forma abusiva y atentaron contra el desarrollo industrial nacional. Esta manía de

5 Entre 2021 y 2022 las tensiones sobre las tecnologías móviles 5G se extendieron a los chips. Las tensiones entre EE.UU., China y China-Taiwán por el control de los chips y la re-ubicación territorial de empresas que producen semiconductores no han hecho más que agravarse y profundizarse (Vercelli, 2022b).

"insertarnos" en el mundo fue muy perjudicial para la Argentina: nos ha dejado sin piezas centrales del Estado, sin planificación y sin protección para los intereses públicos. No seamos ingenuos, cuando alguna de estas grandes empresas tecnológicas sale a competir al mercado internacional (sean chinas, rusas, estadounidenses o europeas), en todo momento representan los intereses de sus casas matrices, del lugar donde efectivamente se las financió durante años, donde se les ofreció cobijo para que puedieran crecer y posicionarse. No es casual que muchas de estas empresas se desarrollen como monopolios o que construyan oligopolios en sus países de origen.

Incluso, estas corporaciones tecnológicas resultan complejas de controlar en los países donde surgieron: corporaciones monstruosas como IBM, Alphabet o Meta, que hasta llegan a poner en jaque la democracia, no solo en otros países, sino también en los propios. Valga como referencia el caso de Facebook Inc. (más Cambridge Analytica) y su responsabilidad en la manipulación y desinformación para favorecer a Donald Trump en la elección de 2016 y para perjudicarlo en su reelección en 2020.[6] Recordemos que, en 2020, Facebook Inc. y Twitter directamente le bloquearon la cuenta a Donald Trump (quien aún era presidente en ejercicio). En ese nivel estamos, donde en los Estados Unidos no se respeta un derecho tan básico como la libertad de expresión.[7]

En este punto es bueno plantearse si todo está cambiando muy rápidamente, o en realidad, estuvimos mirando mal lo que ocurría. Creo que voy a quedarme con las dos opciones. Todo cambia rápidamente y, además, estuvimos mirando mal lo que realmente sucede en el ciberespacio. Aprovecho, entonces, para retomar la pregunta: ¿qué tenemos que hacer en la Argentina? ¿Tendríamos que avanzar sobre empresas mixtas (público-privadas)? Lo dejo así, bien abierto, porque no tengo un posicionamiento claro sobre cuál es la solución. En Argentina hay empresas del Estado, empresas mixtas, empresas privadas nacionales que funcionan asociadas con el Estado nacional y empresas extrajeras que operan servicios naciona-

6 Al respecto se puede revisar el artículo "El extractivismo de grandes datos (personales) y las tensiones jurídico-políticas y tecnológicas vinculadas al voto secreto" (Vercelli, 2021) donde, a través del caso Facebook Inc. - Cambridge Analytica, se analiza cómo el extractivismo de grandes datos y la psicografía pueden favorecer la manipulación de personas y poblaciones.

7 En 2022 Elon Musk compartió documentos internos de Twitter (*Twitter Files* o "Archivos de Twitter") donde se muestra cómo la red social también sabe de censura, ocultamiento, desinformación y operaciones de inteligencia para los gobiernos de turno en los EE. UU. (Vercelli, 2022c). El tema, claro, no es nuevo. En febrero de 2012 también se publicó en *Télam Digital* la columna "Twitter censura y se convierte en una plataforma de control social" (Vercelli, 2012a).

les fundamentales. Incluso, es importante hacer esta aclaración, a diferencia de lo que ocurre en EE. UU. China o Rusia: en Argentina existen enormes empresas supuestamente "nacionales", que son líderes en el mercado interno, pero parecen operar como corporaciones extranjeras y no responden a las políticas estatales. Sobre estas últimas, es bueno aclarar que en los EE. UU., China o Rusia, estas empresas "pseudo nacionales" hubieran sido rápidamente desmanteladas.

Es claro, acá tenemos un problema enorme. El último momento en que discutimos esto fue, a mi entender, hace más o menos diez años, y lo hicimos con relación a la Ley de Servicios de Comunicación Audiovisual. Se debatió la posición dominante de una gran empresa como Clarín, con repetidoras en todos lados, y que, además, hoy maneja telecomunicaciones e infraestructura de conectividad. Como antes les comentaba, en varios puntos esta corporación parece no responder a los intereses nacionales y no se alinea fácilmente ni a las políticas ni a los intereses del Estado argentino. Es decir, no responde de la misma forma que los estadounidenses o los chinos exigen a sus propias empresas, con sujeción a los intereses nacionales. No veo que a Facebook, Alphabet o Huawei se les ocurra no responder a los intereses y a las reglas del juego que les imponen sus Estados.

Entonces, acá quiero ser muy claro: ¿estamos diciendo que las empresas tienen que alinearse con las políticas estatales? Miremos qué es lo que ocurre a nivel internacional. ¿No responde Facebook a lo que finalmente le exige el Estado estadounidense? ¿Cómo se financian estas empresas en los EE. UU.? Por ejemplo, con grandes proyectos estatales, militares y de inteligencia. ¿Cómo se han construido estas enormes empresas del complejo tecnológico? Insisto con esto: ¿son realmente empresas que podríamos llamar del "sector privado"? ¿Es lo mismo analizar Facebook Inc. en los Estados Unidos, que analizar el funcionamiento de esta corporación en Argentina, Brasil, Australia o Irlanda? Queda claro que no son lo mismo, operan según convenga en cada lugar, pero a la larga siempre responden a los intereses permanentes de sus Estados y casas matrices.

Aprovecho para agregar otro punto relevante y que forma parte de los cambios que estamos analizando. A esta diferencia que fuimos hablando, entre lo privado y lo público, es necesario agregarle que estas empresas tecnológicas extranjeras, cuando tocan el suelo argentino u ofrecen servicios a la población argentina, tampoco respetan la separación entre los intereses privados y públicos (ni de los EE. UU., ni de la Argentina u otro país). Es decir, tienen una lógica en su casa matriz, otra lógica de funcionamiento en la Unión Europea, por ejemplo, y otra lógica fuera de su casa

matriz. Basta citar casos históricos sobre cómo operaron Microsoft o Google Inc. en relación con el gobierno chino (a partir de los años 2000). También es posible identificar otras lógicas de funcionamiento cuando van, por ejemplo, a Rusia, o deben operar bajo las regulaciones de la Unión Europea. En realidad, tienen tantas lógicas de funcionamiento como sean necesarias para adecuarse y proteger sus intereses.

Insisto con algo que mencioné al inicio. En la Argentina todavía no vemos correctamente cómo se dan estos procesos. Interpretamos la división entre lo público y lo privado como si fuera monolítica, tajante, bajo la luz de ciertos dogmas liberales o neoliberales que no se aplican en ninguno de los lugares que estamos mencionando (sobre todo no se aplican en los EE. UU.). Pero, entonces, ¿cómo deberíamos operar con estas empresas en territorio argentino? Y, sobre todo, ¿cómo deberíamos empezar a pensar en nuestras empresas nacionales (o en industrias nacionales)?

Las empresas que manejan infraestructuras críticas deben ser argentinas, deben responder de forma directa y permanente a los intereses de la Argentina. En todo caso, si se contratan empresas extranjeras tenemos que saber bien qué contratar, qué negociar, cómo se van a gestionar los datos personales y poblacionales, los derechos intelectuales, los desarrollos tecnológicos y las asociaciones estratégicas. En la actualidad, lamentablemente, aún tenemos una baja capacidad de negociación como Estado en relación con qué tipo de empresas vamos a aceptar en nuestro territorio o qué tipo de servicios van a afectar nuestra población.

Cierro la primera parte de mi intervención reafirmando la necesidad que Argentina tiene de discutir estas problemáticas en profundidad. China, EE. UU. y Rusia invierten mucho dinero en sus propias empresas, las hacen crecer y las protegen durante todo su ciclo evolutivo y adaptativo. Además, las sostienen en términos un poco más serios, en términos soberanos, como parte de su territorio o patrimonio. Las empresas chinas son parte del territorio chino. Los estadounidenses entienden que los chips que te venden son parte de su territorio y así lo defienden, por ejemplo, en términos de derechos intelectuales. No hace falta entrar a ver cuestiones de banderas (como si fueran buques). La infraestructura tecnológica que procesa datos también es vista de la misma forma y, en algún momento, si no llegás a una buena negociación, te apagan la posibilidad de que utilices sus dispositivos. Esto es así hace mucho tiempo y, en lo inmediato, todo indica que se va a mantener igual.

El desarrollo tecnológico de Argentina, queda claro, solo depende de nuestras capacidades. En algún punto, son nuestras capacidades puestas en acción. De hecho, cuando miramos la historia de la informática nacio-

nal, se ven momentos altos y también grandes oportunidades que se perdieron. Hubo cosas muy interesantes que se hicieron y que se pueden recuperar. La mirada histórica para esto que estamos hablando es fundamental. Habilita otro tipo de miradas, si me permiten, en profundidad. Por ejemplo, ¿cuánto tiempo hace que los datos poblacionales de la Argentina están en manos de una gran corporación extranjera? La respuesta es que hace mucho tiempo. Hay que retrotraer el análisis al golpe de Estado de la Revolución Argentina (1966-1973), cuando se creó el Centro Único de Procesamiento Electrónico de Datos (CUPED) en 1967, que concentró los datos previsionales dentro del Ministerio de Bienestar Social. Es decir, desde ese momento los datos poblacionales estuvieron gestionados por una empresa como IBM. Se generó una alianza entre el onganiato y su acercamiento a una corporación extranjera como IBM cuando Argentina, en realidad, tenía posibilidades de volcarse a otras soluciones. El CUPED terminó siendo parte de lo que hoy es ANSES. Por lo tanto, hace mucho tiempo que la gestión de datos poblacionales está atada a la gestión de empresas extranjeras.[8] Está claro que esto no lo vamos a resolver fácilmente, o de un día para otro. Tenemos que charlar un rato largo sobre qué políticas convienen y analizar a 5, 10 y 15 años, como mínimo, y pensar cómo vamos a generar nuestros posicionamientos sobre los datos que gestiona el Estado y, entre otros, el tratamiento de datos personales y poblacionales en Argentina.

Retomemos aquí el tema de las tecnologías críticas. La regulación de Internet no solo es posible, sino que además es deseable. Esa cuestión de que Internet se autorregula es un cuento estadounidense. No podría ser un cuento chino porque ellos sí supieron perfectamente cómo regularla. Y, entre otros países, los rusos también lo hicieron muy bien. La han regulado protegiendo sus industrias, sus empresas, y hoy en día están en una situación de desarrollo nacional impensado para quienes seguimos estos temas hace más de 20 años. Nadie se imaginó que las críticas que les hacían Google y Microsoft a la política de Internet china ("gran muralla china", falta de libertad de expresión, censura, gran cortafuegos) iban a redundar en fuertes políticas públicas, con empresas poderosas y con una competencia extraordinaria por parte de los chinos en el mercado internacional. Yo no me lo imaginé. Los chinos no solo se lo imaginaron, sino que lo lograron y fueron consecuentes con sus intereses. Los estadounidenses dieron batalla

8 Al respecto se puede revisar el libro de Fondevilla, Laguado Duca y Cao (2007), y el capítulo de Bianculli y Vercelli (2022) "Las historias de la informática argentina: una aproximación desde las alianzas socio-técnicas".

desde el primer momento (la puja entre ambos viene de larga data). Y, citando otros ejemplos de relevancia, hace pocos años los rusos lograron, a través del fortalecimiento de la RuNet, desconectarse de Internet y disminuir su dependencia de una conexión externa para el funcionamiento de sus servicios críticos.[9]

¿Este es nuestro horizonte? Sí, con certeza. Este es, claramente, nuestro horizonte, aunque no lo logremos de inmediato. Tener la posibilidad de desarrollar infraestructura propia, poder desconectarse de los cables de Internet y que nuestros servicios críticos sigan funcionando sin mayores problemas es uno de los objetivos que tenemos que poder alcanzar en un tiempo prudencial. Sería un gran paso para proteger los intereses soberanos. Esto tenemos que poder planificarlo y concretarlo. A la Argentina le faltan buenas políticas a mediano y largo plazo. Y no es de ahora, es un patrón repetido en la historia de la informática nacional. La alternancia de gobiernos, en algunos momentos, nos deja mal parados, sobre todo cuando asumen gobiernos que entienden que el Estado no sirve para nada y lo mejor que se puede hacer es desguazarlo. Ahí tenemos un problema, porque la continuidad de estas políticas a largo plazo se ven seriamente afectadas.

Es decir, para desarrollarnos también vamos a necesitar buenas políticas nacionales sobre el ciberespacio (esta es otra de las esferas sobre las que estamos trabajando). Recuerdo siempre que Raúl Zaffaroni hace unos años pedía que, luego del último desastre neoliberal, el próximo gobierno planteara de forma inmediata una reforma constitucional donde, entre otros temas centrales, se cierre la posibilidad del endeudamiento externo. Este punto es crítico y urgente. Cuando se habla de independencia económica se tiene que poder observar que hoy la deuda es para nosotros la imposibilidad de tener políticas soberanas. Y es también la imposibilidad de tener una política soberana en términos tecnológicos. La deuda es un

9 Más información en el texto *Regulaciones en el ciberespacio: reconsiderando la soberanía tecnológica* (Vercelli, 2020) donde se describe la experiencia rusa RuNet: "El 1 de noviembre de 2019 entró en vigor la ley sobre el funcionamiento de la Internet rusa, orientada a garantizar la seguridad y la sostenibilidad de los servicios de Internet en el caso de desconexión de la red global. La ley busca proteger la RuNet de potenciales agresiones externas y garantizar el funcionamiento ininterrumpido de todos los servicios esenciales. La normativa obligó a todos los proveedores de Internet en Rusia a instalar equipos especiales (proporcionados gratuitamente por el gobierno). Entre el 16 y el 23 de diciembre de 2019 se realizaron las pruebas bajo el nombre 'Internet soberano' (medidas orientadas a conseguir un normal funcionamiento de la red rusa ante desconexión de Internet, desastres naturales o amenazas / peligros provenientes del exterior). Las pruebas analizaron la estabilidad y la seguridad en el tráfico de información, la Internet de las cosas, la telefonía móvil y la protección de datos personales".

lastre que nos impide utilizar nuestras fuerzas productivas para el desarrollo nacional.

La Argentina está herida a partir del endeudamiento y la fuga. Algunas empresas ganan en los momentos en donde tenemos gobiernos más cercanos a los intereses populares, pero también ganan cuando se está desmantelando el Estado. Digamos, en términos más económicos: ganan con la cuestión financiera (endeudamiento, bicicleta, fuga, etc.) y también con la reprimarización de nuestro sistema productivo e inhibiendo toda posibilidad de desarrollo industrial. Por ello, es importante resaltar que, cuando tengamos que planificar nuestra industria y nuestras empresas nacionales (sean éstas 100% del Estado, mixtas o 100% privadas), es necesario que estas empresas no solo sean argentinas, sino que también respondan a los intereses nacionales, a los intereses de toda la población argentina. Las políticas que se deben implementar tienen que estar orientadas en este sentido. Y estos temas tienen que estar identificados, abiertos y sobre la mesa para discutirlos.

¿Nos transformamos en grandes herejes por pensar nuestro desarrollo de esta manera, por pensar estas cuestiones? Claro que no. Esto mismo que estamos charlando es lo que implementan los chinos, los rusos y lo que celosamente cuidan los estadounidenses de su impresionante industria. Sus empresas responden a los intereses nacionales y forman parte de la planificación estatal a largo plazo. Si dejamos de escuchar lo que dicen (lo que "nos venden", su ideología, su propaganda) y miramos mejor qué es lo que realmente hacen, creo que aprenderemos mucho más. Les invito a que miremos con atención y analicemos qué es lo que realmente hacen con sus empresas tecnológicas y cómo las gobiernan en sus territorios y a nivel global.

Por ello, y estrechamente vinculado a lo que venimos analizando, la segunda idea que me parece central resaltar es que Argentina necesita demarcar de forma clara lo que queda dentro de sus fronteras y lo que queda fuera. Esto es fundamental. Al inicio hablamos sobre las dificultades de delimitar el ciberespacio en términos soberanos. Y una cosa es entender cómo se construye valor en forma distribuida y otra distinta es tomar decisiones políticas sobre su infraestructura nacional. Nosotros necesitamos delimitar qué es lo nuestro (en términos nacionales y regionales) y qué es lo de otros. ¿Cuánto tiempo necesitamos para esto? El menor tiempo posible. En el plano internacional estas discusiones inhiben que algunos países, como la Argentina, puedan construir políticas adecuadas y convenientes sobre el ciberespacio nacional. No es que al final somos todos torpes y no sabemos lo que tenemos que hacer. En el plano interna-

cional, es claro, no encontramos una llanura para la negociación, sino que nos topamos con un pantano. Sepamos que el escenario internacional es de conflictos varios, una especie de guerra tecnológico-económica que es la continuidad de otras situaciones conflictivas a través de foros y organismos internacionales.

Este mismo escenario es compartido con otras tecnologías asociadas y complementarias al ciberespacio. Si observamos los avances en materia de inteligencias artificiales, se advierte que estos desarrollos llegan a la Argentina completamente cerrados, *cajanegrizados*, con medidas tecnológicas de protección, como tecnologías opacas, con imposibilidad de analizar su funcionamiento y sin transparencia alguna. Esto se agrava ya que, como ocurre en el plano internacional, a muchos en la Argentina se les ocurrió que era una buena idea discutir sobre la ética y no sobre las políticas y las regulaciones de las inteligencias artificiales. ¿Podemos discutir sobre ética? Sí, claro, pero en ningún caso podemos dejar de debatir y dar prioridad a las políticas nacionales, a las regulaciones y al desarrollo de nuestra industria frente a cambios tecnológicos tan importantes.[10]

Incluso, por tomar otro tema sensible y urgente, el poder de la computación cuántica puede hacer que algunas apuestas nacionales dejen de tener sentido. La computación y la internet cuántica que tienen desarrolladas los chinos podrían mostrar una capacidad de cómputo extraordinaria. El poder de cómputo cuántico es tan superior a la computación digital convencional que podría desnudar las formas de seguridad más elementales. Recuerdo que en la década de 1990 se decía "no hay que perder el tren", frase horrible, que nunca nos sirvió. Más cercana en el tiempo también, se usó la de "insertarnos en el mundo", otra construcción absurda. En este y otros puntos sensibles tenemos que saber posicionarnos frente al cambio tecnológico actual (y al de las próximas décadas). Está claro que para este tipo de tecnologías necesitamos ser estratégicos, saber asociarnos y ser creativos para construir nuestros propios desarrollos científico-tecnológicos.[11]

---

10 Al respecto se puede revisar la charla "Ética, política y regulación de las inteligencias artificiales" (Vercelli, 2021b), organizada por la Sociedad Argentina de Informática (SADIO), donde se discutió si la ética es un buen enfoque para analizar las IA y se presentaron casos orientados a trabajar las principales tensiones entre regulaciones e inteligencias artificiales.

11 Al respecto se puede revisar el encuentro del 16 de noviembre de 2022 del Ciclo de Conferencias 2022 del Centro de Estudios Estratégicos para la Defensa "Manuel Belgrano" (CEEPADE), titulado "La industria del *software* y la ciberdefensa", con la apertura de la Dra. Nilda Garré y las intervenciones de Jorge Zaccagnini y Ariel Vercelli (2022a).

A mí me gusta la solución que encontraron los rusos para el desarrollo de su industria. Por un lado, permiten que empresas líderes a nivel internacional –sean chinas, estadounidenses o europeas– operen en su territorio, pero exigen que cada uno de los dispositivos electrónicos que se producen para el mercado ruso (computadoras, teléfonos móviles o televisores) tenga instalado un conjunto de aplicaciones sustitutivas que provienen de empresas rusas. ¿Y qué dicen en Rusia? Que en cualquier momento puede ocurrir una catástrofe o un conflicto comercial o bélico, lo cual exterminaría los servicios de empresas extranjeras en su territorio. Por eso, a través de esta política los usuarios rusos van a poder reemplazar fácilmente y de forma inmediata los servicios corporativos originales de los artefactos por las aplicaciones rusas, dado que ya están embebidas e instaladas en los dispositivos (entre otros: navegadores, correos, sistemas operativos).[12]

Esta es una excelente medida que Argentina podría implementar para desarrollar su industria. Podría criticarse que las aplicaciones no están efectivamente en funcionamiento porque los usuarios no las usan. Sin embargo, en algún momento y bajo ciertas circunstancias, pueden pasar a ser vitales. ¿Es posible que las aplicaciones rusas no funcionen tan bien como las aplicaciones de los fabricantes o de empresas líderes? Tal vez. No conozco la calidad de estas aplicaciones, pero sí me queda claro que, aunque fueran deficientes, siempre se pueden mejorar. El otro punto clave aquí es que siempre es preferible tener algo que funciona más o menos antes que no tener nada.

En la actualidad, salvo raras excepciones, la mayoría de los artefactos tecnológicos con los que interactuamos nos llegan a través de mediaciones y redes industriales. Estas transforman el conocimiento científico-tecnológico, atravesado por el concepto de innovación (habría que ver este concepto y cuáles son los intereses que tiene detrás) y por una larga cadena de

12 En el artículo "Regulaciones en el ciberespacio: reconsiderando la soberanía tecnológica" (Vercelli, 2020) se describe la política rusa para protección de los consumidores y el desarrollo de *software* nacional para artefactos tecnológicos que circula en su territorio: "En diciembre de 2019 la Federación Rusa sancionó una reforma al artículo 4 de la Ley de protección de los derechos del consumidor vinculada a la calidad de los productos que se venden en el país. Específicamente, estableció la obligatoriedad de pre-instalación de *software* ruso (desde fábrica) en los dispositivos electrónicos que se comercializan en tu territorio. La reforma, en vigencia desde el 1 de julio del 2020, obliga a instalar *software* y aplicaciones producidos en Rusia en todas las computadoras y en los teléfonos y televisores inteligentes. Por un lado, se busca proteger los intereses de las empresas rusas (generando capacidades locales y trabajo) y, por el otro, se intenta reducir el número de abusos cometidos por corporaciones extranjeras. La regulación no excluye aplicaciones, pero sí obliga a que los dispositivos también tengan pre-instalado, por ejemplo, el navegador Yandex. Browser u otras aplicaciones (Yandex.Disk, Cloud Mail.ru, Rutube, Kaspersky o MTS)".

comercialización y usos muy diversos. Ahora bien, ¿por dónde comenzar un desarrollo tecnológico informático o computacional nacional?

Yo creo que Argentina tiene una enorme oportunidad de retomar su desarrollo científico-tecnológico e informático dentro del sistema educativo por múltiples razones. Siempre vamos a necesitar que nuestro sistema público de educación incorpore las nuevas tecnologías. Debemos invertir en tecnología permanentemente para las generaciones que vienen, en el primario y en el secundario, aunque esta tecnología no sea de punta ni con los últimos *gadgets*. Dentro del sistema educativo se pueden desarrollar tecnologías nacionales, incluso asociados con otros países de la región, que acompañen los aprendizajes y las producciones colaborativas. Hay mucho potencial para avanzar en este sentido.[13]

Otra de las grandes discusiones es dónde tenemos que alojar nuestros datos poblacionales. Nosotros, afortunadamente, tenemos ARSAT. Sin embargo, necesitamos alimentarla muchísimo más, e insisto en este punto: debemos definir tajantemente un adentro y un afuera en relación con los datos. Por ejemplo, definir: dónde queda nuestra información y dónde permanecen nuestros datos poblacionales. Recuerden lo que charlamos antes sobre el CUPED. Además, existe una enorme discusión sobre qué tecnologías comprar.

Antes comenté sobre las políticas estadounidenses que prohibieron las tecnologías chinas dentro de la administración pública de los EE. UU. Específicamente, se prohibió por decreto la compra de computadoras como Lenovo, además de la utilización de redes sociales como TikTok o WeChat (relacionada con monederos virtuales). Ellos lo llaman "sanciones económicas". Si Alberto Fernández tomara este tipo de medidas, prohibiendo, por ejemplo, la compra de computadoras HP en Argentina o prohibiendo la compra de Lenovo, creo que le dirían de todo, tanto interna como externamente. Existen muchos casos más a los que podríamos referirnos, esta enumeración es sólo un comienzo.

Finalmente, me gustaría repasar rápidamente las dos ideas centrales a las que nos referimos en esta charla. Por un lado, las tensiones vinculadas a la cuestión de lo público y lo privado. Los invito a cuestionar que las grandes empresas tecnológicas sean empresas privadas que se ubican en un libre mercado internacional (en un *laissez faire - laissez passer* o en la neutralidad de la red). Entendamos, mejor, que estas son enormes em-

13 Sobre la incorporación de tecnologías en el sistema educativo se puede leer Vercelli y Bianculli (2019).

presas de los Estados (chino, estadounidense, europeo y ruso). En este sentido, marco un punto clave: las empresas que sostengan la infraestructura crítica de nuestro país deberían ser empresas argentinas que, por supuesto, respondan a los intereses nacionales. La otra idea sobre la que trabajamos fue cómo hacemos para desarrollarnos industrialmente y, sobre todo, qué políticas tenemos que implementar en el país para superar la dependencia de tecnologías y empresas extranjeras (sobre todo para servicios críticos). Al respecto, bien podríamos preguntarnos, ¿vamos a tardar mucho en lograr esto en Argentina? Yo no tengo apuro, hay que hacerlo bien. De todas formas, a decir verdad, es preferible que sea lo antes posible y que lo empecemos nosotros.

Referencias

Assange, J. (2013). *Criptopunks. La libertad y el futuro de Internet*. Buenos Aires: Trilce.

Assange, J. (2014). *Wikileaks: When Google Met Wikileaks*. Nueva York: OR Books.

Bianculli, K. y Vercelli, A. (2022). *Las historias de la informática argentina: una aproximación desde las alianzas socio-técnica*s. En Pereira, L.; Perold, C. y Vianna, M. (Org.). *História(s) de Informática na América Latina – reflexões e experiências Argentina, Brasil e Chile* (pp. 51- 86). San Pablo: Paco Editorial.

Fondevila, P.; Laguado Duca, A. y Cao, H. (2007). *40 años de informática en el estado argentino*. Buenos Aires: EDUNTREF.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the Surveillance State*. Nueva York: Metropolitan.

Poitras, L. (Dir.) (2014). *Citizenfour* [Película]. Praxis Films; Participant Media; HBO Films.

Vercelli, A. (1 de noviembre de 2004). Corea y la ubicuidad de la información: U-Corea. *Ariel Vercelli. Tecnologías, Regulaciones y algo más…* https://arielvercelli.org/2004/11/01/corea-y-la-ubicuidad-de-la-informacin-u-corea/

Vercelli, A. (2012a, 15 de febrero). Twitter censura y se convierte en una plataforma de control social. *Télam Digital*. https://www.telam.com.ar/notas/201202/15397-twitter-censura-y-se-convierte-en-una-plataforma-de-control-social.html

Vercelli, A. (2012b, 5 de diciembre). Un hermoso rootkit (de fábrica) en tu teléfono / computadora móvil. *Télam Digital*. https://www.telam.com.ar/notas/201112/13528-un-hermoso-rootkit-de-fabrica-en-tu-telefono--computadora-movil.html

Vercelli, A. (2012c, 8 de diciembre). Otros investigadores habían alertado sobre el rootkit Carrier IQ. *Télam Digital*. https://www.telam.com.ar/notas/201112/13530-otros-investigadores-habian-alertado-sobre-el-rootkit-carrier-iq.html

Vercelli, A. (2012d, 10 de diciembre). Más que clientes, rehenes: crece el escándalo del rootkit Carrier IQ. *Télam Digital*. https://www.telam.com.ar/notas/201112/15394-mas-que-clientes-rehenes-crece-el-escandalo-del-rootkit-carrier-iq.html

Vercelli, A. (2012e, 14 de diciembre). El fabricante del masivo *software* espía intentó minimizar acusaciones. *Télam Digital*. https://www.telam.

com.ar/notas/201112/15395-el-fabricante-del-masivo-*software*-espia-intento-minimizar-acusaciones.html

Vercelli, A. (2012f, 15 de diciembre). Pack navideño todo incluido: minutos libres, sms, datos, rootkits ilimitados. *Télam Digital*. https://www.telam.com.ar/notas/201112/13534-pack-navideno-todo-incluido-minutos-libres-sms-datos-rootkits-ilimitados.html

Vercelli, A. (2012g, 21 de diciembre). Empresas de telefonía móvil cancelan contratos con Carrier IQ. *Télam Digital*. https://www.telam.com.ar/notas/201112/13534-pack-navideno-todo-incluido-minutos-libres-sms-datos-rootkits-ilimitados.html

Vercelli, A. (2020). Regulaciones en el ciberespacio: reconsiderando la soberanía tecnológica. *Revista Mugica*. https://revistamugica.com.ar/regulaciones-en-el-ciberespacio-reconsiderando-la-soberania-tecnologica-2/

Vercelli, A. (2021). El extractivismo de grandes datos (personales) y las tensiones jurídico-políticas y tecnológicas vinculadas al voto secreto. *THEMIS Revista De Derecho*, (79), 111-125. https://doi.org/10.18800/themis.202101.006

Vercelli, A. (2022b, 17 de diciembre). La guerra de los chips entre los EE. UU. y China: sanciones económicas, bloqueos y demandas en la omc. *Ariel Vercelli. Tecnologías, Regulaciones y algo más…* https://arielvercelli.org/2022/12/17/32-micro-columna-radio10mdp-universidad-residencias-y-radio-de-las-madres-la-guerra-de-los-chips-entre-los-ee-uu-y-china-sanciones-economicas-bloqueos-y-demandas-en-la-omc/

Vercelli, A. (2022c, 31 de diciembre). Twitter y su relación con la censura: la desinformación y las operaciones de inteligencia a partir de los Twitter Files. *Ariel Vercelli. Tecnologías, Regulaciones y algo más…* https://arielvercelli.org/2022/12/31/34-micro-columna-radio10mdp-universidad-residencias-y-radio-de-las-madres-twitter-y-su-relacion-con-la-censura-la-desinformacion-y-las-operaciones-de-inteligencia-a-partir-de-los-twitter-f/

Vercelli, A. [Sadio Bs As] (2021b, 22 de junio). *Ética, política y regulación de las inteligencias artificiales* [video]. YouTube. https://www.youtube.com/watch?v=G9Mo-l8Xgno

Vercelli, A. [UNDEF | Universidad de la Defensa Nacional] (2022a, 16 de noviembre). CEEPADE "La industria del *software* y la ciberdefensa" [video]. YouTube. https://www.youtube.com/watch?v=JPM_Rd9clwk

Vercelli, A. y Bianculli, K. (2019). Consideraciones para re-Conectar Igualdad. En Aguiar, D.; Capuano, A. y Vercelli, A. (Comp.). *Una política pública educativa en la era digital: El programa conectar igualdad*. Viedma: Editorial UNRN. https://www.doi.org/10.4000/books.eunrn.2417

Construcción de sentido

ALDO FELICES

Es un gusto intentar hacer un aporte en este campo, que a mi se me antoja definirlo como muy controvertido y controversial, pero a su vez atractivo, y que, al menos, me parece que provoca tensiones y tentaciones de conquistas. En definitiva, se trata de un campo por conquistar, y la construcción de sentido es un recurso inexorable para cualquier pretensión de conquista. No creo que nadie pueda aspirar a un cierto dominio sobre algún territorio si no le aporta cierto sentido, aunque sea discursivamente. Es decir, en principio, eso a lo que llamamos sentido admite la posibilidad de ser leído como un recurso discursivo de dominio.

Básicamente todo relato persigue un sentido, incluso un relato que impugna a otro también tiene pretensiones de sentido. Lo que me parece que ya no podemos tomar como premisa es la existencia de un sentido único. La verdad yo no creo que exista, contundentemente diría que no. Eso no quita que existan argumentos que sí pretenden la instalación de un único sentido (no sólo único sino también totalizante) al evitar la filtración de cuestiones diferentes de lo que ese sentido intenta sostener.

La buena noticia es que eso puede ser una pretensión, pero de ninguna manera se puede lograr un sentido único y totalizante. A veces se cree poder obtenerlo por una vía que, por mi parte, prefiero descartar. Ya voy a detallar a qué me refiero con esta vía, pero, como adelanto, diría que una vía de sentido con pretensiones totalizantes es siempre una vía sintomática. El síntoma, aunque no lo crean, está lleno de sentido, explota de sentido. En el plano discursivo, una vez que el sentido se instala en un discurso, es muy difícil contraponer argumentos. A veces me pregunto si el sentido no se solidifica a tal punto que la única vía para contraponer alguna idea, frente a tal apariencia de solidez, es la vía del absurdo. Porque el sentido se alimenta de sentidos y llega un momento en que esa voracidad se vuelve insostenible, o tiene que recurrir a forzamientos, y allí se abre la posibilidad de que alguien contraponga la vía del absurdo, a través de la cual muchas veces se evidencia la falacia del sentido con el que se construyó el discurso en primera instancia. A mí no me asusta mucho la vía del absurdo porque,

se sabe, es un recurso de la matemática, y un recurso de demostración de cuya validez nadie duda. Por su parte, la matemática tiene algunas características que el discurso corriente no posee, como la apelación a la letra. La matemática confía mucho en las letras y le va bien, no se trata de una confianza ciega ni vana. Todos pasamos por el secundario y sabemos, aunque no lo recordemos, que [y = ax + b] es la ecuación de cualquier recta en el plano. Y no hay mucho más que decir, representa todas las rectas del plano, con la pendiente que quieran, no importa, todas están representadas por esa ecuación, no se necesita agregarle más palabras. Es eso: un conjunto de letras que, articuladas, representan algo que se supone fijo y seguro. Nada que agregar, no es opinable. Esto no se puede trasladar de la misma forma a la construcción de sentido.

¿Cuál sería, entonces, el problema que afecta a la ilusión del sentido? Pues bien, el discurso corriente está hecho de significantes, por lo que la cuestión es cómo alcanzar el sentido por la vía del significante sin que esa pretensión deje un resto resistente a la significación. Me refiero a que no se puede esperar una significación cerrada a partir del uso de la palabra, porque el mismo campo simbólico de la palabra es incompleto, entonces ahí tenemos un problema para confrontar esta aspiración de lograr sentidos cerrados y totalizantes. Estos, por suerte, siempre nos dejan algún intersticio, algún hueco, un agujero por donde poder colar –y acaso contraponer– alguna otra función, aunque sea metafórica.

Nadie duda de que en algún momento –y esto no es una cuestión opinable– existió una física a la que se llamó aristotélica. ¿Qué significa eso? Que había un sentido antes de la revolución científica del siglo XVII, pero se montaba sobre un paradigma geocéntrico, es decir, era un montaje de sentido apoyado en un enorme sinsentido, en una premisa falsa. Sin embargo, lo curioso es que eso no impedía que las cosas funcionaran, a su manera, obvio, pero no dejaron de funcionar. Lo que estoy planteando es una invitación a ir por el camino de fluidificar la confianza en el sentido. No hay sentido único, no hay sentido totalizante, no hay sentido completo: las cosas funcionan en algún sentido, a pesar de que estén apoyadas en un paradigma falaz, digamos.

Ahora bien, ¿cómo funcionan estas cosas actualmente y en el ámbito que nos convoca? Bueno, en la implementación y puesta en marcha de cierta tecnología, la cuestión hoy se instala como una especie de cabecera de playa en el discurso, detrás del cual se organiza el despliegue de una supuesta y necesaria exclusividad. Lo que sigue es el verdadero desembarco, que consiste en aportar sentido a lo que se implementó tecnológicamente, al comienzo, como cabecera de playa. Una vez que el hecho se consuma, o sea, cuando el discurso recogió los efectos de las implementa-

ciones tecnológicas, es bastante poco lo que queda por hacer, porque el sentido se colectiviza y se convierte en una de las cuestiones más difíciles de desarmar. En otras palabras, se convierte en el síntoma colectivo que todos vemos funcionar en gran medida, incluso con lo no vinculado a lo tecnológico (voy a volver sobre el asunto).

¿Qué pasa cuando llevamos esto al plano de la soberanía, al plano de lo nacional y lo supranacional? Entre otras cosas, los Estados definen sus estrategias basándose en datos, o al menos eso sería lo esperable. Diría incluso que es imposible pensar en una definición de estrategia consistente sin contar con datos, de modo que la disponibilidad de datos es, de por sí, parte de la misma estrategia. Ahora bien, por algún artificio del lenguaje se logró instalar que los datos residen, viven o se alojan en la nube. Eso otorga falsas ideas de accesibilidad, como si esa nube que hace llover, y que por el momento sigue siendo de todos, pudiera alojar datos sin más y que a su vez estos resultarían accesibles, a tal punto que, si tuviéramos algo de paciencia, finalmente lloverían datos para todos. Es una cosa seria. Ahora bien, estas formulaciones se leerían muy distinto si se explicara que los datos están en servidores físicos, localizados en un lugar y replicados en otro, y que hay una dirección IP que identifica esos servidores, por lo que esa arquitectura es conocida por fulano y sultano y no por el resto. También debería explicarse que el control de acceso no es tan libre y tan público, y que los canales físicos y lógicos para el transporte de datos son propiedad de algún fulano y sultano, pero no necesariamente los mismos. Teniendo en cuenta esto, las cosas ya tienen otra connotación. ¿Y cuál sería la trampa? La trampa comienza con el uso de un significante en apariencia neutro e inocente, hasta poético: nube.

En todo caso, la infraestructura que da soporte a la navegación de internet no se parece en nada a una nube, yo no le veo ningún parangón. Los servidores, como decimos en el lenguaje informático o como llamamos en general a los componentes de *hardware*, son fierros. Los canales son físicos: cables, fibras ópticas, que van por la tierra, por el aire, láser… eso no se parece en nada a una nube. ¿Y cuál sería la cuestión de la soberanía entonces? Que soberano es quien dispone de la infraestructura y complementariamente de las herramientas de acceso y protección para esta.

Sabemos también que hay un montante lógico sobre esos componentes físicos que yo llamé infraestructura. Los programas de acceso, comunicación y protección son componentes lógicos, claramente, pero están montados sobre una infraestructura, porque no pueden soportarse a sí mismos. O sea, por más ilusión que queramos meter en esta cuestión, finalmente todo esto tiene una base física, dura.

Hace muy poco, cuando por unas horas dejaron de funcionar WhatsApp y Facebook, la pregunta que todos nos hacíamos era "¿quién podría restituir los servicios?". Evidentemente no era cualquiera, y alguno se habrá preguntado "¿qué pasó con mis datos?". ¡Ah! Y alguno quizás cayó en la cuenta de que esos datos, que uno cree propios, tan propios no son, porque había alguien que estaba intentando restituir los servicios y probablemente ese alguien también tuviera nuestros datos. La cuestión es que los usuarios no tuvimos otra alternativa más que esperar. Mientras tanto, habían quedado pendientes servicios de envío de documentación, análisis médicos, confirmación de negocios, citas amorosas, todo eso quedó en espera, aguardando que alguien restituyera las funciones. ¿No fue así? Esto evidencia, aunque en general quede disimulado, que los que disponen del acceso determinan qué, quiénes y cuándo se hacen o no ciertas cosas. ¿Es eso en sí mismo una herramienta de control, de poder? Pero ¿cómo? ¿La nube no es de todos? Evidentemente no. ¿Entonces no es nube? Evidentemente no.

Volvamos al plano de la soberanía y de las estrategias de soberanía. En ese territorio, las cosas se tornan serias. No es que las citas amorosas no sean serias, pero, por el alcance que tiene cualquier estrategia de soberanía –o la falta de ella–, verdaderamente es una cuestión seria. Nosotros estaríamos obligados a ejercer soberanía sobre la nube, ese sería el objeto. Estamos al horno si tenemos que ejercer soberanía sobre un objeto tan inmaterial, muy bien no nos va a ir. Yo me permití modificar una frase de Lupercio de Argensola, que decía: "ese cielo azul que todos vemos, ni es cielo ni es azul". Yo le agregaría que ni es de todos. Si la nube es el término que aloja aquello de lo que estamos hablando, hay que salir rápidamente de esa pésima metáfora. El significante para utilizar es "infraestructura" y ella, claramente, no es de todos. Fíjense a las equivocaciones que nos puede llevar la musicalidad poética que tiene ese significante "nube".

Con el significante "ciber" no pasa algo muy diferente. No es tan poético, pero igualmente se lleva puestas todas las significaciones, bien y malintencionadas. Además, hay otra trampa: si yo tuviera que desarrollar un concepto a partir de "ciber" se haría muy difícil, por lo difuso que resulta. En todo caso, es un prefijo. Por otra parte, y mientras tanto, aquello con lo que se lo complementa sirve para el despliegue, en general, de un concepto. Y un concepto cualquiera lo que pretende es abarcar y –la mayoría de veces– cerrar un campo de significación. Uno entiende que hay un concepto en la medida en que logra cerrar el campo de la significación. Muchas veces se recurre a ciertos forzamientos porque, en definitiva, cómo uno podría abarcar y cerrar un campo que en principio se despliega y se re-

pliega según momentos tecnológicos, instrumentales y especialmente comerciales y políticos. A lo sumo uno podría captar algo en un tiempo y un lugar, luego intentar una definición balbuceante de ese algo, pero con eso no lograría el estatuto de un concepto. Insisto: las pretensiones de cerrar una significación que persigue todo concepto se llevan mal con la dinámica de las tecnologías de la información y la comunicación (TIC) y la metonimia del significante. En todo caso lo ciber, como tal, no hace fronteras con otros territorios, más bien defiende litorales, que se supone que no son tan fijos ni definidos.

Si asumo por válidas las denominaciones de ciber y nube como significantes privilegiados de este campo al que nos referimos, lo que estoy instalando es un agujero inicial. Y una vez colocado en el origen ese agujero inicial queda expedito el camino para definir arbitrariamente el alcance de cualquier noción. Y eso es lo que pasa, ese es el punto estratégico, la vacuidad inicial de sentido promueve una enorme profusión ulterior de sentido. Uno podría decir: "bueno, entonces en conjunto se trata de un enorme sinsentido". Claro que sí, ¿por qué no?

Cuando estábamos analizando estas intervenciones y tratábamos de organizar nuestras exposiciones, me atreví a proponer que aquello que Oscar Niss tituló como el Ciclo Evolutivo del Ciberespacio, encuentra en la banda de Mohebius, quizás, la presentación más adecuada para esto que estoy diciendo ahora. Intencionalmente o no, lo que digo recoge nociones planteadas por Ariel Vercelli y seguramente derivarán cuestiones que podrá o no recoger el siguiente expositor y así sucesivamente, en un recorrido que va a intentar alcanzar la totalidad de nociones, en una superficie que es a su vez única y provoca efectos diferentes en cada sujeto. Si el año venidero tuviera que organizar una exposición de este tipo y sobre este mismo tema, el contenido va a ser necesariamente distinto, aunque no tiene por qué ser contrario, ya que el recorrido de los temas relacionados, por el solo hecho de recorrerlos, cambian las expectativas de un nuevo abordaje. Sí, ya pasé por ahí, pero soy distinto, precisamente por ya haber pasado.

¿Qué me interesa remarcar? Que este efecto de significación, tan dinámico y tan cambiante, se va a dar aún cuando intentemos ceñirlo, procuremos congelarlo o solidificarlo. El objeto que nos ocupa será cambiante y dinámico, aún cuando no interpongamos ninguna intencionalidad política o comercial. Es decir, se trata de una especie de destino inexorable de indefinición, más allá del conjunto de personas del que se trate y de sus aportes bien intencionados.

Un territorio como el señalado siempre está expuesto al sesgo de las buenas y de las no tan santas intenciones, y ambas definen el campo en

cuestión permanentemente. Entonces, si esto es así, si tiene esa laxitud que acabo de describir, ¿qué se puede hacer? Y, entre otras cosas, intentar desmitificar los pilares sobre los que se soporta el discurso arbitrario y dominante. Interrogarlo es el primer gesto para cualquier intento de desmitificación. Una estrategia contundente es denunciar el sin sentido, porque la mitificación casi siempre es una acción que pretende obturar una falta en el origen, esa vacuidad del sentido inicial a la que hacía referencia. Cuestionar el prefijo "ciber" puede colaborar para hacer desvanecer el mito, no sé si para hacerlo caer, pero sí para ponerlo en cuestión y, en todo caso, seguramente a ese gesto le seguirá un intento por llenarlo semánticamente y dejarlo estancado en otra significación, que a su vez también necesitará ser interpelada.

Una pregunta interesante, por lo menos para mí, es saber desde qué discurso intentaríamos leer los efectos de significación. Para el tema que nos ocupa se podría hacer una lectura orientada a la confluencia, no forzada, sino más bien histórica. Me refiero a un maridaje político-comercial. Y no estoy pensando en un orden de privilegio de una cosa sobre la otra: esta desmitificación que propongo apunta a limpiar un territorio discursivo y abonar la posibilidad de implantación de nuevos significantes que den el soporte que nos interesa. Sí, también apelar a acciones interesadas, por supuesto que serían interesadas. Las nuevas definiciones que podamos arreglar estarán tomadas por el sesgo del interés, porque en términos de soberanía hay interés y tiene que haberlo. Pienso que se pierde soberanía cuando se pierde participación en el discurso, por eso estoy haciendo tanto hincapié en que ocupemos un lugar en el discurso. Más aún, es en el territorio discursivo donde libran las grandes batallas culturales. Lo que estoy tratando de aportar ahora va en esa dirección y en ese sentido (estoy en la teoría de vectores). ¿No?

Vuelvo al prefijo ciber, rescato ese carácter demasiado impreciso para establecer un contorno de significación y pensarlo como una referencia firme, común. Sabemos que ese prefijo está ahí en el argot tecnológico para servirse de él y hacerlo significar lo que cada quien pretenda. Cada uno completa ciber con otra palabra y se obtiene una derivación, "ciber tal cosa, ciber tal otra". El resultado, la musicalidad de esa combinación, por lo general luce, como mínimo, importante, tan importante como opaca, pero las palabras no son inocentes, ni impolutas: siempre están ligadas a una intención. ¿De qué se trata? De que es en el marco de este momento cultural que deberíamos iniciar la acción por despejar la opacidad ciertas cuestiones que están intencionalmente ligadas a significantes y que, por su prevalencia, generalmente terminan disimulando la necesidad de justificar

la evidencia de ese mismo alcance. Rescato una frase que alguna vez leí y siempre me acompañó para estas cuestiones: "autorizarse a pedirle a la evidencia que se justifique". Y, como en la mayoría de las cuestiones dificultosas, el objeto involucrado tiene un carácter decisivo, participa de un modo determinante, hasta me animo a plantear que ciertos objetos invierten la relación de dominio y en vez de ser el sujeto quien domina al objeto, termina por ser el objeto quien domina al sujeto. Vale pensarlo, esto se ve muy comúnmente y más en este ámbito.

En el tema que estamos planteando el objeto en cuestión se presenta como indómito en un doble sentido: en el de resistir su dominio y en eludir cualquier intento de demarcación. O sea, es un objeto que no se puede dominar, o que el dominio no está a nuestro alcance, y que a su vez es difícil de demarcar. Ya todos sabemos que surgen dificultades cuando uno intenta controlar algo que no es detectable, medible. ¿Entonces qué ocurre? Se presenta lo virtual y lo real como un par antitético, como un binario cerrado: o es virtual o es real. Esta formulación complica la cuestión innecesariamente, para mi lectura es una torpeza decir que si no es virtual es real. En todo caso, eso que llamamos virtual es un semblante etéreo de algo que no es. Este objeto al que estamos apuntando es a su vez virtual y real, se soporta sobre algo físico que opera detrás, debajo. Está acá cerca, no allá en quién sabe dónde.

Se nos pierde de vista que hay varios tipos de espacios, estamos muy acostumbrados al espacio euclídeo, pero nosotros deberíamos leer el comportamiento de los objetos según el espacio en el cual intentamos estudiarlos. El ciberespacio puede o no ser planteado como un nuevo espacio, lo que pasa en él es que cualquier objeto luce como virtual y para mí el desafío sería aprehender el objeto sin perder de vista el esquema físico en el cual se despliega. Hay una matriz que tiene un nombre concreto, al principio a Internet se lo conocía como red de redes y en esa referencia la cosa era más simple. Claro, el poder metafórico de la palabra nos llevó a hablar de nube, entonces ahí, como decíamos antes, depositamos cuanto imaginario haga falta, insisto, pensando en algo que queda "detrás de", "encima de", "perdido en" y cualquier excusa que apunte a opacar la transparencia, digamos. ¿Y qué pudo haber pasado? Es bastante simple, se convirtió en un medio privilegiado y, como tal, en el mensaje mismo, y entonces todo lo que por allí circula luce interesante y enigmático a su vez, ese es el estado actual del monstruo que todos alimentamos sin solución de continuidad.

Hay algo que sostengo, pero no lo pienso desde ahora, sino que en realidad es parte de una acción diría militante: en cuestiones de tecnología la desmitificación siempre ayuda, como mínimo, a establecer perspectivas

más sanas de acceso, uso y apropiación, desde otra mirada. En definitiva, tratando de ser menos alcanzados o tomados por el síntoma, con perspectivas menos sintomáticas.

Oscar Niss siempre pone especial énfasis en la necesidad de establecer un marco, cosa que a mí me parece una aspiración también necesaria y a su vez lícita, porque de alguna manera hay que acotar la dispersión que promueve este tipo de temas que tratamos hoy. La soberanía misma supone una jurisdicción, es decir, la definición de un objeto sobre el cual aplicar un decir jurídico. Si la nube es ese objeto que se instaló en el imaginario colectivo, no es muy identificable, entonces el contorno sobre el cual aplicar las normas y establecer derechos y obligaciones se vuelve difuso. La nube siempre acerca la sensación de un espacio ilimitado, la perspectiva de un objeto móvil, por eso decía que no es lo mismo decir nube que decir redes, infraestructura, conexiones, conectividad. El solo hecho de tener que definir un marco nos enfrenta con una dificultad, precisamente la definición del objeto a enmarcar. El nuestro se presenta como un objeto indómito, y lo será en alguna medida para muchos de nosotros. No hay nada más alejado de la realidad en el plano objetivo, puesto que hay dominios sobre ese objeto. Hay dominio sobre las redes, sobre los datos, sobre las comunicaciones, es decir, sobre toda esa topología física y lógica. Hay dominio, por lo cual alguien tiene ese dominio. Que sea presentado como indómito es una cuestión que nosotros podemos creer o no, aceptar o no, para no llevar ésto al plano de la creencia, pero siempre es un buen recurso apelar a la precisión de la nominación. Se trataría de perfilar objetos más reales y menos imaginarios, en todo caso, y parece ser que la definición de un marco colaboraría para esta pretensión de denominación, porque un marco sería como un encuadre y este a su vez sería la referencia necesaria de la nominación y entonces sí, con objetos nominables y con un marco que los contenga, podríamos aspirar a una confluencia de sentido. No sería un sentido único, pero sí propio, lejos de la actual dispersión de sentidos que se pretenden únicos pero no lo son, aunque esa aspiración se renueve. Por el momento no son únicos ni propios, pero tienen propietarios.

Tenemos pendiente la tarea de delimitar estos objetos parciales con un encuadre, sin perder de vista que se trata de objetos aceptados, utilizados y que forman parte de discursos diferentes (jurídico, tecnológico, social, académico). Por supuesto, sí, por esa red circulan significantes y contenidos que no tienen propiedad única ni exclusiva. Ahora bien, ¿qué ocurre si no nos decidimos a abordar esa convergencia? Ocurre lo que ya está ocurriendo y que de alguna manera motiva estos encuentros: prevalecen los discursos sociales y políticos con una alternancia entre uno y el otro. No

estoy pretendiendo supremacías, pero ambos discursos, por definición, tienen pretensiones de sentido y eso en sí es lícito. No estoy cuestionando la licitud de esas operaciones, lo que sí digo es que, aunque sean lícitos, el discurso político y el del mercado podrían someterse a la lógica de una conveniencia o no, porque ni lo político ni lo comercial son malas cosas *per se*, sino que es el marco de la incumbencia lo que le otorga un estatuto de conveniente o no.

Insisto: el discurso necesariamente aspira al sentido y no es el sentido del discurso lo que hace que sea aplicable tal o cual política, sino cómo ella afecta los objetos parciales que dan sentido al encuadre previamente definido. Dije previamente definido, ahí me tomé una enorme licencia, porque cuando el objeto es opaco y etéreo, lo habíamos dicho, es difícil de encuadrar. Por otra parte, sin un marco no se puede pretender ningún tipo de normalización del objeto. ¿Se entiende la trampa? Si yo pretendo un tratamiento normalizado del objeto voy a necesitar un encuadre, pero para tener objetos normalizables tendría que despojarlos de esa opacidad de significación, entonces la tarea es doble y simultánea: desmitificar los objetos y en la misma medida definir el marco referencial. Así, ambas cosas podrían alimentarse mutuamente, entrarían en relación.

Finalmente, quería referirme a una cuestión que tal vez les resulte curiosa, aunque a mí, ya a esta altura del ejercicio profesional del psicoanálisis, no me resulta tan curioso. Hay dos cuestiones que desbordan de sentido: una es la religión y la otra es el síntoma. En este sentido, existe un problema mayor, que ocurre cuando el síntoma se hace colectivo y entonces es muy difícil desarticularlo. ¿Alguien vio que alguna vez un síntoma colectivizado remita por sí mismo? Al contrario, se hace resistente a la remisión, el síntoma colectivizado se solidifica. La tarea no es fácil, pero hay que empezar.

Soberanía y ciberespacio

JULIÁN DI CÉSARE

Introducción

Muchas gracias, buenas tardes. La temática que vamos a intentar abordar hoy está vinculada a la soberanía y el ciberespacio, en el marco del Ciclo Evolutivo del Ciberespacio. En función de ello, me gustaría empezar retomando algunos de los conceptos que Aldo Felices esbozó en su presentación preliminar en relación con la construcción de sentido.

Aldo hizo una mención interesante respecto de la necesidad de establecer un marco para pensar estos temas. Definió "marco" como "un encuadre necesario para nominaciones, para la confluencia de un sentido, no único, pero propio" y mencionó que, frente a la ausencia de estos marcos propios, priman marcos políticos y comerciales que no necesariamente responden a nuestra conveniencia u objetivos. Basándonos en esas primeras aproximaciones que Aldo dio y considerando que, en esa construcción de sentido vigente –asumida– que a veces utilizamos para el ciberespacio se acuñan conceptos como el de nube, que soslayan o enmascaran la realidad material que lo sostiene, trataremos de evaluar algunos de los tópicos centrales para construir un marco de análisis propio que, obviamente, en temas tan amplios como soberanía y ciberespacio, será incompleto, unas primeras aproximaciones. Sin embargo, no dejará de ser un intento de avanzar en pos de una construcción propia de sentido, orientada a pensar qué rol juega la infraestructura del ciberespacio, es decir, su realidad material, y cómo se vincula con la soberanía.

En función de ello, y considerando la complejidad de la temática, me pareció interesante comenzar representando cada uno de estos conceptos –ciberespacio y soberanía– a partir de conjuntos integrados por algunos de los elementos que los componen o comprenden. Estos elementos fueron elegidos arbitrariamente con el objeto de demarcar los límites y puntos de apoyo necesarios para la construcción de nuestro marco de análisis. Buscaremos entonces, a partir de esta representación, escrutar el área de inter-

sección donde ambos conjuntos se superponen y sus elementos constitutivos interactúan.

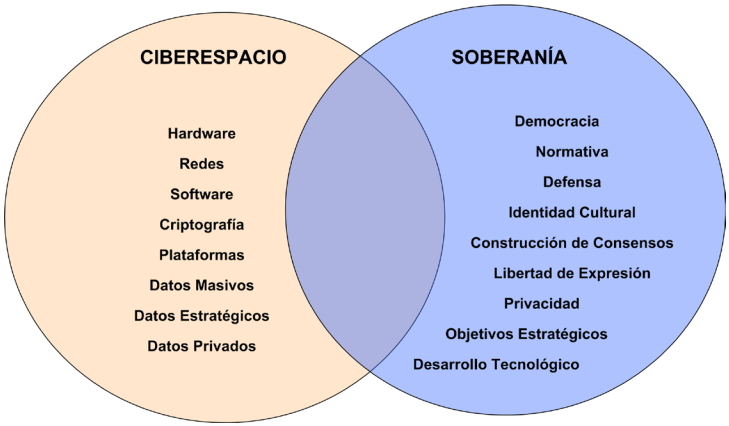
En el caso del ciberespacio, apuntaremos al conjunto de elementos materiales que lo constituyen o soportan, es decir: *hardware*, *software*, redes, cables submarinos de fibra óptica, criptografía, plataformas tecnológicas, datos masivos, datos estratégicos y privacidad de los datos.

Por otro lado, podríamos pensar la soberanía como un conjunto de elementos a través de los cuales esta se materializa mediante su ejercicio. Desde esta perspectiva, podemos construir el concepto de soberanía a partir de elementos como la democracia y la posibilidad de elección de los representantes gubernamentales sin la intervención de terceros actores. Otro elemento es la normativa, es decir, la posibilidad de que un Estado pueda, a través de normas, definir algunos aspectos del ciberespacio dentro de su ámbito soberano o sobre la tecnología que se utiliza. Al vincular el concepto de soberanía con defensa, diremos que el ciberespacio es considerado actualmente un dominio[1] más sobre el cual se dirimen los intereses estratégicos de los Estados y la geopolítica en general. A su vez, el ciberespacio, a través de plataformas y redes sociales, cataliza los procesos de formación de identidad cultural y construcción de consensos. Surgen entonces nuevos desafíos vinculados a estas plataformas digitales de comunicación, desde el punto de vista de la soberanía y el real ejercicio de la libertad de expresión y la privacidad de los datos. Asimismo, hoy la vida moderna se encuentra íntegramente atravesada por el ciberespacio. En mayor o menor medida, todas las actividades que desarrollamos tienen alguna vinculación con él y es por ello que el ejercicio de la soberanía en el ciberespacio de cualquier Estado nación deberá velar por asegurar el normal desarrollo de estas actividades para sus sociedades.

El último elemento que hemos seleccionado para conformar el conjunto de conceptos sobre los que analizaremos el ejercicio de la soberanía por parte de un Estado es el desarrollo tecnológico. Un nivel de desarrollo tecnológico determinado nos permitirá, como Estado, tener mayor o menor incidencia o pretensiones soberanas en el ciberespacio.

Ahora bien, así conformado, este ciberespacio se encuentra *compartido* por todos los Estados. Los Estados nación tienen participación en él. Poseen, controlan o utilizan determinadas tecnologías, se nutren y construyen

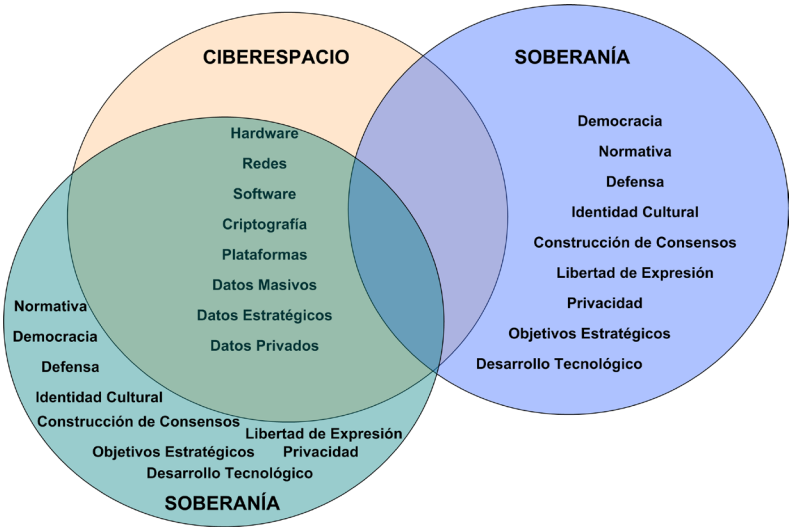
1 Para los lectores poco familiarizados con la temática, son considerados dominios convencionales para el ámbito de la defensa: la tierra, el mar, el aire y el espacio. El ciberespacio ha sido recientemente incorporado como quinto dominio, transversal a los anteriores.



con ellas y toman decisiones soberanas sobre estas, decisiones cuyo alcance dependerá de sus posibilidades materiales vinculadas al ciberespacio.

Bajo esta perspectiva, el espacio de conflicto en la intersección entre soberanía y ciberespacio –desde mi percepción, claro– se hace manifiesto al observar que no todos los Estados tienen la misma posibilidad de injerencia sobre este último. Es decir, cuando existe un Estado cuyas pretensiones de soberanía en el ciberespacio pueden verse afectadas pero su capacidad de acción sobre este se encuentra lejos de permitirle establecer normas que regulen cuestiones vinculadas a él. Se debe tener en cuenta, además, cuando existen terceros Estados con un nivel de desarrollo tecnológico y capacidad de acción que le otorgan una posición hegemónica en el ciberespacio, al poseer sobre su territorio empresas que son dominantes o piezas fundamentales de la infraestructura que lo sostienen y cuyas decisiones soberanas afectan el espacio de intersección con aquellos Estados previamente mencionados, meros usuarios de dichas tecnologías.

Estos intereses soberanos contrapuestos tienen, desde esta perspectiva, un importante nivel de solapamiento. Las decisiones soberanas de un Estado sobre el ciberespacio pueden influir, entre otros, en el *hardware*, las redes, las rutas de la información, los protocolos, el *software* o la criptografía que se utiliza, de modo que puede afectar también las pretensiones de soberanía de otro Estado. Este es, a mi entender, uno de los dilemas más importantes que tenemos en la actualidad asociado a la soberanía y el ciberespacio y que se encuentra en plena discusión. En función de lo expuesto, consideraremos en adelante esta intersección como nuestro espacio de conflicto para el ejercicio de soberanía vinculada al ciberespacio.



Agenda

Luego de esta presentación introductoria del problema, me gustaría ahondar en esta problemática mediante el desarrollo de la siguiente agenda. Comenzaremos con una breve evolución temporal del ciberespacio, para analizar el contexto histórico de su desarrollo, focalizándonos en la descripción del ciberespacio constituido fundamentalmente por tecnología militar de uso civil. Los sistemas de cómputo digital surgieron en el ámbito militar. La interconexión de las redes creció también al interior de sistemas de defensa y particularmente la criptografía fue una herramienta restringida a dicho ámbito. Asimismo, el *software* en la actualidad da lugar, para aquellos que estamos más familiarizados con la temática de ciberdefensa, al desarrollo de herramientas para los sistemas de defensa –ciberarmas– utilizadas para la consecución de objetivos estratégicos. Tanto las vulnerabilidades como la explotación de estas, hoy por hoy, ocupan un rol importante en este ámbito.

Avanzaremos luego sobre el almacenamiento masivo y análisis de datos, que constituyen actualmente otro de los territorios conceptuales en disputa, debido a los efectos que producen en las decisiones soberanas de los Estados, la privacidad y las libertades individuales. En relación con este último punto, vamos hablar de algunos acontecimientos históricos que de-

finieron las regulaciones que afectan la disponibilidad y el tratamiento de datos masivos en las redes digitales.

A continuación, para ir pensando en la próxima charla, que estará vinculada a normativa, hablaremos sobre cómo algunos países están comenzando a generar un marco normativo y tecnológico que les permita alcanzar sus pretensiones de soberanía en el ciberespacio, buscando que estas se materialicen en este ámbito que de por sí es complejo.

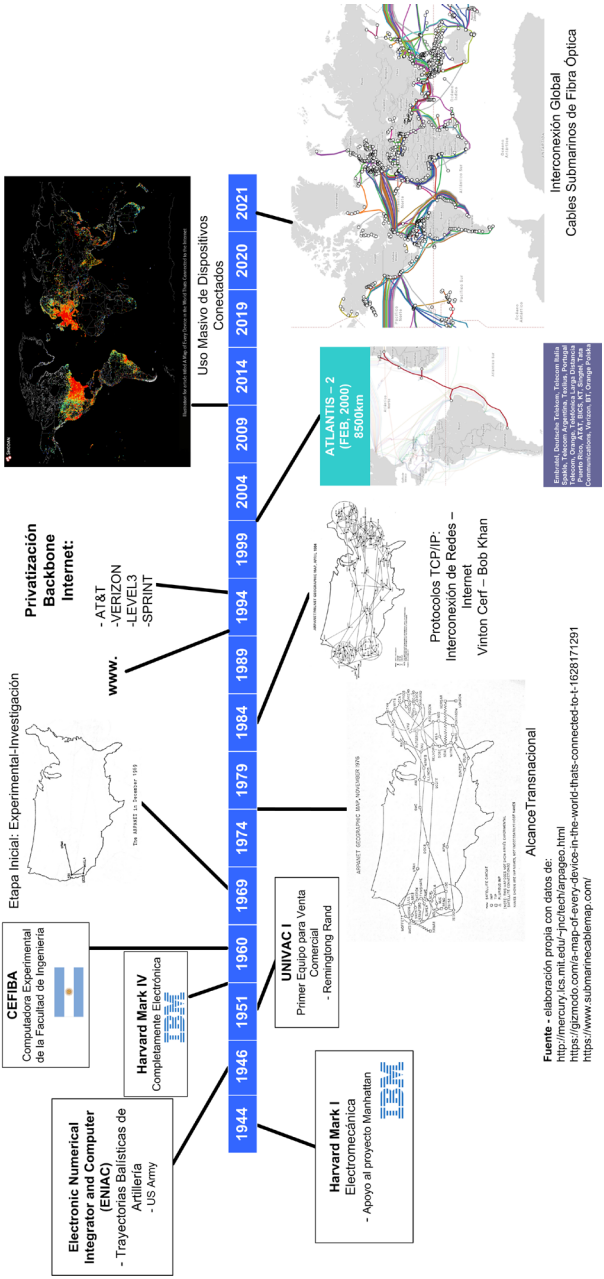
Finalmente, el último punto que desarrollaremos estará centrado en destacar algunos aspectos de nuestro país que podrían ser utilizados como herramientas para pensar tanto en la normativa como en el desarrollo nacional de tecnología, con miras a mejorar nuestras capacidades soberanas en el ciberespacio.

Breve evolución temporal del ciberespacio: tecnología militar de uso civil

Vamos a comenzar con la primera parte de la charla, abordando el concepto de ciberespacio a partir del desarrollo de sus elementos constitutivos como tecnología militar de uso civil. Para ello, buscaremos apoyarnos en un breve análisis de su evolución temporal. Si bien elaborar una línea temporal del ciberespacio resultaría pretencioso para una charla de cuarenta y cinco minutos, intentaremos mencionar algunos hitos fundamentales que nos permitan establecer un marco de referencia para los puntos subsiguientes y ahondar en el desarrollo del presente.

Sistemas digitales de cómputo

Como puede observarse en la figura siguiente, los sistemas de cómputo digital (*hardware* y *software*) fueron desarrollados en el ámbito militar, en un proceso que se inició durante la Segunda Guerra Mundial. En aquel entonces (1944), esta fue concebida como una tecnología de apoyo para el proyecto Manhattan, con objeto de facilitar el conocimiento de las condiciones de criticidad que permitieran el desarrollo de armamento nuclear, como así también para el cálculo de las trayectorias de misiles balísticos. Sobre este punto, no debe soslayarse que la tecnología nuclear caracterizó


BREVE EVOLUCIÓN TEMPORAL DEL CIBERESPACIO
1944
1946
1951
1960
1969
1974
1979
1984
1989
1994
1999
2004
2009
2014
2019
2020
2021
Electronic Numerical Integrator and Computer (ENIAC)
- Trayectorias Balísticas de Artillería
- US Army
Harvard Mark I
Electromecánica
- Apoyo al proyecto Manhattan
Harvard Mark IV
Completamente Electrónica
CEFIBA
Computadora Experimental de la Facultad de Ingeniería
UNIVAC I
Primer Equipo para Venta Comercial
- Remington Rand
Etapa Inicial: Experimental-Investigación
Protocolos TCP/IP:
Interconexión de Redes – Internet
Vinton Cerf – Bob Khan
www.
Privatización Backbone Internet:
- AT&T
-VERIZON
-LEVEL3
-SPRINT
Uso Masivo de Dispositivos Conectados
ATLANTIS – 2
(FEB. 2000)
8500km
Interconexión Global
Cables Submarinos de Fibra Óptica
Alcance Transnacional
Fuente - elaboración propia con datos de:
http://mercury.lcs.mit.edu/~jnc/tech/arpageo.html
https://gizmodo.com/a-map-of-every-device-in-the-world-thats-connected-to-t-1628171291
https://www.submarinecablemap.com/

el siglo pasado y definió, de algún modo, las capacidades de negociación en materia geopolítica que aún existen hoy.[2] En este sentido, esos sistemas de cómputo digital surgieron junto con aquella tecnología crucial y fueron gestados dentro de la órbita militar con financiamiento público y empresas privadas que participaron en su construcción.

Redes de datos

Para abordar este punto, debemos retroceder en el tiempo y pensar que los sistemas de cómputo digital solían ser sistemas muy voluminosos, algo muy diferente de los sistemas de producción masiva que hoy conocemos. Es decir, había pocos y se encontraban en lugares estratégicos. En tal sentido, la interconexión de estos permitió establecer enlaces entre instituciones estratégicas dentro del ámbito de la defensa. El objetivo de interconectar estos dispositivos digitales en red, entre otros, se hallaba vinculado al contexto imperante durante la Guerra Fría y la posibilidad de que un ataque externo sobre el territorio propio destruyera la infraestructura de comunicaciones estratégicas. En este sentido, la interconexión de sistemas digitales de cómputo a través de redes de datos buscó, inicialmente, generar un sistema resiliente de comunicaciones que permitiese, en caso de interrumpirse un enlace, disponer de muchos otros alternativos para la transmisión de la información.

Ya en 1984 se propone, a través del protocolo TCP/IP, no solo conectar dispositivos individuales, sino también conectar redes de dispositivos entre sí. En otras palabras, generar una red de redes, que es como conocemos hoy Internet. Para ese entonces, la tecnología aún pertenecía al ámbito de la defensa y la investigación, no era tecnología dada a publicidad o comercial. Sin embargo, los niveles de integración de los componentes y la capacidad de producción masiva de los sistemas de cómputo digitales hicieron que estos equipamientos mostraran una veta comercial de gran potencial, generando un mayor interés del sector privado por su explotación.

2 [Nota del Autor] Los países que aún hoy conforman el Consejo de Seguridad de Naciones Unidas, únicos miembros con capacidad de veto, coinciden con los primeros cinco países capaces de realizar detonaciones nucleares exitosas: EEUU, URSS, Inglaterra, Francia y China cronológicamente.

En la década de 1990 comienza entonces la privatización del *backbone*[3] de Internet. Es decir, empiezan a participar empresas privadas en la interconexión de sistemas digitales para dar lugar a Internet como la conocemos hoy. Aparece también el protocolo "http", uno de los tantos protocolos que se utilizan para la comunicación digital y que luego fue el más utilizado por años[4] al posibilitar la navegación web. Nace, junto con él, la denominada World Wide Web.

Cerca de los años 2000 podemos destacar como hito, dentro de esta línea temporal, la llegada del primer cable submarino de fibra óptica a la Argentina. Simultáneamente, el vertiginoso tendido global de cables submarinos de fibra óptica, junto al desarrollo y la utilización masiva de aplicaciones basadas, entre otros, en alguno de los protocolos previamente mencionados, catalizó la interconexión de redes y dispositivos en red, dando lugar al ciberespacio que hoy conocemos. Actualmente observamos una enorme cantidad de dispositivos interconectados y una infraestructura que permite la intercomunicación entre ellos a nivel global. Esta infraestructura de interconexión se asienta fundamentalmente sobre cables submarinos de fibra óptica, que será el próximo elemento del ciberespacio que analizaremos.

Cables submarinos de fibra óptica

Como mencionamos previamente, el primer cable submarino de fibra óptica llegó a la Argentina en el año 2000. Los dos siguientes llegaron también a comienzos de este nuevo siglo, en 2000 y 2001 respectivamente. Pasaron luego más de 15 años hasta que llegaron los últimos cables, que son relativamente recientes. El último de estos cables llegó a la Argentina en 2020 y pertenece a Facebook y GlobeNet. Malbec, como fue denominado, comenzó a tener actividad en febrero de 2021. El anterior a este es propiedad de Google y arribó en 2018.

3 Redes troncales del sistema interconectado global.

4 Si bien aún hoy el protocolo http sigue utilizándose, este fue dando lugar al protocolo https, el cual añade una capa criptográfica para evitar la escucha de tráfico en texto claro. De allí su nombre, http Secure (https).

EVOLUCIÓN TEMPORAL DEL TENDIDO DE CABLES SUBMARINOS PARA INTERCONEXIÓN GLOBAL DE INTERNET EN AMÉRICA LATINA

ATLANTIS – 2 (FEB, 2000) 8500km	SOUTH AMERICAN CROSSING (SAC) - (Sep, 2000) 20000km	SOUTH AMERICA – 1 (Sam -1) – (Marzo, 2001) 25000km	TANNAT – (2018) 2000km	MALBEC (2020) 2500km
				
Embratel, Deutsche Telekom, Telecom Italia Spakle, Telecom Argentina, Texlius, Portugal Telecom, Orange, Telefónica Larga Distancia Puerto Rico, AT&T, BICS, KT, Singtel, Tata Communications, Verizon, BT, Orange Polska	Century Link – 3 fibras (EEUU) Telecom Italia Sparkle – 1 fibra (ITALIA)	Telxius Telefónica – Emergia (España) 4 pares de fibras 40 Gbps potencial 1.92 Tbits/sec.	Google, Antel Uruguay (EEUU – URUGUAY) 6 pares de fibras 90Tbps	Facebook, GlobeNet (EEUU - BRASIL) 6 pares de fibras 90Tbps

Fuente: elaboración propia con información obtenida de https://www.submarinecablemap.com

Si bien uno puede pensar cada cable submarino de fibra óptica en términos unitarios, lo adecuado sería considerarlos en función de su capacidad de transmisión de datos. Los últimos cables arribados al país tienen una capacidad de transmisión de datos muy superior a la de los primeros. Resulta interesante, además, observar que los primeros cables que llegaron a la Argentina eran propiedad de un consorcio de empresas de telecomunicaciones, mientras que los últimos pertenecen a plataformas digitales. Desde esta perspectiva, nos encontramos entonces frente a una importante integración vertical de dichas plataformas. Las plataformas ofrecen servicios digitales, analizan y almacenan en *datacenters* propios una enorme cantidad de datos y están avanzando sobre la infraestructura de los cables submarinos de fibra óptica. Esto puede confirmarse extrapolando nuestro análisis a escala global. Así lo muestra, por ejemplo, una nota muy interesante de *The New York Times* (Satariano *et al.*, 2019) que analiza la evolución temporal de los cables submarinos de Internet. Se observa allí cómo en 2012 prácticamente no había participación de Microsoft, Google, Facebook ni Amazon en la infraestructura global de cables de fibra óptica. Sin embargo, en 2021 más del 50% del ancho de banda global pertenecía o era arrendada por estas plataformas, tendencia que pareciera acelerarse.[5]

Es interesante pensar en este elemento central que constituye el ciberespacio desde una perspectiva de soberanía. Estas plataformas, que detentan una posición dominante, tienen, de alguna manera, un asiento geográfico determinado, están alcanzadas por alguna legislación y responden entonces a ciertos intereses estratégicos. Dada su posición dominante, tienen una capacidad muy importante de influir en lo que denominamos ciberespacio, es decir, un peso específico enorme dentro de este nuevo dominio.

Criptografía

Otro de los elementos constitutivos del ciberespacio que elegimos abordar es la criptografía. Como vimos hasta aquí, si los sistemas digitales

5 Al momento de transcribir esta charla, Google fue autorizado por el gobierno argentino a instalar un nuevo cable submarino de fibra óptica en Las Toninas. "Google instalará en Las Toninas el cable de internet más largo del mundo que llegará hasta Estados Unidos". Ver el siguiente enlace: https://www.clarin.com/tecnologia/google-instalara-toninas-cable-internet-largo-mundo-llegara-unidos_0_k9sS6zDDiV.html (consulta: agosto de 2022).

están interconectados y la información se transmite sobre cables submarinos de fibra óptica de terceros, se pierde entonces la capacidad de asegurar que aquellos no injieran sobre la misma. Se pierde, de algún modo, la posibilidad de saber qué sucede con esta información una vez en tránsito.

Dentro de los cables submarinos de fibra óptica, fluye un universo de informaciones. Información privada y personal, pero también estratégica y confidencial. Cada uno de esos tipos de datos –antes de ser información, datos en primera instancia– tienen aplicaciones, es decir, resultan de interés para terceros actores. En este sentido, una de las maneras de proteger la información estratégica –en el caso de un Estado, por ejemplo, si hablamos de soberanía– es a través de la criptografía. La criptografía es, nuevamente, una tecnología de uso dual –militar y civil– y, como tal, su desarrollo y comercialización se encuentra restringido o normado. Dentro de los Estados Unidos de América, por ejemplo, la criptografía está catalogada como munición de guerra. Es decir, si uno desarrollase un algoritmo criptográfico robusto, no podría comercializarlo sin la previa autorización del Estado. Dicha decisión estará supeditada entonces a determinados intereses nacionales. El Estado ejerce, de este modo, sus decisiones soberanas sobre tecnología que considera estratégica.

Desde esta perspectiva, resultaría importante que nosotros como país pudieramos tener cierta autonomía en la materia, ya sea mediante el desarrollo nacional de esta tecnología o mediante la capacidad de análisis para la incorporación y uso de tecnología de terceros. Al respecto, hay algunos ejemplos históricos interesantes que quisiera recordar para que sean considerados.

Hoy sabemos que el sistema criptográfico alemán Enigma, fundamental durante el desarrollo de la Segunda Guerra Mundial, fue comercializado por las potencias coloniales como herramienta para la protección de la información, luego de haber sido quebrado (Scolnik, 2014). Si los sistemas criptográficos fueron comercializados una vez comprendido el método de codificación, difícilmente una comunicación interceptada podría mantener luego la confidencialidad de los datos transmitidos.

Más recientemente, conocimos por investigaciones periodísticas que el sistema criptográfico Crypto AG –un tema extenso que nos toca de cerca, vinculado a la guerra de Malvinas– había sido desarrollado por una supuesta empresa neutral, que luego resultó no ser neutral, ya que sistemas de inteligencia extranjeros la habían adquirido de forma secreta. La información cifrada con estos sistemas durante la mencionada guerra, según comenta *Washington Post* (Miller, 2020), pudo haber sido descifrada y compartida

por sistemas de inteligencia de terceros Estados, algo que debió afectar claramente nuestras capacidades operacionales durante el conflicto.

De acuerdo con estos acontecimientos históricos, ahora sí podemos abordar eventos recientes vinculados con los estándares criptográficos utilizados en Internet. DES (*Data Encryption Standard*), desarrollado por IBM, es un estándar criptográfico viejo y bien conocido de Internet, ya fuera de uso como tal. Este algoritmo criptográfico provenía de otro estándar criptográfico mas fuerte (Lucifer), el cual posiblemente fue debilitado antes de ser aceptado como estándar y autorizado para su utilización masiva en la red (Scolnik, 2014). Uno podría entender las razones de ello, considerando que algunos Estados conocen la importancia de esta tecnología estratégica y entienden de qué modo podría ser utilizada para afectar su propia soberanía. Desde esta perspectiva, corresponde entonces asociar a los sistemas criptográficos con el concepto de tecnología sensible a la que debemos prestar especial atención. Si la información, estratégica o no, se cifra con un algoritmo vulnerado o vulnerable, no tendremos confidencialidad sobre nuestros datos y comunicaciones.

En la actualidad, una de las herramientas criptográficas más utilizadas para proteger la confidencialidad de nuestra información digital en tránsito es PGP (*Pretty Good Privacy*). Su utilización generalizada fue posible gracias a que su creador, Phil Zimmermann, permitió que fuera libremente descargada (Scolnik, 2014) de la red en 1991. No comercializó el sistema criptográfico que desarrolló, sino que permitió su descarga. Sin embargo, debido a ello, tuvo que afrontar causas judiciales iniciadas por el gobierno de los Estados Unidos, ya que esa tecnología, considerada estratégica, no debía ser liberada para el uso público sin previa autorización gubernamental. Zimmermann centró su alegato de defensa basándose en la importancia que dicha tecnología tendría para asegurar la privacidad de las personas, aspecto alcanzado por el derecho internacional. Definió dicha aplicación como una herramienta vinculada a la defensa de los derechos humanos.

Como último ejemplo, me gustaría mencionar la criptografía aplicada a las comunicaciones sobre la red de telefonía móvil. Los algoritmos de cifrado desplegados sobre esta red de telecomunicaciones fueron débiles (A52) para países por fuera de la OTAN y más robustos (A51) para países miembros (GSM L. A., 2007).

Los previamente mencionados son solo ejemplos orientados a permitirnos comprender la importancia de la criptografía para la defensa de los intereses soberanos en el ciberespacio. El concepto interesante aquí quizás sea el de pensar la criptografía como una forma de proteger la información, aún cuando está en tránsito y cuando los Estados no pueden ejercer

ningún tipo de control de seguridad sobre la información que fluye por la infraestructura del ciberespacio que a diario utilizamos. Infraestructura que, como hemos mencionado, tiene sus propietarios, los cuales responden a determinados intereses estratégicos.

Software

El *software* es otro de los elementos constitutivos del ciberespacio que hemos elegido para desarrollar nuestro marco de análisis. Quizás no todos los que estamos participando de estas charlas estamos consubstanciados con las temáticas específicas de ciberdefensa y ciberguerra, o desarrollo y uso de ciberarmas. Es por ello que me pareció interesante tomar un caso en particular, el de WannaCry, para ilustrar esta temática tan importante vinculada a la utilización del ciberespacio como dominio para la consecución de objetivos estratégicos de Estados nación.

WannaCry fue un ataque de *ransomware* que en 2017 afectó alrededor de 200.000 dispositivos digitales en más de 150 países de todo el mundo. Nadie se explicaba en ese momento cómo un único actor pudo haber tenido acceso a un número masivo de equipos pertenecientes a tantas redes diferentes de forma casi simultánea, ya que no era nada sencillo llevar adelante un ataque de esa magnitud. Con el tiempo se supo –o por lo menos se estima, ya que esas aseveraciones resultan extremadamente difíciles en este ámbito– que el ataque pudo difundirse a esa escala global valiéndose de una vulnerabilidad o puerta trasera explotable mediante una herramienta de *software*, Ethernalblue, que en principio había sido desarrollada por un sistema de inteligencia extranjero (NSA) que permitía el acceso remoto a sistemas operativos Windows. Se estima que la vulnerabilidad fue descubierta por dicha agencia de inteligencia, la cual, a partir de esta, desarrolló una herramienta para su explotación ofensiva. Tanto la vulnerabilidad como la herramienta de explotación asociada habrían sido robadas y utilizadas por otro sistema de inteligencia, atribuyendo Estados Unidos e Inglaterra el ataque masivo WannaCry a Corea del Norte.

Ahora bien, todos alguna vez utilizamos sistemas operativos privativos, sistemas no auditables en los cuales no puede *a priori* analizarse la existencia de algún *backdoor*. Es decir, sistemas sobre los que no podemos saber si poseen una puerta trasera o no y, de este modo, si son vulnerables y accesibles remotamente. Considerando lo expuesto, si los sistemas infor-

máticos que utiliza el Estado, es decir, sistemas gubernamentales, se encuentran operando sobre *software* no auditable, debe entenderse que están expuestos a este tipo de operaciones cibernéticas características de la ciberguerra y el ciberespionaje.

¿Por qué elegí estos temas para abordar el análisis del espacio de conflicto existente entre soberanía y ciberespacio? Porque detrás de ese concepto ficcional de nube existen este tipo de infraestructuras, de herramientas que, en mayor o menor medida, se solapan con el concepto de soberanía. Si uno no tiene soberanía sobre las comunicaciones y sus sistemas digitales, difícilmente en un mundo intercomunicado pueda llevar adelante sus objetivos estratégicos como Estado nación.

Almacenamiento masivo y análisis de datos

Otro de los elementos que me parece fundamental, y que deberíamos considerar para analizar la superposición de conceptos tales como soberanía y ciberespacio, es el almacenamiento masivo y análisis de datos. Todos somos usuarios del ciberespacio. Cada acción que realizamos en un sistema digital conectado genera una huella e información. Compartimos –o entregamos– esa información "libremente". Ahora bien, si a uno le toca ocupar un lugar de toma de decisión vinculado a los intereses estratégicos del Estado, sus comunicaciones y los datos asociados no son iguales a los míos, por ejemplo, que no tengo esa responsabilidad. Debemos entonces saber que la información que transmitimos, detrás de todo el dispositivo físico que vemos, tiene una realidad material. Si esa información puede ser almacenada y analizada, ya sea información específica, estratégica, o grandes volúmenes de datos (cada una tiene una aplicación distinta), tenemos que saber qué implicancias puede tener todo ello para nuestra soberanía.

Sobre este tema, hay un libro muy interesante de una profesora emérita de la Universidad de Harvard, Shoshana Zuboff. El libro se llama *Era del capitalismo de la vigilancia. La Lucha por un futuro humano frente a las nuevas fronteras del poder* (2021). Este analiza, mediante un desarrollo muy meticuloso y documentado, cómo, a partir de la situación de excepción acontecida luego de los atentados terroristas del 9 de septiembre a las Torres Gemelas, se habilitó la posibilidad para la modificación de algunas leyes que afectan el funcionamiento del ciberespacio. Una fue la Ley de Inteligencia Extranjera de los Estados Unidos (*Foreign Intelligence Surveillance Act*, FISA) y otra la Ley Patriota (*Patriot Act*).

Podríamos, en este punto, citar a Milton Friedman para ayudarnos a analizar dichos acontecimientos:

> *...sólo una crisis –real o percibida– da lugar a un cambio verdadero. Cuando esa crisis tiene lugar, las acciones que se llevan a cabo dependen de las ideas que flotan en el ambiente. Creo que ésa ha de ser nuestra función básica: desarrollar alternativas a las políticas existentes, para mantenerlas vivas y activas hasta que lo políticamente imposible se vuelva políticamente inevitable.*

Estas modificaciones jurídicas permitieron reorientar los esfuerzos de inteligencia de señales (SIGINT, por sus siglas en inglés), hasta entonces desactualizados dada la nueva y vertiginosa reconfiguración de las telecomunicaciones globales, hacia el almacenamiento y análisis de grandes volúmenes de datos que fluyen por Internet (Snowden, 2019). Estas modificaciones, por cierto, contenían aspectos discutibles respecto de la violación de libertades individuales y el derecho a la privacidad alcanzado por el derecho internacional.

Esta decisión soberana, de interceptar y analizar grandes volúmenes de datos que fluyen por Internet tiene sobre la soberanía de terceros Estados, tiene un impacto que debiera ser analizado en función de los elementos y antecedentes previamente utilizados para caracterizar el ciberespacio. La configuración y propiedad de la red, como hemos visto, no es simétrica. No toda la información atraviesa las diferentes regiones geográficas soberanas por igual.

Shoshana Zuboff (2019) describe cómo esa enorme cantidad de datos almacenables a partir de este nuevo marco jurídico necesitaría de nuevas tecnologías, de nuevas herramientas para ser analizada. Estas nuevas herramientas surgirían a partir de una fuerte inversión pública, fundamentalmente en Silicon Valley. Dicha inversión pública fue canalizada a través de los sistemas de defensa e inteligencia para el desarrollo –entre otras tecnologías– de algoritmos de *machine learning* eficientes, *data mining*, *big data* e inteligencia artificial. De este contexto y bajo estas políticas surgieron empresas como Google, por ejemplo. No surgieron de una mera actividad emprendedora, sino que contaron con el financiamiento y direccionamiento del Estado y se integraron a un sistema de desarrollo de tecnología para el ciberespacio orientados a la defensa de su soberanía.

En igual sentido, Edward Snowden reveló en 2013 que el tráfico de Internet tiene particularidades propias de la topología global de la red. Las asimetrías postuladas por Snowden pueden inferirse al analizar la distribu-

ción y propiedad de los cables submarinos de fibra óptica. Los anchos de banda devenidos del actual tendido de estos cables hace que existan rutas prioritarias por donde se transmiten los datos. Al respecto, desde nuestra ubicación geográfica podemos observar el necesario pasaje a través del hemisferio norte para cruzar a Europa o para llegar a Asia Pacífico. Sumando ambos aspectos –por un lado, que los datos transmitidos atraviesen necesariamente dicha jurisdicción y, por otro, que las leyes soberanas de la misma permitan el almacenamiento masivo de datos y su análisis– encontramos entonces una importante colisión entre las pretensiones de soberanía de Estados con capacidades asimétricas respecto del control del tráfico global de Internet. Este es uno de los aspectos notables donde se superponen los intereses soberanos propios de cada Estado y las capacidades asimétricas de acción sobre el ciberespacio compartido, que habíamos definido como espacio del problema en nuestra introducción. En igual sentido podemos pensar la asimétrica distribución geográfica de los centros de almacenamiento de datos o *datacenters* (Daigle, 2021). Estos se encuentran, por lo general, lejos de nuestro ámbito jurisdiccional soberano, mayormente en el hemisferio norte.

Sin disponer de soberanía sobre estos elementos centrales que constituyen el ciberespacio, resulta extremadamente difícil cualquier intento normativo, ya que toda iniciativa propuesta podría ser de imposible cumplimiento, meras ideas o expresiones de buena voluntad. Entonces, la pregunta es de qué manera como Estado nación se podría regular este fenómeno si no se dispone de injerencia jurídica sobre la tecnología o sobre el uso que de esa tecnología se hace.

Algunos efectos de las nuevas tecnologías sobre los sistemas democráticos

Hasta aquí, hemos hablado inicialmente de los elementos materiales que componen el ciberespacio buscando establecer un marco de referencia material para ese concepto de nube. De igual modo, hemos indagado en algunos de sus aspectos que se superponen con aquellos constitutivos de la soberanía de los Estados y la posibilidad de ser alcanzados mediante normativa. Buscaremos a continuación estudiar algunos de los efectos que tiene esta configuración del ciberespacio que, como mencionamos en la introducción, seguramente será incompleta e imperfecta, pero que intenta

ofrecer un marco conceptual posible para futuras reflexiones. En otras palabras, esto de ninguna manera pretende ser un decálogo de verdades sobre el ciberespacio, sino que es simplemente un análisis, uno de los tantos posibles.

Uso de datos masivos para afectar procesos electorales

Dijimos en nuestra introducción que dentro de la órbita soberana está la democracia. Creo que, si hay un concepto que puede asociarse mejor al concepto de soberanía, para una sociedad como la nuestra, es el concepto democracia. Si el uso masivo de los datos puede servir para hacer un "targeting psicográfico", como presenta en un informe Cambridge Analytica (2015), los procesos democráticos están en serio riesgo. Difícilmente Estados como los nuestros dispongan de herramientas suficientes para combatir el tipo de injerencias que existen actualmente. El informe citado fue publicado por el parlamento inglés a partir de los estudios realizados para determinar los efectos de la injerencia externa y el desarrollo de operaciones de ciberinfluencia sobre el proceso electoral vinculado al Brexit. Al respecto, debemos decir que nuestro país no se encuentra ajeno a esta temática. Alexander Nix, CEO de la compañía Cambridge Analytica, reconoció frente al parlamento inglés la participación de su empresa en la realización de campañas de ciberinfluencia durante el proceso electoral de 2015.

En igual sentido, Estados Unidos analizó la posible interferencia extranjera por parte de la Federación Rusa en su proceso electoral de 2016 (Mueller, 2019). Es interesante este informe, ya que analiza, por ejemplo, el uso que hizo Hillary Clinton de servidores que no estaban bajo la custodia federal para comunicaciones oficiales. Esta información debiera servirnos para, fundamentalmente, pensar un marco normativo que exija que todos aquellos agentes gubernamentales que tienen funciones públicas relevantes se manejen dentro de estándares de seguridad de la información, para que esta no transite sin una capa de cifrado adecuada por cualquier servidor accesible por terceros actores, estatales o no. En términos concretos, que dicha información estratégica no se deposite en una carpeta compartida de Google Drive, por ejemplo, o en cualquier sistema de carpetas compartidas en la nube. Porque la nube no es tal, no hay una nube, hay un servidor que está en un lugar geográfico claramente definido y sobre el que nosotros probablemente no podamos ejercer control soberano.

Uso de datos masivos para el desarrollo de inteligencia artificial

Por otro lado, esa recopilación masiva de datos es fundamental para generar una tecnología que promete modificar las relaciones de poder preexistentes, la inteligencia artificial. Para quienes estamos más familiarizados con esta temática, la inteligencia artificial no es un nuevo paradigma, sino que esta tecnología ya existe y su alcance presenta actualmente un crecimiento exponencial notable.

Hay un análisis muy interesante realizado por la Comisión Nacional de Seguridad para la Inteligencia Artificial de los Estados Unidos (NSCAI, 2019) vinculado al avance de China, tanto en materia de empresas tecnológicas como en el desarrollo subsecuente de inteligencia artificial. Este fue desclasificado recientemente a pedido de la organización Electronic Privacy Information Center (EPIC), dadas las posibles implicancias que dicha información tendría para el resguardo de la privacidad de los ciudadanos frente a decisiones gubernamentales vinculadas a nuevas implementaciones tecnológicas.

Me pareció interesante compartir con ustedes en esta charla la placa número veintidós de dicha presentación. En ella se destaca la referencia a los dichos de Henry Kissinger, quien hace notar que, aún cuando tuvo la capacidad de llevar adelante una negociación entre países en el plano nuclear, piensa que sería imposible sentar en una mesa de negociación a los actores en el campo de la inteligencia artificial para arribar a acuerdos de cooperación y establecer ciertos límites en el desarrollo de esta tecnología. Con esta cita, Kissinger establece una comparación directa entre una tecnología que, como hemos mencionado previamente, definió las capacidades de negociación geopolítica durante el siglo pasado (la tecnología nuclear), con una tecnología en pleno desarrollo, que pareciera capaz de alcanzar una idéntica función para el siglo en curso. En tal sentido, se establece en el informe de NSCAI que es probable que la regulación que defina la inteligencia artificial para el futuro próximo sea discutida entre actores ya no necesariamente estatales. Quienes estén en capacidad para negociar los marcos regulatorios de tales desarrollos tecnológicos serán probablemente las empresas tecnológicas y sólo algunos exponentes gubernamentales, potencialmente Estados Unidos y China, que son los que lideran este proceso. Se pone en duda incluso la posibilidad de que Estados Unidos, como Estado nación, pueda participar de ese debate. Fuera de discusión se encuentra la participación de empresas tecnológicas como Amazon, Alibaba y Microsoft.

Debemos pensar que un proceso de regulación de la inteligencia artificial será fundamental para normar problemas asociados al desarrollo de armas autónomas y ciberguerra, todas cuestiones que afectan de forma clara las pretensiones de soberanía de los Estados.

Antecedentes de política soberana aplicada al ciberespacio

Utilizando, ahora sí, el marco de referencia construido para esta charla, que es uno de los tantos que podrían generarse según qué interpretación se quiere dar a dos conceptos tan amplios como ciberespacio y soberanía, me pareció interesante presentar propuestas de políticas soberanas generadas por algunos Estados como respuesta a esta nueva realidad, a este nuevo escenario de conflicto denominado ciberespacio.

Brasil

La República Federativa del Brasil tuvo una reacción muy rápida cuando se hicieron públicas las revelaciones de Snowden vinculadas al dispositivo de espionaje masivo en marcha. Una de las alternativas que propusieron (cada Estado o cada región plantea soluciones en función de sus capacidades) fue la de realizar un tendido de cable submarino de fibra óptica compartido con los países miembros del BRICS (Lee, 2016). Este uniría Brasil con Sudáfrica, India, China y Rusia respectivamente. La idea, que se había pensado previamente, pero que tomó auge a partir de las mencionadas revelaciones, no prosperó, aunque es destacable el intento de establecer una opción soberana sobre la propia infraestructura de Internet mediante el tendido de un cable submarino de fibra óptica compartido por otros Estados. Era una propuesta difícil y costosa, pero no imposible. Debe considerarse al respecto que este tipo de iniciativas sólo podrían lograrse mediante acuerdos entre países, de ninguna manera podría llevarlo a cabo un país unilateralmente.

Por otro lado, Brasil generó un marco jurídico que buscó dar respuesta a esta problemática relativamente rápido. En 2014 publicó una ley que obliga a las empresas que tienen contratos con el Estado a depositar los datos dentro de Brasil. Para lograrlo deberían instalar servidores y *datacenters* fronteras dentro de Brasil, de modo que la información generada e intercambiada quede circunscripta a su ámbito jurisdiccional soberano.

Debe considerarse, para comprender la viabilidad de propuestas de este estilo, que la economía brasileña es lo suficientemente grande como para otorgar al Estado brasileño la capacidad de influir sobre el sector privado. Al ser un mercado grande, el no cumplimiento de las exigencias normativas harían perder cuotas de mercado importantes a las empresas tecnológicas.

Unión Europea

La Unión Europea generó un marco regulatorio respecto de la utilización de los datos personales, la General Data Protection Regulation (GDPR). Imagino que debió ser muy difícil reunir los intereses de tantos Estados en un marco regulatorio común. Sin embargo, la Unión Europea tiene una particularidad que nosotros no tenemos: ellos poseen una gran cantidad de *datacenters* dentro de Europa. De este modo, proponer esto en términos tecnológicos implica, de forma muy simplificada, definir legalmente que los datos de interés que estén almacenados fuera de la Unión Europea deban almacenarse dentro de ella y quedar alojados bajo el ámbito de su propia normativa (GDPR, 2016).

De igual modo, hace muy poco y vinculado a la utilización de *software* privativo no auditable, Francia prohibió utilizar la nube de Microsoft 365 en todos los organismos gubernamentales por temor a que dicha empresa esté obligada a compartir información sensible con el gobierno de los Estados Unidos.

Este es uno de los grandes dilemas que se observan actualmente. De hecho, en la contienda internacional entre China y Estados Unidos en relación con la propiedad de la infraestructura digital, el alegato en general es ese: las empresas prestadoras pueden ser privadas pero responden a intereses gubernamentales o deben responder frente a determinada situación a intereses gubernamentales de terceros Estados. Entonces, si nosotros usamos infraestructura de terceros y esos terceros, aún perteneciendo al sector privado, tienen que responder a los intereses soberanos de otros Estados –y está bien que así sea–, nuestra soberanía podría verse vulnerada.

Rusia

Rusia publicó en 2019 un conjunto de adendas, comúnmente denominadas Ley de Soberanía de Internet, a través de las cuales propone avanzar sobre la infraestructura de Internet dentro de su territorio y alcanzar cierto nivel de control sobre los puntos de interconexión con la red global. Lo que

propone es la instalación de equipamiento técnico dentro de la red instalada sobre territorio soberano para poder realizar análisis del tráfico administrado por los grandes proveedores de servicios de internet (ISP, por sus siglas en inglés) pertenecientes al sector privado. En igual sentido, se pretende establecer un marco legal que permita al Estado un manejo centralizado de la infraestructura nacional de Internet frente a amenazas externas.

Como podemos observar en estos ejemplos elegidos, la realidad de cada país es diferente, como también lo es el escenario para el que cada uno pretende estar preparado. No resultará equivalente planificar acciones para la construcción de soberanía en el ciberespacio en el marco de una contienda global permanente, que realizar dicha planificación evaluando un escenario de paz y pretendiendo solo el resguardo de los datos nacionales mediante el establecimiento de normativas que den lugar a un potencial ciberespacio soberano.

Por otro lado, como comentaba previamente, en estas adendas se propone tener control sobre los puntos de interconexión de la red nacional con la internacional. Vinculado a ello, el avance en la aplicación de estas normativas tuvo un impacto manifiesto al ensayarse exitosamente la desconexión total de Rusia de la Internet global en 2019.[6] Para ayudarnos a pensar en esto, podemos imaginar un punto de interconexión global de Internet a partir de nuestro análogo, el cual se encuentra ubicado geográficamente en Las Toninas.

De igual modo, para lograr una desconexión exitosa de Internet es necesario implementar una infraestructura de servidores de nombre de dominio (DNS, por sus siglas en inglés) propia. Esta es otra de las propuestas desarrolladas a partir de las adendas mencionadas. Para los neófitos presentes, los servidores DNS son básicamente las "guías telefónicas" de Internet. El nombre de una página en particular tiene una dirección IP asociada y esta información asociada está manejada de forma centralizada para el normal funcionamiento de la red. Lo que resulta importante comprender en este punto es que gran parte de los servidores raíz de este sistema crítico de Internet están radicados en los Estados Unidos. La Federación Rusa evidentemente vio en esto un nivel de dependencia inaceptable.

Finalmente, Rusia desea instrumentar, en las redes desplegadas dentro de su territorio soberano, una inspección profunda de paquetes. Este último punto atenta contra la privacidad de la información en tránsito. Con

6 Al respecto, véase la desconexión exitosa de Rusia de la Internet global del 2019 en el siguiente artículo de la *BBC*: https://www.bbc.com/news/technology-50902496 (consulta: julio de 2023).

este tipo de implementaciones tecnológicas, la privacidad del ciudadano quedaría claramente vulnerada.

Me gustaría remarcar aquí que este tipo de propuestas, que impulsan la implementación de modificaciones sobre la infraestructura de Internet dentro del territorio soberano de los Estados, es denominada comúnmente "balcanización de Internet". Con su materialización, pasaríamos del concepto actual de "red global interconectada y neutral" (el término neutral, con el actual nivel de concentración de la infraestructura, sería discutible) hacia un escenario donde los Estados empiezan a generar este tipo de políticas que buscan segregar, en cierto sentido, la red nacional de la red global. De este modo, Internet dejaría de ser esa unidad global única y pasaría a tener áreas de protección soberana donde aplican este tipo de soluciones tecnológicas, políticas y normativas.

China

Este es un ejemplo complejo de analizar, tanto por la enorme capacidad tecnológica que distingue a este país, como así también por las características propias de su sistema de organización social y cultural. De algún modo, el ejemplo de la política china sobre Internet difícilmente sea extrapolable a sociedades como la nuestra.

La infraestructura de Internet en China es 100% estatal, algo que no sucede en Rusia, por ejemplo. No pasa en la Argentina tampoco y resultaría difícil encontrar otro Estado que tenga el 100% de la infraestructura de Internet en manos del Estado.

China, al igual que Rusia, implementó controles tecnológicos en los puntos de interconexión con la red global mediante el denominado Escudo Dorado o *Firewall* de Oro. A través de este analizan y operan sobre el tráfico en la interconexión de borde –fronteras adentro, fronteras afuera–, es decir, sobre los puntos de interconexión con la Internet global. Además, la República Popular China desarrolla circuitos integrados. Posee una estratégica capacidad de desarrollo tecnológico soberano a nivel de *hardware* específico. Por su configuración soberana de Internet tiene, asimismo, una gran capacidad para el almacenamiento masivo de datos que utilizan para potenciar un desarrollo acelerado de inteligencia artificial. Están avanzando también en el concepto de Smart Cities, a partir de la generación y acumulación de cada vez más datos, catalizando así el desarrollo de inteligencia artificial. Esta capacidad acelerada de desarrollo soberano de tecnologías estratégicas la posicionan como uno de los grandes contendientes en la arena internacional respecto del dominio total de la inteligencia artificial.

Por otro lado, China tiene una política expansiva sobre la infraestructura global de telecomunicaciones, tanto en lo referido al mercado de dispositivos móviles, como sobre el despliegue de antenas 5G. Posee plataformas de contenidos y buscadores propios, para uso dentro de su territorio nacional, pero también con un enorme nivel de penetración en el escenario global. Este proceso expansivo se encuentra en pleno crecimiento y comienza a generar escenarios de tensión con los otrora actores hegemónicos del ciberespacio. Vinculado a estos aspectos, tiendo a pensar que la contienda por el 5G no está circunscripta a una mera cuestión económica –es decir, quién vende la tecnología–, sino que fundamentalmente apunta a quién se apropia de los datos para alimentar su desarrollo de inteligencia artificial, entre otras motivaciones. Estados Unidos y China son dos grandes actores que conocen el poder que se detenta al poseer la tecnología intermediaria entre el usuario final y la plataforma. Conocen, además, la importancia de las plataformas para la penetración social y construcción de sentido a partir de los contenidos que ellas brindan.[7]

Por otro lado, China tiene una importante cuota de participación en el mercado de la India a través de sus billeteras virtuales. El pago con billeteras virtuales en este país, que constituye un mercado de más de mil millones de personas, se realiza a través de plataformas de pago pertenecientes a empresas chinas.

Ya para finalizar este breve análisis de la situación China, vinculada a soberanía y ciberespacio, quisiera mencionar lo siguiente. En el análisis realizado por la Comisión Nacional de Seguridad para la Inteligencia Artificial de los Estados Unidos (NSCAI), que referenciamos previamente, se presta especial atención a la dependencia que China tiene en materia de aprovisionamiento de semiconductores. Según este estudio, la provisión de microchips es, aún hoy, el principal cuello de botella para el crecimiento de la tecnología China.[8]

---

7 Al respecto, véase la definición de Riesgo para la Seguridad Nacional de plataformas como Tik Tok por parte del gobierno de los Estados Unidos e Inglaterra, en el siguiente enlace: https://edition.cnn.com/2020/07/09/tech/tiktok-security-threat/index.html (Consulta: agosto de 2022).

8 Al respecto, debe prestarse especial atención al rol que juega Taiwán como principal proveedor de microchips avanzados para el desarrollo de aplicaciones civiles y militares, tanto para China como para los Estados Unidos, y sus posibles implicancias como desencadenantes de un conflicto entre ambas potencias. Véase el siguiente enlace: https://www.reuters.com/investigates/special-report/taiwan-china-chips/ (Consulta: agosto de 2022).

Argentina

Quisiera, para finalizar nuestra charla sobre soberanía y ciberespacio, pensar en las capacidades que tenemos nosotros como país y que nos permitirían apuntar hacia el desarrollo de una política soberana vinculada al ciberespacio.

Argentina posee infraestructuras tecnológicas estratégicas sobre las cuales podríamos apoyarnos para el desarrollo de una política soberana respecto del ciberespacio. Por un lado, contamos con una red de fibra óptica propia. La Red Federal de Fibra Óptica (REFEFO) está actualmente constituida por más de 35.000 km de fibra desplegados en una parte importante del territorio nacional. Tenemos, además, la capacidad de diseñar y fabricar satélites geoestacionarios que nos permiten actualmente tener conexión nacional y regional sobre zonas geográficas que aún no fueron alcanzadas por la REFEFO. Tenemos un importante datacenter de primer nivel internacional como el de ARSAT, calificado como Tier 3, y una industria del *software* ampliamente desarrollada, tanto en materia de recursos humanos como en el ámbito de desarrollo para la ciencia y técnica y la investigación, desarrollo e innovación.

Tenemos también la capacidad para desarrollar sistemas criptográficos soberanos. Al respecto, me pareció interesante tomar un ejemplo particular de desarrollo criptográfico nacional para dispositivos IoT. El organismo que define los estándares criptográficos que utilizamos en Internet, llamado NIST, convocó a un concurso global en 2019 para el desarrollo de criptografía liviana aplicable en dispositivos IoT. Una de las propuestas realizadas fue desarrollada por profesionales de las instituciones académicas argentinas, con una propuesta de algoritmo denominado *Yarará y Coral* (Montes y Penazzi, 2019). Esta propuesta fue aceptada y, si bien no resultó ganadora, es importante destacar el nivel de este trabajo, ya que no resulta fácil que una propuesta de algoritmo criptográfico sea aceptada y evaluada por NIST.

Por otro lado, tenemos en construcción en la Argentina un reactor nuclear experimental diseñado íntegramente en el país, RA10, en Ezeiza, que tendría la posibilidad de producir semiconductores de silicio a escala industrial. Los semiconductores de silicio son el sustrato base para la fabricación de circuitos integrados. Con esto no quiero decir que en el corto plazo podamos tener microchips de fabricación nacional, pero, de alguna manera, teniendo la materia prima, el Estado nacional podría pensar en un intercambio de material y tecnología para tener cierto nivel de soberanía, cuando menos, para el desarrollo de algunos componentes críticos vinculados a tecnologías estratégicas y de defensa.

En la República Argentina, además, contamos con un caso de éxito concreto vinculado al desarrollo de tecnología sofisticada y sensible, al cual podríamos referirnos para el desarrollo de tecnología soberana vinculada al ciberespacio. Me refiero al Plan Nuclear Argentino. El Plan Nuclear nacional nació en 1950 y combinó en el famoso triángulo de Jorge Sábato. Este consistía en una política pública de largo plazo donde el Estado nacional debía diseñar las políticas para el desarrollo tecnológico; el sistema científico tecnológico y las universidades, aportar conocimiento soberano; y el sector privado, dinamizar y potenciar los procesos productivos que materialicen dicho desarrollo tecnológico. Al respecto me gustaría decir, ya que estamos en el ámbito de la defensa, que durante los primeros 30 años del Plan Nuclear, la protección y custodia de ese desarrollo soberano de tecnología estuvo a cargo de nuestras Fuerzas Armadas. La presidencia de la Comisión Nacional de Energía Atómica fue, a lo largo de ese periodo, llevada adelante por representantes con formación técnica de las Fuerzas.

Conclusiones

De acuerdo con lo previamente expuesto, creo entonces que nuestro país dispone actualmente de las potencialidades y herramientas necesarias para alcanzar un adecuado nivel de soberanía en el ciberespacio. Quizás lo que necesitemos sea discutir en profundidad estos temas para elaborar un Plan Estratégico a mediano y largo plazo que, según los escenarios posibles, fundamente nuestros objetivos y nuestras pretensiones de soberanía en el ciberespacio. Debiéramos, además, a mi entender, instalar en el debate público la importancia de dicho Plan Estratégico para que, con la plena concientización de la dirigencia política del país y el apoyo y participación de nuestras sociedades, dicho Plan alcance el estatus de política de Estado, para buscar una necesaria continuidad que dé lugar a la consecución de los objetivos propuestos.

Referencias

Cambridge Analytica (2015). *Leave.EU: Psychographic Targeting for Britain*. Recuperado de: https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/BK-Background-paper-CA-proposals-to-LeaveEU.pdf.

Daigle, B. (2021). *Data Centers Around the World: A Quick Look - United States International Trade Commission*. Recuperado de: https://usitc.gov/publications/332/executive_briefings/ebot_data_centers_around_ the_world.pdf.

DINUM-DIR-210901 (15 de septiembre de 2021). Doctrine "Cloud au Centre" et offre Office 365 de Microsoft. https://acteurspublics.fr/upload/media/default/0001/36/acf32455f9b92bab52878ee1c8d-83882684df1cc.pdf

Epifanova, A. (2020). *Deciphering Russia's "Sovereign Internet Law". Tightening Control and accelerating the Splinternet.* Recuperado de: https://dgap.org/en/research/publications/deciphering-russias-sovereign- internet-law

GSM L. A. (2007). *Vision*. Recuperado de: https://www.gsma.com/latinamerica/wp-ontent/uploads/2010/01 /revistagsm2007.pdf.

Lee, S. (2016). International Reactions to U.S. Cybersecurity Policy: The BRICS undersea cable. *The Henry M. Jackson School of International Studies. University of Washington*. https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/

Ley n.° 12.965 (23 de abril de 2014). Marco Civil da Internet. DOU de 24.4.2014.

Miller, G. (11 de febrero de 2020). The Intelligence 'coup of de century'. *The Washington Post*. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Montes, M. y Penazzi, D. (2019). *Yarará and Coral v.* Recuperado de: https://csrc.nist.gov/CSRC/media/Projects/ Lightweight-Cryptography/documents/round-1/spec-doc/yarara_and_coral-spec.pdf

Mueller, R. S. (2019). Report *On The Investigation Into Russian Interference In The 2016 Presidential Election- U.S. Department of Justice* [Archivo PDF]. https://www.justice.gov/storage/report_volume2.pdf

National Security Commission on Artificial Intelligence (NSCAI) (2019). *Chinese Tech Landscape Overview*. Recuperado de: https://epic.org/wp-content/uploads/foia/epic-v-ai-commission/EPIC-19-09-11-NSCAI-FOIA-20200331-3rd-Production-pt9.pdf

Satariano, A.; Russell, K.; Griggs, T. y Migliozzi, B. (10 de marzo de 2019). People think that data is on de cloud, but it's not. It's on the ocean. *New York Times.* https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html

Scolnik, H. D. (2014) *¿Qué es la seguridad informática?* Barcelona: Paidós SAICF.

Snowden, E. (2019). *Vigilancia permanente*. Barcelona: Planeta.

Unión Europea (27 de abril de 2016). *General Data Protection Regulation (GDPR)*. Recuperado de: https://gdpr-info.eu/

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Londres: Profile Books Ltd.

El marco normativo

MARIELA CARDOZO

Entendemos la propuesta metodológica del Ciclo Evolutivo del Ciberespacio como un proceso en constante movimiento. Sin embargo, es preciso saber dónde estamos parados para una evolución conveniente a nuestros intereses como nación. En ese sentido, si se logra determinar en qué momento del ciclo está detenida nuestra construcción, será posible poner los esfuerzos en esa etapa para impulsarla. Si logramos congelar el ciclo para un correcto análisis de determinación de causas y problemas, se podría poner el énfasis en buscarle una solución. Consideremos que la complejidad del ciclo planteado lleva inexorablemente a un árbol de soluciones necesarias para seguir su giro evolutivo. Es frecuente, en políticas complejas, dedicar esfuerzos y poner la energía en resolver cuestiones que no son las causantes de los problemas.

Sin embargo, un elemento clave, necesario abordar para el desarrollo de políticas para el Ciberespacio, es el marco normativo. La charla de hoy vamos a dividirla en dos partes, ya que debemos diferenciar, por un lado, el delito contra las personas y la propiedad, y por otro, el delito contra los Estados o la violación de soberanía. La primera tiene que ver con el ciberdelito y sobre todo con la preservación de datos personales. La segunda parte está referida a las normas del derecho internacional aplicadas al ciberespacio.

Ciberdelito

Dentro del ciclo que venimos debatiendo, relacionado con la planificación estratégica en un escenario digital, nos centraremos en el aspecto de la normativa. Es importante destacar la Directiva de Política de Defensa Nacional (Decreto 457/2021), que propone al ciberespacio como eje fundamental de una de nuestras políticas para implementar, dándole un marco de suma importancia en lo referido a la Defensa Nacional.

Además de los aspectos de la defensa, es necesario ampliar el eje temático incluyendo a la ciberseguridad, al ciberdelito y a la criptografía como lo están haciendo muchos países europeos y americanos. En ese sentido, analizaremos los aspectos legales del ciberdelito, que afecta al individuo particular. El contexto, el espacio, va a ser el digital, pasando de una criminalidad que la vemos latente, de personas a personas, a una donde al sujeto no lo vemos, no es palpable, no es visible, donde generalmente se ocultan las identidades. El *Corpus Iuris*, o el cuerpo del delito, tampoco es palpable, porque generalmente es algo digital, y además la tecnología, por lo general intangible, es utilizada como objetivo o bien como herramienta. Hay muchas formas de ser vulnerados en nuestros derechos individuales, y a esto se le suma la problemática de los límites de la jurisdicción, ya que los actores traspasan fronteras, lo que sucede desde la ciberdelincuencia organizada hasta el terrorismo internacional, en conceptos de Naciones Unidas.

Otra característica que debemos tener en consideración es la asimetría de capacidades, porque podemos tener organizaciones de ciberdelincuentes actuando contra individuos, cuyos derechos son vulnerados (como el derecho al honor, la dignidad y la privacidad). Tengamos en cuenta que el artículo 77 del Código Penal de la Nación equipara documentos de papel con el documento digital, y su vulneración tiene las mismas implicancias legales. La preservación de datos personales es considerada hoy un derecho humano y ahí radica también su importancia. Suele suceder, por otro lado, que la vulneración de la privacidad o del honor se da por parte de corporaciones empresarias, dentro de marcos legales, como por ejemplo con buscadores de Internet, donde también existe el problema de la asimetría.

Debemos partir de la siguiente base: un dato es la simple representación gráfica de la realidad, que para un conjunto de individuos cobra un sentido particular o le asignan una consecuencia jurídica, para luego transformarse en información, que integra en ocasiones las llamadas bases de datos –pueden ser físicas o digitales–, cuyos administradores tienen la responsabilidad de garantizar en su seguridad y buen uso.

Desde el concepto de preservación de los datos personales tenemos, a nivel internacional, el primer organismo que le da la relevancia al tema, que es la Organización para la Cooperación de Desarrollo Económico (OCDE). Fue la primera en resaltar que debíamos proteger los datos de las personas individuales.

Luego, en el año 1995, en la Comunidad Económica Europea se dictó la Directiva n. 46 para la protección o preservación de datos personales. Más tarde, viniéndose ya de Europa a Iberoamérica, tuvimos un primer

encuentro en el año 2003, en Guatemala. Este, por la importancia del tema, fue avalado por la reunión de los jefes de Estado de Iberoamérica. También en 2003 surgió la red Iberoamericana de preservación de datos personales. Se reunió en varias ocasiones, hasta que en el año 2017, en el ámbito del decimosexto encuentro, realizado en Chile, se labraron los estándares mínimos y guías orientadoras para la preservación de datos personales para los Estados iberoamericanos que no lo tuvieran en la legislación. Se fijó, además, un mínimo para contemplar en las legislaciones internas. Estos estándares oficiaron una suerte de derecho convencional vigente para los Estados iberoamericanos, para que lo incorporen al derecho interno, y para que tengan un mínimo de garantías respecto de la preservación de datos personales para los conciudadanos de cada uno de los países.

En la legislación argentina hay que destacar que, con la reforma constitucional de 1994, se incorporó al artículo 43 de la Constitución Nacional el *habeas data* (protección de datos). Este se encuentra al mismo nivel que el amparo, en general, como procedimiento de acceso a la justicia de manera rápida cuando se vulneran derechos o garantías constitucionales. También está al mismo nivel del *habeas corpus* (protección del cuerpo) cuando hay casos de desaparición de personas, en las situaciones donde hay un agravamiento en las penas privativas de libertad u otro que conlleve un menoscabo a la privación de la libertad.

La preservación de los datos personales, que se garantiza a ese nivel –el máximo de nuestra carta magna–, contempla la protección de los datos de las personas humanas. Nos da una vía rápida de acceso al conocimiento de nuestros datos, almacenados en bases de datos. Por otro lado, en caso de que ocurra algún tipo de alteración, modificación o falsedad, podemos pedir la modificación o la rectificación, y hasta llegar a la supresión de los datos en las bases de datos donde estuvieran consignados.

Con posterioridad, desde el nivel constitucional, con las leyes que protegen los datos personales, tenemos específicamente regulada la Ley 25.326, que otorga el procedimiento particular para interponer una acción. En primer lugar, busca el conocimiento de la información que se posee en la base de datos, y por otro lado propende a la rectificación si así correspondiese.

El derecho a la rectificación tiene también sustento convencional en el artículo 14 de la Convención Americana de Derechos Humanos. Como contracara de la preservación de datos personales, está la Ley de Acceso a la Información Pública. Además, vinculada al Ciberdelito, está la Ley 26.388, que prevé una serie de tipos penales en cuanto a los delitos infor-

máticos. Hay jurisprudencia a nivel nacional e internacional sobre este tipo de casos contra el buscador de Google, por ejemplo, argumentando una grave vulneración a los derechos a la dignidad personal y al honor. En esos casos, la Justicia le dio la razón a las víctima al permitir la pericia tecnológica solicitada.

En conclusión, la importancia asignada normativamente a la preservación de datos personales, hace que la información personal digitalizada requiera de ciertos parámetros de licitud, exactitud y objetividad; que quienes vulneren esas normas sean sancionados o penados con multas, penas privativas de libertad o lo que le corresponda según el código penal; y que, por otro lado, también sean sancionados y penados quienes infringen la preservación de datos personales y vulneran derechos de garantías constitucionales aunque estos sean empresas (por ejemplo buscadores), según corresponda, porque están obstruyendo el deber de garantía o el deber de cuidado que tienen bajo su responsabilidad al asumir el rol de guardar de esos datos.

Las normas del derecho internacional aplicado al ciberespacio

OSCAR NISS

Contexto

Lo explicado en el texto anterior sobre los inconvenientes legales para el resguardo de los datos personales es una gran introducción de la problemática que plantea la información digitalizada o virtualizada, ya que conlleva un importante grado de abstracción, difícil de materializar, así como de normar para proteger y defender. Se necesitaría de normativas especiales, más allá de que, en definitiva, el dato del que estamos hablando es impreso en un silicio, a diferencia del dato impreso en un papel. Esta virtualización y esta complejidad es lo que conduce a cuestiones conceptuales divergentes, aún no saldadas. Esto se refleja, con más notoriedad, en las normas y reglas del derecho internacional aplicadas al ciberespacio. Si bien el consenso es que se aplican, no está zanjada la discusión sobre *cómo* lo hacen. En esta materia hay diversos ámbitos de discusión, siendo el más importante el de la Organización de las Naciones Unidas (ONU), en cuyo seno se crearon dos grupos de trabajo.

Por un lado, el Grupo Expertos Gubernamentales (GEG), creado en 2010, luego de que la Federación de Rusia presentara por primera vez en 1998 un informe sobre la problemática de las tecnologías de la información y la comunicación (TIC) y la seguridad internacional. Cuenta con veinte miembros y renueva versiones hasta el 2021. Entre sus conclusiones incluye que, en el uso de las TIC, los Estados deben observar, entre otros principios de derechos internacionales, la soberanía del Estado, la solución de controversias por medios pacíficos y la no intervención en los asuntos internos de otros Estados. Se agregan las obligaciones de respetar y proteger los derechos humanos y las libertades fundamentales, además de garantizar que su territorio no es utilizado por agentes no estatales para cometer actos delictivos en el ambiente ciberespacial. Por recomendación

del GEG emergió la ONU para desempeñar un papel de liderazgo en la promoción del diálogo sobre la seguridad de las TIC, en su uso por los Estados y en el desarrollo de un entendimiento común sobre la aplicación de leyes y normas internacionales, así como también normas y principios para la conducta de un Estado responsable.

El otro es el Grupo de Trabajo de Composición Abierta (GTCA o OEWG, por sus siglas en inglés), creado en 2010 mediante la Resolución 65/182 de la Asamblea General de Naciones Unidas. En este ámbito se reúnen expertos de todos los países, organismos y organizaciones no gubernamentales que hacen llegar sus opiniones sobre los temas que se debaten, aunque estas no son vinculantes. Los miembros, por lo general, son una comitiva que representa a cada país y algunos grandes *jugadores* del mercado de las TIC, que tienen voz pero no voto al momento de buscar consensos. Una iniciativa de Egipto en 2021 llevó a crear un nuevo grupo de acción desde 2025, que efectivizaría las recomendaciones del GTCA, el único grupo que permanece en funciones.

Hay otras iniciativas regionales en materia de ciberseguridad, como la Organización de los Estados Americanos (OEA); el Comité Interamericano contra el Terrorismo (CICTE) y el Programa de Seguridad Cibernética; la Organización para la Seguridad y la Cooperación en Europa (OSCE), que promueve la seguridad de las tecnologías de la información y las comunicaciones cibernéticas desde el año 2013, principalmente mediante las medidas de fomento de la confianza; y la Asociación de Naciones del Sudeste Asiático (ASEAN), con enfoque en los riesgos de ciberseguridad para las empresas, además de la protección de las infraestructuras de ciudades inteligentes. Como se observa, la discusión se da en todo el mundo, desde Asia hasta Occidente.

Hay también iniciativas de debate regionales y específicas en materia de ciberdefensa. Tengamos en cuenta que cuando hablamos de ciberdefensa lo hacemos sobre una capacidad que está muy orientada al accionar de las Fuerzas Armadas y la defensa de la soberanía de las naciones. En este ámbito entonces, hay tres iniciativas regionales en nuestra región, Continente Americano. Uno es la Junta Interamericana de Defensa en el marco de la OEA, la Conferencia de Ministros de las Américas, que también discute el tema, y el Foro Iberoamericano de Ciberdefensa, donde también participan, Portugal y España.

Son todos ámbitos de debate fundamentalmente sobre temas de soberanía y cómo impactan, en las decisiones libres de cada país, las acciones que se toman en el ciberespacio.

La ONU y el derecho internacional aplicado al ciberespacio

El debate en las Naciones Unidas, así como también la aplicación del derecho internacional en el ciberespacio, pasó en principio por el GEG, quienes reafirmaron las recomendaciones de grupos anteriores, confirmando en particular que el derecho internacional y la Carta de las Naciones Unidas es aplicable y esencial para mantener la paz y estabilidad, y para promover un entorno de las TIC abierto, seguro, estable, accesible y pacífico. Es decir, los grupos de trabajo de Naciones Unidas dicen que el derecho internacional es aplicable a las TIC, específicamente al ámbito de las TIC en relación con el ciberespacio, y esto está plasmado en el informe UN GGE 2021 (Documento de las Naciones Unidas A/76/135).

Por supuesto que en esto hay opiniones que difieren del mencionado informe, incluso algunas sosteniendo que es necesario un marco normativo particular. Sin embargo, la mayoría de los países comparten esta declaración, afirmando la validez del actual marco normativo para el ciberespacio. Sin embargo, el estado actual del arte, y la configuración actual del ciberespacio, conllevan legítimas dudas sobre la aplicabilidad.

El informe expresa que, al utilizar las TIC, los Estados deben observar los principios de la Carta de las Naciones Unidas referidos a: la igualdad soberana; la solución pacífica en controversias internacionales, de manera que la paz y la seguridad y la justicia no se vean en peligro; la abstención, en sus relaciones internacionales, de la amenaza o el uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado; el respeto de los derechos humanos y las libertades fundamentales; y la no intervención en los asuntos internos de otros Estados. Estas normas son aplicables al ciberespacio y es importante destacar que todas las recomendaciones de aplicación giran en torno a la soberanía.

Al ser todo el cuerpo del derecho internacional aplicable al ciberespacio, el problema y la pregunta principal es *cómo* se aplica, porque indudablemente la cuestión de la virtualización complica el análisis de los hechos y el dictamen sobre la manera de proceder ajustada a la normativa. La aplicación entonces, debe estar determinada por la interpretación, por un lado, de los Estados individualmente, y por otro, de la comunidad internacional a través de los organismos que debaten el tema y mediante tratados especiales de interpretación de las obligaciones existentes o nuevas. En ese sentido, teniendo en cuenta los atributos exclusivos del ciberespacio, es necesario interpretar el marco normativo para ver cómo se aplica, y esto

es a partir de las posiciones que toman cada uno de los Estados mediante comunicaciones y su expresión en organizaciones internacionales.

Soberanía y obligaciones de los Estados en el ciberespacio

El GEG reafirma que la soberanía estatal y las normas y principios internacionales que surgen de la soberanía se aplican a la práctica de actividades relacionadas con las TIC por parte de los Estados y a su jurisdicción sobre la infraestructura de las TIC en su territorio (UN GEG, 2021). Al no tratarse de un ámbito distinto ni exento de jurisdicción, las ciberoperaciones o actividades conducidas a través del ciberespacio deben respetar las normas jurídicas aplicables y los principios soberanos de las naciones. El derecho no prohíbe *per se* las ciberoperaciones. Sin embargo, su uso malicioso puede constituir una violación del derecho internacional.

En ese sentido, la soberanía es un principio fundamental del derecho internacional. En el ámbito cibernético, el Manual de Tallin 2.0 aclara que, en su componente interno, los Estados tienen autoridad soberana con respecto a la infraestructura cibernética, e incluso actividades cibernéticas localizadas dentro de su territorio.

El debate en el OEWG comienza desde la cuestión de fondo: ¿la soberanía es *regla* o *principio*? La mayoría de los Estados que se han pronunciado consideran que la soberanía es una regla del derecho internacional cuya violación genera responsabilidad de los Estados. Por otro lado, una minoría, particularmente el Reino Unido apoyado por Estados Unidos, considera que no es una regla independiente, sino que es un principio que guía las relaciones internacionales.

Desde el enfoque de la soberanía como principio del derecho internacional del que fluyen ciertas normas prohibitivas, como la no intervención o prohibición del uso de la fuerza, esta no constituye una norma en sí misma.

Bajo el enfoque de que la soberanía es una regla o norma independiente, debe entonces determinarse en qué casos una ciberoperación resulta violatoria de la soberanía de otro Estado. En ese sentido, algunos países consideran que cualquier penetración de una red computacional ubicada en el territorio de otro Estado viola su soberanía. Otros, por el contrario, indican que no todas serían violatorias, sino únicamente aquéllas que producen más que efectos mínimos (este último es el denominado enfoque de mínima). Es esclarecedor el aporte de Noruega:

> *La Corte Internacional de Justicia ha sostenido constantemente que los Estados tienen la obligación de respetar la integridad territorial y la independencia política de otros Estados en virtud del derecho internacional. En un contexto cibernético, esto significa que un Estado no debe realizar operaciones cibernéticas que violen la soberanía de otro Estado. Una Ciberoperación que se manifieste en el territorio de otro Estado puede, dependiendo de su naturaleza, la magnitud de la intrusión y sus consecuencias, constituir una violación de la soberanía. (Documento de las Naciones Unidas A/76/136).*

Obsérvese que el aporte habla de manifestación en el territorio. En el enfoque de mínima, sostenido por la mayoría de los países, debiera producirse un efecto físico o de interrupción de procesos de un gobierno para que prospere una violación de soberanía. "En cualquier caso, los efectos físicos insignificantes y las deficiencias funcionales por debajo de un determinado umbral de impacto no pueden considerarse como una violación de la soberanía territorial", sostiene Alemania.

Algunos problemas no resueltos en el enfoque de mínima según especialistas serían:

i Discrepancia con el enfoque de ciberseguridad/ciberdefensa y ciberdelito, en cuanto al discernimiento ante cualquier violación del sistema de confidencialidad, integridad y disponibilidad.

ii Deja el espionaje cibernético no regulado, ya que la implantación de una pieza de *malware*, una munición, no ocasionaría efectos de impacto manifiesto.

iii En el mismo sentido, coloca ciertos ataques cibernéticos debajo del umbral (por ejemplo, el posicionamiento de *malware* previo al robo de datos) y fuera del alcance del derecho internacional público.

A pesar de las discrepancias mencionadas, el GEG reafirma que la soberanía estatal, así como las normas y principios internacionales que surgen de la soberanía, se aplican a las prácticas de actividades relacionadas con las TIC por parte de los Estados y a su jurisdicción sobre la infraestructura de su territorio. Esta afirmación es de gran importancia. Acá Naciones Unidas –o el GEG de Naciones Unidas 2021– dice que se aplican los principios soberanos de cada nación y que cada Estado tiene jurisdicción sobre la infraestructura de las TIC apoyada en su territorio. Porque, como siempre decimos, las TIC, o el ciberespacio, se componen esencialmente de una capa que está anclada a un territorio físico. Hemos comentado que en general esa capa física tiene que ver con los *datacenters*, con las redes de

comunicación, que están siempre en territorio físico y sobre el cual generalmente algún Estado ejerce la soberanía. De este modo, hay un reconocimiento explícito entre las naciones sobre que el ciberespacio tiene un anclaje territorial, sin ser 100% virtual.

En el presente trabajo trataremos las acciones ofensivas en el ciberespacio, o ciberoperaciones, cuando son realizadas contra los Estados, no contra particulares. Por eso hablamos de los aspectos soberanos en lo cibernético.

Si las normas y principios que proceden de la soberanía se aplican en el ciberespacio, veamos entonces cuáles son: 1) jurisdicción sobre el territorio, incluida la infraestructura de las TIC que se encuentra ahí ubicada; 2) prohibición del uso de la fuerza del ciberespacio; 3) prohibición de la intervención interna de los asuntos de otros Estados; 4) obligación de respetar el territorio; 5) obligación de no permitir, a sabiendas, que el territorio sea usado para actos contrarios de usos de otros Estados; 6) obligación de respetar los derechos humanos tanto en línea como fuera de línea.

La complejidad sigue apareciendo, en definitiva, en cómo lo aplicamos, y esto tiene mucho que ver con cuestiones técnicas de cómo configuramos el ciberespacio en nuestro país. Sin duda, configuraciones del ciberespacio parecidas a las de algunas naciones, como China o Rusia (que difieren entre sí), incluso Estados Unidos de América por su centralidad en la red, permiten saber, de manera más sencilla, cómo aplicar el derecho internacional.

El problema alrededor de cómo aplicarlo reside fundamentalmente en el diseño topológico y en el despliegue de la infraestructura tecnológica en algunos países. También el uso del ciberespacio influye. Si se alojan datos sensibles –de los que hacen al funcionamiento de un gobierno– de un país "A" en un país "B" también encontraremos problemas para aplicar la soberanía sobre los datos en caso de ser necesario. Estos tres elementos deberían estar alineados para una razonable aplicación de las normas del derecho internacional.

Veamos con un ejemplo cómo se podrían aplicar en el ciberespacio estas normas que proceden de la soberanía, teniendo en cuenta el estado del arte de la actual configuración del promedio de los países. Pongamos como ejemplo una ciberoperación de destrucción de información y veamos el caso en cada una de las normas. Aclaremos que la destrucción puede lograrse de manera lógica o física. En ambos casos, el no contar con información puede ocasionar la detención de un proceso o alterar su funcionamiento, con consecuencias que podrían trasladarse al mundo físico, saliendo de la virtualidad de lo cibernético, o incluso causar daños reputacionales. Por ejemplo, podría detener el funcionamiento de un sistema de refrigeración de una planta generadora de energía, que a su vez podría

ocasionar problemas a los habitantes de una zona o hasta incluso provocar la pérdida de vidas.

Básicamente la destrucción de la información afectaría a todas, o al menos a parte de la conocida tríada de confidencialidad, integridad y disponibilidad, pudiendo afectar también a la seguridad nacional, a su reputación y hasta a algunos de sus servicios esenciales. En este sentido, afectaría:

i. La confidencialidad, al publicar la información que podría ser sensible para la seguridad nacional.
ii. La integridad, al alterar, borrar, corromper o denegar el acceso a ciertos datos o *software*, interfiriendo en servicios esenciales.
iii. La disponibilidad, al interrumpir parcial o totalmente el funcionamiento de una red o sistema que preste servicios del Estado.

Si hablamos de soberanía y de agresiones entre Estados o a activos de un Estado, debemos tener en cuenta el principio de distinción, uno de los preceptos fundacionales del derecho internacional humanitario (DIH), que exige que las partes en un conflicto armado deben distinguir en todo momento entre activos de carácter civil y objetivos militares y, en consecuencia, solo pueden dirigir sus operaciones contra objetivos militares.

En lo que se refiere a los activos, los objetivos militares se limitan a aquellos bienes que, por su naturaleza, ubicación, propósito o uso contribuyen efectivamente a la acción militar y cuya destrucción total o parcial, captura o neutralización, en las circunstancias que prevalezcan en ese momento, ofrecen una clara ventaja militar.

Para arrojar más claridad u oscuridad sobre el análisis de este ejemplo, debemos considerar si la información, manifestada inicialmente en datos, constituye o no un objeto. Algunos expertos consideran que la noción de objeto se limita a algo con propiedades físicas, que es visible y tangible en el mundo real. Otros consideran que la noción de objeto refiere a lo no abstracto, siendo los datos correspondientes a esta categoría de cosas concretas, porque son susceptibles de ser atacados y destruidos.

Dicho lo anterior, veamos cómo se pueden tratar las normas citadas internacionales derivadas de la soberanía como fuente del derecho.

Prohibición del uso de la fuerza

Acá empiezan las preguntas y los problemas. La ONU dice que "Todos los miembros se abstendrán, en sus relaciones internacionales de la amenaza de la fuerza, contra la integridad territorial o la independencia polí-

tica de cualquier Estado" (artículo 2, inciso 4, de la Carta de las Naciones Unidas).

Al examinar la aplicación del derecho internacional a la utilización de las TIC por los Estados, el GEG consideró de importancia fundamental los compromisos de los Estados con el principio de la Carta de las Naciones Unidas en cuanto a abstenerse el uso de la fuerza, incluso en lo que respecta a las TIC. En este sentido, todavía es necesario definir un tema no menor: ¿cuándo una operación cibernética equivale al uso de la fuerza? Esto, según la posición de algunos países –como Alemania, Francia, Australia y el Reino Unido de Gran Bretaña, entre otros– tiene que ver con la escala y los efectos, y obviamente debe haber alguna prueba de estos. Noruega, en particular, expresa que una ciberoperación puede constituir el uso de la fuerza o incluso un ataque armado si su escala y sus efectos son comparables a los del uso de la fuerza o de un ataque armado por medios convencionales. Además, alega que esto debe determinarse sobre la base de una evaluación, caso por caso, teniendo en cuenta las circunstancias específicas.

Ahora bien, en ese sentido, ¿cómo medimos un ataque cibernético? ¿Una operación cibernética constituye un ataque? El efecto y escala se pueden medir por indicadores cualitativos y cuantitativos. Por ejemplo, se miden: por el origen de operación y la naturaleza del instigador, si es militar o no; por la naturaleza del objetivo previsto, como el carácter militar de la infraestructura atacada; por el alcance de la intrusión o gravedad del ataque; por los efectos reales o previstos de la operación, porque probablemente los efectos no se hayan conseguido, pero sí están previstos en esa operación; por la inmediatez de los efectos; por la profundidad de la penetración de la estructura cibernética; por sus efectos en el mundo físico. En todos los casos se considera como objeto a la información, aunque produzca efectos en lo social de una población o en la moral del enemigo.

Consideremos que si el instigador es de origen militar y la operación cibernética es contra un conjunto de datos civiles esenciales, se estaría violando el principio de no uso de la fuerza, independientemente de la causa y efecto. Esto, bajo el principio del DIH, se constituye en una operación prohibida, debido al carácter y uso no militar de los conjuntos de datos en cuestión. En cambio, la operación sería permisible en la medida en que el conjunto de datos cumpliera con ambos aspectos de la definición de objetivos militares.

Algunos ejemplos de operaciones cibernéticas que pueden constituir uso de la fuerza son: lesiones a personas o muertes; daños o destrucción de objetos físicos, como podría ser la interferencia con el funcionamiento

de un reactor nuclear, algo que sucedió en Irán con Stuxnet; pérdida generalizada de vidas humanas; inhabilitación de sistemas de control de tráfico aéreo que luego dé lugar al derribo de un avión (o sea, no solamente tiene que ser la inhabilitación de un sistema de control de tráfico aéreo, sino que debe dar lugar a un efecto tal como el derribo de un avión); abrir una presa sobre una zona poblada que provoque alguna destrucción; penetrar en los sistemas militares, para comprometer los sistemas de defensa de una nación. Algunas naciones sostienen que financiar o capacitar personas para que realicen ataques contra un Estado también constituye un ciberataque calificable como uso de la fuerza. Graves repercusiones financieras o económicas, así como la interferencia con servicios médicos esenciales o de transporte, también podrían calificar, siempre que se apreciaran efectos físicos de razonable magnitud contra una población.

En todos esos casos una ciberoperación de destrucción de información podría constituir una violación al uso de la fuerza, con los considerandos tratados. Téngase en cuenta que, en una operación convencional, la sola penetración de un arma de un país en el territorio de otro tampoco constituiría un acto de uso de la fuerza. Siempre deben darse otras circunstancias.

Intervención en los asuntos internos de un Estado

Tanto Naciones Unidas como sus dos grupos de trabajo, GEG y OEWG, confirmaron que "…en su utilización de las TIC, los Estados deben observar, entre otros principios del derecho internacional, la no intervención en los asuntos internos de otros Estados" (Documento de la ONU A/70/174). Una intervención está prohibida si atenta contra las cuestiones que cada Estado tiene autorizadas, por el principio de soberanía de los Estados de decidir libremente. Son ejemplo de ello: la elección de un sistema político, económico, social y cultural, y la formulación de la política exterior.

Decimos que la intervención requiere siempre de dos elementos: la interferencia con el dominio reservado del país en cuestión (*domaine réservé*) y acciones de coerción. Recordemos que, de acuerdo con la teoría permisiva del derecho internacional público, aceptada en la práctica general, todo asunto no delegado a este por los Estados, permanece bajo la órbita competente de estos.

Entonces lo que debe definirse es la coerción en el contexto cibernético. La contribución que hace Francia en el OEWG es interesante, porque expresa que, aún en el ciberespacio, "la coerción significa obligar a un Es-

tado a tomar una medida (ya sea un acto u omisión) que de otra manera no emprendería voluntariamente".

En nuestro ejemplo de ciberoperación con destrucción de información se infringe el principio de no intervención antes mencionado. Por ejemplo, si la operación en cuestión alterara la capacidad de un país para celebrar elecciones o el resultado de estas (si se viola su integridad), o si se impidiese el normal funcionamiento de la administración pública o se provocase inestabilidad en el sistema financiero. Evidentemente, con esa operación, se está interviniendo en las cuestiones internas de otro país a través de un método coercitivo proveniente del ciberespacio.

Un capítulo aparte merece el tema de las campañas de desinformación para anular o encauzar la opinión pública a favor o en contra de determinados actos de la política, como por ejemplo el acto electoral. En ese caso, cabe determinar si las campañas de desinformación pueden constituir una intervención o, dicho de otra manera, si puede la información, en sí misma, ser coercitiva. Por otro lado, habría que determinar el objeto de la coerción. Estos son los dos elementos que debemos considerar para saber si hay una violación del principio de no intervención.

En ese sentido es muy ilustrativo el aporte de Alemania, que expresa:

> *En el contexto de la intervención ilícita, el problema de la interferencia electoral extranjera por medio de actividades cibernéticas maliciosas se ha vuelto particularmente virulento. En general, Alemania está de acuerdo con la opinión de que las actividades cibernéticas maliciosas dirigidas a elecciones extranjeras pueden –ya sea individualmente o como parte de una campaña más amplia que involucre tácticas cibernéticas o no relacionadas con la ciberactividad– constituir una intervención ilegal. Por ejemplo, es concebible que un Estado, al difundir desinformación a través de internet, pueda incitar deliberadamente a violentos levantamientos políticos, disturbios y/o conflictos civiles en un país extranjero, impidiendo así de manera significativa la realización ordenada de una elección y la emisión de votos. Esas actividades pueden ser comparables en escala y efecto al apoyo de grupos insurgentes y, por tanto, pueden ser similares a la coerción en el sentido mencionado. (Documento de las Naciones Unidas A/76/376)*

Está clara la posición. Sin embargo, se deberían analizar algunas particularidades, como hacia quién está dirigida la coerción y cuáles fueron los efectos reales de la campaña, cosa difícil de mensurar.

En resumen, una ciberoperación de destrucción de información podría constituir una violación a la norma de no intervención en los asuntos de otro Estado, dependiendo de la escala y los efectos ocasionados.

Responsabilidad de los Estados

Veamos la responsabilidad estatal en el ciberespacio y sus problemáticas. En ese sentido, el Grupo de Expertos Gubernamentales (GEG) de la ONU reafirma que los Estados deben cumplir con sus obligaciones en relación con los hechos ilícitos internacionales atribuibles en virtud del derecho internacional. La invocación de la responsabilidad de un Estado nacional por un hecho internacionalmente ilícito entraña complejas consideraciones técnicas, jurídicas y políticas.

La responsabilidad se rige por los artículos de la Comisión Internacional de Responsabilidad de los Estados ante los actos internacionales irregulares:

> *Artículo 1. Responsabilidad del Estado por sus hechos internacionalmente ilícitos. Todo hecho internacionalmente ilícito del Estado genera su responsabilidad internacional.*
>
> *Artículo 2. Elementos del hecho internacionalmente ilícito del Estado. Hay hecho internacionalmente ilícito del Estado cuando hay un comportamiento consistente en una acción u omisión: si es atribuible al Estado según el derecho internacional; y si constituye una violación de una obligación internacional del Estado.*

En este compromiso, el mayor problema que vamos a tener es el de la atribución. Sabemos que en el ciberespacio uno de los mayores problemas es atribuir la agresión, es decir, atribuir el ataque, la operación cibernética. En otras palabras, para saber si un Estado infringió o violó la soberanía de otro Estado, primero tenemos que atribuírselo. Para ello, en el contexto del ciberespacio hay diferentes formas de atribución: técnica, política o legal.

La atribución técnica es la más complicada, porque requiere una investigación fáctica y técnica sobre los posibles autores de una operación cibernética, además de determinar un grado de certeza con el que se puede establecer su identidad. Con el estado del arte actual, respecto de la configuración y topología de la Internet –principal red de comunicación del

ciberespacio– es casi imposible la identificación del autor de una operación cibernética, a menos que el atacante no tome recaudos operativos.

La atribución política es la más sencilla y la que más se usa. Es una consideración política por la cual la decisión se toma para atribuir (en público o de otra manera) una ciberoperación específica a un actor, sin necesariamente causar consecuencias legales por la decisión. La atribución no tiene que estar necesariamente relacionada con un Estado, sino que también puede afectar a un actor privado que está actuando desde un Estado, y ahí entra la diligencia debida en el ciberespacio.

Por último, la atribución legal es una decisión por la cual el Estado de la víctima –no necesariamente el Estado tiene que ser la víctima, puede ser una infraestructura de un Estado– atribuye un acto u omisión a un Estado específico, con el fin de hacer que ese Estado sea legalmente responsable por la violación de la obligación de responsabilidad con el Derecho Internacional.

A diferencia del delito contra las personas, la responsabilidad de los Estados no establece cargas ni normas o pruebas para la atribución. Esas cuestiones pueden ser pertinentes para los procedimientos judiciales o de otro tipo, pero no se aplican como asunto jurídico internacional a la determinación de un Estado sobre la atribución de ciberactos internacionalmente ilícitos, a los efectos de su respuesta a esos actos, incluso si adopta medidas unilaterales de autoayuda permitidas en virtud del derecho internacional, como las contramedidas. En ese contexto, un Estado actúa como su propio juez de los hechos y puede tomar una decisión unilateral con respecto a la atribución de una ciberoperación a otro Estado. Esta posición es sostenida por Alemania, los Países Bajos y los Estados Unidos de América, entre otros pocos. Sin embargo, el GEG recuerda que la indicación de que se inició una actividad de las TIC, o de que se originó de alguna otra manera desde el territorio o la infraestructura de TIC de un Estado, puede ser insuficiente en sí misma para atribuir el ciberacto a ese Estado.

Aunque es difícil sostenerlo en los hechos, Alemania sostiene que es necesario alcanzar un nivel suficiente de confianza para la atribución de hechos ilícitos, y Francia que la práctica y la jurisprudencia requieren de una certeza suficiente sobre el origen del ataque y la identidad del autor del ataque, antes de que pueda adoptarse una medida como respuesta. Ahondando en su opinión, el país galo también sostiene que para atribuir una ciberoperación no es necesario que un Estado revele la evidencia subyacente. Las pruebas, en el sentido jurídico, son pertinentes solo si se inician procedimientos legales. Un Estado que toma contramedidas, o se basa en su derecho inherente de autodefensa en respuesta a una operación ciber-

nética, puede solo tener que explicar sus acciones, por ejemplo, si el asunto se presenta ante la Corte Internacional de Justicia. En tal situación, debe ser posible proporcionar pruebas que justifiquen la contramedida o el ejercicio del derecho de autodefensa. Esto puede incluir tanto información obtenida a través de canales regulares como de inteligencia.

Aquí entra a jugar el compromiso de debida diligencia. La mayoría de los Estados que se pronunciaron consideran que la jurisdicción exclusiva que tienen los Estados sobre la infraestructura cibernética localizada en sus territorios crea derechos, pero también obligaciones. Según lo ha indicado la Corte Internacional de Justicia, todo Estado tiene la obligación de no permitir, a sabiendas, que su territorio se utilice para actos contrarios a los derechos de otros Estados. Siguiendo este criterio, una de las normas voluntarias contenidas en el informe del GEG de 2015 fue que los "Estados no permitan, a sabiendas, que su territorio se utilice para hechos internacionalmente ilícitos usando TIC" (ONU, 2015).

Claro que esta declaración es de bastante difícil cumplimiento, ya que dependerá de las capacidades logradas en el ciberespacio por parte de cada Estado y por el recurrente problema de la actual configuración y topología del ciberespacio.

Como lo indica el informe del GEG de 2021: "no se espera que los Estados puedan o deban controlar todas las actividades relacionadas con las TIC que se realizan en su territorio" (ONU, 2021). Es, por supuesto, muy dificultoso lograr este compromiso. Muchas opiniones asocian esta posibilidad al hecho de que:

> *…podría constituir una justificación peligrosa de sistemas de vigilancia masiva. En este sentido, Estados Unidos aclara que la soberanía sobre TIC en el territorio de un Estado no debe servir de excusa para violar derechos humanos y otras obligaciones bajo derecho internacional. (ídem)*

Sin embargo, vigilar el ciberespacio, con el fin de detectar las anomalías que suelen presentar los ataques, no necesariamente conlleva la violación de la privacidad de las personas y mucho menos de los derechos humanos. Se podría percibir aquí un pretendido posicionamiento en favor de estos derechos de las personas, con el objetivo de mantener el *statu quo* del ciberespacio.

Opciones de respuesta

Una vez atribuida la responsabilidad del ataque, ¿cuáles son las opciones de respuesta que tienen los Estados frente a esta ciberoperación? Siempre se aboga por la solución pacífica de las controversias. En este sentido, el GEG del 2021, el último, dice que los Estados parte en cualquier controversia internacional, incluidas las que impliquen la utilización de las TIC cuya continuidad pueden poner en peligro el mantenimiento de la paz y la seguridad internacionales, deben procurar, ante todo, una solución por los medios propuestos por el artículo 33 de la Carta de las Naciones Unidas, a saber: la negociación, la investigación, la mediación, la conciliación, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su propia elección. Es decir, la solución pacífica ante todo.

El OEWG, con palabras similares, refiere a lo mismo: la solución pacífica. ¿Cuáles son, entonces, las opciones de respuesta? En principio, protestas diplomáticas; atribuciones públicas, nombrar y avergonzar, que es la que más se usa; procedimientos penales contra los autores, aunque es un poco más complicado porque ya depende de la normativa de cada país y de las pruebas que se puedan recaudar; sanciones, medidas restrictivas y autoayuda.

Conclusión

Como vimos, la aplicación del derecho internacional en el ciberespacio es un tema aún en debate, llevó años y llevará otros tantos. Uno de los problemas es que estamos tratando de normar y ponernos de acuerdo sobre la base de un ciberespacio con tres elementos claves, o tríada continente, que se pretenden inmutables: 1) infraestructura territorial; 2) topología; y 3) usabilidad. Mientras se mantenga el *statu quo* de estos tres elementos, cualquier debate será vano.

Más allá del debate internacional, algunos países avanzaron con normativas internas que conllevaron adecuaciones en la tríada continente. De esa manera, se va camino a una Internet personalizada, adecuada a los intereses soberanos de cada nación. No por ello esa personalización implica la desagregación o fragmentación de la Internet global, con todos los benefi-

cios que puede conllevar para el desarrollo de las naciones, del comercio internacional, de la educación y del acceso a la información.

Esta adecuación se viene dando debido a las necesidades referidas a la seguridad o defensa de los países que las ciberarmas y su uso pusieron en riesgo. La dependencia tecnológica lleva a considerar esta personalización del ciberespacio, y aquí no hablamos de teorías conspirativas, que también puede haberlas, sino de hechos fácticos, como desastres naturales, aislamientos y conflictos armados que atentan contra la cadena de suministros tecnológicos, privilegios de comunicación y otras acciones que cualquier nación tiene la obligación de tomar para el resguardo de su seguridad y soberanía.

A modo de ejemplo, podríamos hablar de normativas que requieren alojar los datos de las infraestructuras críticas, incluido el Estado, en centros de datos localizados dentro de las fronteras físicas del país. También de utilizar servidores de nombres de dominios (DNS, por sus siglas en inglés) de servicios nacionales, o del alojamiento de servicios que afecten a datos sensibles en infraestructuras dentro del territorio, así como también de configuraciones y usos regulados para las infraestructuras críticas, y sin duda de la necesidad de la concientización ciudadana y la capacitación técnica que colabore con la mirada estratégica nacional.

Normativa Nacional

A continuación hay, a modo de ejemplo, normativas en Argentina que podrían contribuir a la personalización del ciberespacio, llevadas adelante desde principios del siglo XXI. Podemos citar:

Ley Argentina Digital – Ley 27.078/2014

Su objeto fue posibilitar el acceso de la totalidad de los habitantes de la República Argentina a los servicios de la información y las comunicaciones en condiciones sociales y geográficas equitativas, con los más altos parámetros de calidad.

Esta es una ley que fundamenta todo lo relacionado con el ciberespacio, ya que lo declara como necesario para la producción y la independencia tecnológica, sin olvidar la función social que conlleva. Podemos ver estos conceptos en sus primeros dos artículos:

> *ARTÍCULO 1° —Objeto. Declárese de interés público el desarrollo de las Tecnologías de la Información y las Comunicaciones, las Telecomunicaciones, y sus recursos asociados, estableciendo y garantizando la completa neutralidad de las redes (…). Esta norma es de orden público y excluye cualquier tipo de regulación de los contenidos, cualquiera fuere su medio de transmisión.*
>
> *ARTÍCULO 2° —Finalidad. Las disposiciones de la presente ley tienen como finalidad garantizar el derecho humano a las comunicaciones y a las telecomunicaciones, reconocer a las Tecnologías de la Información y las Comunicaciones (TIC) como un factor preponderante en la independencia tecnológica y productiva de nuestra Nación, promover el rol del Estado como planificador, incentivando la función social que dichas tecnologías poseen, como así también la competencia y la generación de empleo mediante el establecimiento de pautas claras y transparentes que favorezcan el desarrollo sustentable del sector…*

Por supuesto, luego de una ley viene su aplicación, la autoridad de aplicación correspondiente y el poder de policía que pueda ejercer el Estado para su efectivo cumplimiento. Posteriormente, el Decreto 690/2020 modifica la mencionada ley, agregando el artículo 15, que establece "…que los Servicios de las Tecnologías de la Información y las Comunicaciones (TIC) y el acceso a las redes de telecomunicaciones para y entre licenciatarios y licenciatarias de servicios TIC son servicios públicos esenciales…".

Ley de Economía del Conocimiento – Ley 27.506/2019

Cuando hablamos de normas, no solo nos referimos a obligaciones de comportamiento, sino también a políticas públicas de promoción de determinadas actividades, como la promoción de la industria del *software* en Argentina, o la actual Ley de Economía y Conocimiento, derivada de esa, que expresa:

> *Créase el Régimen De Promoción De La Economía Del Conocimiento que regirá en todo el territorio de la República Argentina, y que tiene como objetivo promocionar actividades económicas que apliquen al uso del conocimiento y la digitalización de la información apoyado en los avances de la ciencia y de las tecnologías, a la obtención de bienes, prestación de servicios y/o mejoras de procesos. (art.1, Ley 27.506/19).*

Si bien no haya una relación directa ni orientativa respecto al ciberespacio, sienta las bases para el desarrollo de uno de los tres pilares de su tríada continente.

Ley de Protección de Datos Personales – Ley 25.326/2000

Esta ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes. Su objetivo es garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre ellas se registre. Como en el caso anterior, si bien esta ley no tiene implicancia directa en el ciberespacio, sí la tiene sobre el aspecto de usabilidad de la tríada.

Ley de Firma Digital – Ley 25.506/2001

En su texto se reconoce el empleo de la firma electrónica y de la firma digital, además de su eficacia jurídica. Al igual que en el caso anterior, impacta en los aspectos usabilidad de la tríada.

Directiva de Política de Defensa Nacional (DPDN) – Decreto 457/2021

La DPDN, el decreto presidencial que da los lineamientos y la orientación política para el Ministerio de Defensa y las Fuerzas Armadas, es la base para dar inicio al Ciclo de Planeamiento Estratégico Militar.

En el posicionamiento estratégico, coloca al ciberespacio como un dominio transversal, donde resulta imprescindible "evaluar, desde la perspectiva soberana y en el campo de la ciberdefensa, el impacto de las próximas tecnologías, como las redes 5G o la comunicación cuántica" (DPDN, 2021). En ese sentido, "es necesario realizar un ajustado análisis prospectivo sobre los posibles escenarios que implicarán las TIC para la gobernanza de Internet y su topología, tanto desde el punto de vista tecnológico como político" (ídem).

Atenta a cuestiones explícitamente planteadas, relacionadas con la soberanía, la DPDN instruye al Ministerio de Defensa:

> *…desarrollar el objetivo operacional del Sistema de Ciberdefensa, consistente en la observación, vigilancia y control de la actividad que acontece en (…) las redes del Sistema de Defensa*

> *Nacional y de las infraestructuras (…) que le sean asignadas, con el fin de prevenir y contrarrestar incidentes provenientes del ciberespacio. (DPDN, 2021)*

A diferencias de anteriores DPDN, esta tiene un apartado específico para la ciberdefensa, reconociéndola como un espacio operacional para las Fuerzas Armadas, transversal a los espacios convencionales y que impacta en la soberanía.

Otras normas

Además de las leyes referidas y las concernientes al delito informático, hay otra serie de normas específicas que impactan sobre el Ciberespacio:

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos.
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de Aplicaciones Seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Resolución 1523/2019. Definición de Infraestructuras Críticas.
- Decreto 577/2017. Creación del Comité de Ciberseguridad.
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.

Decreto 1407/2004

Norma que crea el Sistema Nacional De Vigilancia y Control Aeroespacial (SINVICA), propiciando no solo la radarización, sino también la construcción de radares secundarios argentinos.

ARSAT – Ley 26.092/2006

Otra ley por ejemplo, fue la que creó a la empresa ARSAT. Esta política pública tiene que ver con el Ciberespacio y con los aspectos soberanos. A través de sus unidades de negocio, explota un *Data Center Tier III*, uno de

los mejores de la Argentina y de Sudamérica; también una red de fibra óptica (REFEFO) de más de 30.000 kilómetros iluminados; y comunicación satelital, poniendo en órbita tecnología construida en el país. Entonces, estas son políticas públicas referidas al ciberespacio, más específicamente a la parte dura de la tríada, que es la infraestructura tecnológica controlable.

Por otro lado, un breve digesto de la normativa argentina relacionada con las TIC, ordenado por fecha, podría ser:

- Ley 25.326 de Protección de Datos Personales (2000). Establece el marco legal para la protección de los datos personales en Argentina.
- Decreto 764/2000 de Firma Digital (2000). Reglamenta el uso de la firma digital y su equivalencia con la firma manuscrita en el ámbito de las relaciones jurídicas y comerciales.
- Ley 26.032 de Acceso a la Información Pública (2005). Garantiza el derecho de acceso a la información pública y establece los procedimientos para su ejercicio.
- Ley 26.388 de Delitos Informáticos (2008). Tipifica los delitos informáticos y establece sanciones para estos.
- Decreto 864/2010 de Plan Nacional de Telecomunicaciones "Argentina Conectada" (2010). Establece los objetivos, estrategias y acciones para la construcción de una infraestructura de telecomunicaciones de última generación en Argentina.
- Ley 26.522 de Servicios de Comunicación Audiovisual (2009). Regula el funcionamiento de los medios de comunicación audiovisual en Argentina y establece las condiciones para la adjudicación de licencias.
- Decreto 117/2016 de Argentina Digital (2016). Establece los objetivos, principios y estrategias para la transformación digital del Estado y la sociedad en Argentina.
- Ley 27.078 de Accesibilidad de las Tecnologías de la Información y la Comunicación (2014). Garantiza el acceso a las tecnologías de la información y la comunicación para personas con discapacidad y establece las obligaciones de los prestadores de servicios.
- Decreto 27/2018 de Simplificación Regulatoria (2018). Establece medidas para la simplificación de trámites y procedimientos en el ámbito de la Administración Pública Nacional.
- Ley 27.541 de Solidaridad Social y Reactivación Productiva en el Marco de la Emergencia Pública (2019). Establece medidas para la reactivación económica y social en el marco de la emergencia pública declarada en Argentina.

Es importante destacar que existen otras normativas que, si bien no están directamente relacionadas con las TIC, tienen impacto en el sector, como por ejemplo la Ley de Defensa del Consumidor, la Ley de Propiedad Intelectual y la Ley de Contratos de Trabajo. Además, se deben considerar las normativas provinciales y municipales que complementan la normativa nacional.

Estado del arte en cuestiones normativas

En definitiva, toda esta discusión de la aplicación del derecho internacional en el ciberespacio, en la práctica, impacta hacia el interior de cada país. Cada Estado es, obviamente, quien define y desarrolla sus propias normas. Cabría preguntarse si estas se encuentran alineadas respecto de la opinión del derecho internacional o, quizás, a su propia mirada dentro del debate internacional.

Las normas escritas referidas a la protección de datos, a la ciberseguridad, y a la ciberdefensa, dan cuenta de una conceptualización del ciberespacio y su relación con la soberanía. ¿Las normas contemplan la paz y la seguridad en el ciberespacio? ¿Contemplan el respeto a los derechos humanos e individuales en el uso de las TIC? ¿Contemplan el desarrollo sostenible? Estos tres principios son los que menciona Naciones Unidas cuando empieza a discutir el tema del ciberespacio. ¿Existen normas que dispongan aumentar la ciberseguridad en la cadena de suministro? ¿Y en el desarrollo de tecnología? Esas y otras preguntas son las que tendríamos que hacer para determinar cómo estamos, como nación, en esta burbuja que llamamos normativa aplicada al desarrollo y uso de las TIC.

Referencias

Arnaudo, E. (2011). *La privatización de las grandes empresas nacionales. El caso de la E.N.T.E.L.* [Trabajo final]. Universidad Nacional de Córdoba.

Buzai, G. D. (2012). El Ciberespacio desde la Geografía. Nuevos espacios de vigilancia y control. *Meridiano - Revista de Geografía*, *1*: 265-278. Disponible en: <http://www.revistameridiano.org/n1/13/>.

Calandra Bustos, P. y Araya Arraño, M. (2009). *Conociendo las TIC*. Santiago: Universidad de Chile, Facultad de Ciencias Agronómicas.

Cámara Argentina de Internet – CABASE (2019). *CABASE Internet Index. Estado de Internet en Argentina y la Región.* Recuperado de: https://www.cabase.org.ar/wp-content/uploads/2019/12/CABASE-Internet-Index-II-Semestre-2019.pdf

Comité Internacional de la Cruz Roja (2014). *Report of the ICRC Expert Meeting on 'Autonomous weapon systems: technical, military, legal and humanitarian aspects'*. Recuperado de: https://www.icrc.org/en/doc/assets/files/2014/expert-meeting-autonomous-weapons-icrc-report-2014-05-09.pdf

Decreto 457/2021 [Poder Ejecutivo Nacional]. Directiva de Política de Defensa Nacional. 19 de julio de 2021.

Decreto 62/90 [Poder Ejecutivo Nacional]. Concurso Público Internacional Privatización del Servicio Público de Comunicaciones. Pliego de Bases y Condiciones. 12 de enero de 1990.

Decreto de Necesidad y Urgencia 690/2020 [Poder Ejecutivo Nacional]. Argentina Digital. Argentina. 22 de agosto de 2020.

Dunayevich, J.; Ramirez, G.; Trentadue, C.; Franca, D. y Zylbersztejn, T. (2017). *Historia de NIC Argentina en el marco de la evolución de Internet en el país*. Recuperado de: https://nic.ar/sites/default/files/paper_-_historia_de_nic_argentina_en_el_marco_de_la_evolucion_de_internet.pdf.

Gago, L. N. y Beccaria, H. (2013). El lenguaje y la construcción de sentido. La producción y la interpretación de imágenes. *Question/Cuestión, 1*(40), 297–309.

Gallardo, O. S. (2005). *Jorge A. Sabato y el desarrollo tecnológico necesario y posible*. Córdoba: El Emporio Ediciones.

García Delgado, D. (1997). *La reforma del Estado en la Argentina: de la hiperinflación al desempleo estructural*. Flacso. Recuperado de: García Delgado, D. (1997). La reforma del Estado en la Argentina: de la hiperinflación al desempleo estructural. Recuperado de: http://biblioteca.

municipios.unq.edu.ar/modules/mislibros/archivos/reforma_argentina.pdf

INDEC (s.f.). Censo 2010. Recuperado de: https://www.indec.gob.ar/indec/web/Nivel4-CensoNacional-3-6-Censo-2010.

International Telecomunicacion Union. (2016). *Tecnologías digitales para el cumplimiento de los Objetivos de Desarrollo Sostenible de las Naciones Unidas*. Recuperado de: https://www.itu.int/es/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx

International Telecomunicacion Union. *ICTs for a Sustainable World*. Recuperado de: https://www.itu.int/es/sustainable-world/Pages/default.aspx

Junta Interamericana de Defensa (2020). Guía de Ciberdefensa. Recuperado de: https://www.jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf

Ley 27.078/2014. Argentina Digital. Tecnologías de la Información y las Comunicaciones. 18 de diciembre de 2014.

Miranda, O. A. (2021). Operaciones multi-dominio: soluciones tácticas para desafíos estratégicos y operacionales. *Revista Ensayos Militares*, 7(1), 111 - 125.

Mora y Araujo, M. (2002). *La estructura social de la Argentina: Evidencias y conjeturas acerca de la estratificación social*. Santiago de Chile: CEPAL.

ONU (1987). Informe de la Comisión Mundial sobre el Medio Ambiente y el Desarrollo. A/42/427. Recuperado: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N87/184/70/PDF/N8718470.pdf?OpenElement

ONU (2002). Informe de la Cumbre Mundial sobre el Desarrollo Sostenible. A/CONF.199/20. Recuperado de: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/636/96/PDF/N0263696.pdf?OpenElement.

ONU (2010). Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/65/201. Recuperado de: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/60/PDF/N1046960.pdf?OpenElement

ONU (2015). Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. A/70/174. Recuperado de: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/38/PDF/N1522838.pdf?OpenElement

ONU (2017). Labor de la Comisión de Estadística en relación con la Agenda 2030 para el Desarrollo Sostenible A/RES/71/313. Recuperado de: https://ggim.un.org/documents/A_Res_71_313_s.pdf

ONU (2021). Informe de las Naciones Unidas A/76/135. Recuperado de: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/89/PDF/N2107589.pdf?OpenElement

Poder Ejecutivo Nacional (2019). *Estrategia Nacional de Ciberseguridad*. Recuperado de: https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf

Resolución 1/2023 [Jefatura de Gabinete de Ministros]. Declárase la apertura del procedimiento de consulta pública respecto del documento SEGUNDA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD. 4 de enero de 2023.

Resolución 727/2020 [ENACOM]. Apruébase el "Programa de acceso a servicios TIC a poblaciones de zonas adversas y desatendidas para el despliegue de redes". 3 de julio de 2020.

Schweitzer, M. (2020). La producción de un territorio desigual en Argentina. Concentración, primacía y macrocefalia. *Redes, 25*(3), 1051-1070.

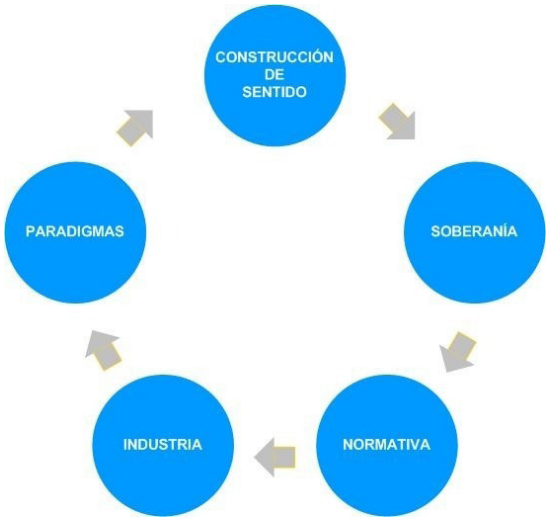
La industria nacional para la ciberdefensa

DANIEL FEIPELER GÓMEZ

Introducción

Es válido que en principio nos preguntemos si realmente es necesario hablar de industria nacional *para* la ciberdefensa. Es decir, si además de que pueda resultar deseable para los intereses nacionales, es también una condición necesaria para nuestra soberanía.

Figura 1: Ciclo Evolutivo del Ciberespacio



En lo que Oscar Niss ha denominado el Ciclo Evolutivo del Ciberespacio (como muestra la Figura 1) el nodo correspondiente a industria es simbólicamente determinado por normativa y, a su vez, determinante de los nuevos paradigmas. Claro que, si se entiende conceptualmente el Ciclo

Evolutivo como una espiral ascendente y no como un ciclo cerrado en sí mismo, se puede ver que, en cada nueva vuelta de la espiral, los nodos se co-determinan mutuamente y constantemente van incorporando, en su nueva constitución, elementos de los momentos anteriores.

La idea del Ciclo como espiral nos ayuda a comprender que la industria nacional no se relaciona únicamente con la normativa y los nuevos paradigmas, sino que estará determinada también por la construcción de sentido y lo que se conceptualice sobre la soberanía, que la precede, pero aún se encuentra presente en su realidad.

Siempre la construcción de sentido responde a intereses concretos, como dice Niss en el primer capítulo de este libro:

> *Volviendo al título que nos ocupa, según Beccaria "la construcción de sentido que surge del diálogo entre quien produce una imagen/texto y quien la reconoce a través de una práctica hermenéutica, pone en relieve el carácter permanentemente abierto que le confiere a la obra el intérpete" (2013, p. 2). Esto tiene una implicancia literal en el caso de algo tan abstracto como el ciberespacio. De esta forma, la producción del concepto asociado, consecuente de esa rutina de diálogo, nunca es producto de una situación azarosa, sino de una intención de su creador. Esa intención, que dista de una teoría conspirativa, puede ser por conservar intereses económicos o políticos, en ambos casos desbordados por tensiones geopolíticas.*

Es importante comprender que el sentido construido permanece oculto, ya que es pre-reflexivo (previo al ejercicio consciente de la reflexión). Es decir, es una certeza estratégica a la cual nadie cuestiona y por eso es "sentido común". En particular, en torno a la industria nacional, se suele construir un sentido de impotencia, de inferioridad, de "no poder", que obviamente abona intereses concretos, en este caso de potencias extranjeras dominantes y transnacionales tecnológicas.

Si el desafío está en lograr la protección del ciberespacio para resguardar la soberanía nacional, habrá que construir una normativa soberana que incentive, promueva y promocione una industria nacional para la ciberdefensa, capaz de intervenir en los paradigmas actuales y futuros, de modo que permita participar y contribuir con la construcción de sentido en favor de los intereses nacionales.

En este humilde aporte, lo que intentaremos es fundamentar la necesidad de desarrollar una industria nacional para la ciberdefensa y lo haremos en tres puntos claves.

Auditabilidad de los sistemas

El primer punto tiene que ver con la utilización de herramientas extranjeras o privativas. Cuando hablamos de herramientas para la ciberdefensa, en general son sistemas no auditables, ya sea por la licencia que los acompaña o por resguardo de secreto comercial o militar. Muchas veces esta situación impide garantizar que un sistema adquirido para una función específica cumpla efectiva y únicamente dicha función. La verificación asociada a un desarrollo de *software* proporciona la confirmación objetiva de que los resultados obtenidos cumplen los requisitos especificados en la etapa de diseño de este. Estos dos momentos, verificación y diseño, son parte del proceso de desarrollo del *software*, es decir, no se pueden realizar si solo se cuenta con el producto final, con los componentes ejecutables (sin acceso al código fuente o con restricciones de licencia).

No hay forma de garantizar que las herramientas adquiridas no realicen tareas sin el conocimiento del usuario o que no contengan vulnerabilidades de seguridad introducidas adrede (lo que se conoce técnicamente como *backdoors*). Este último aspecto es inaceptable, sobre todo si de estos sistemas depende la seguridad nacional. Probablemente el caso reciente más conocido sea la infiltración de la CIA (Agencia Central de Inteligencia de EE. UU.) y los servicios de inteligencia de Alemania Occidental en la empresa suiza Crypto AG, revelada en febrero de 2020 (Miller, 2020), por su alcance, su impacto y el tiempo que se mantuvo inadvertido. Esta empresa privada (y supuestamente neutral) abasteció durante casi 70 años a más de cien Estados con máquinas para cifrar información que podían ser vulneradas por dichos servicios de inteligencia, que, en secreto, compraron la compañía en la década de 1970. Así, EE. UU. y sus socios alemanes espiaron durante décadas a funcionarios y militares de alto rango en todo el planeta. En el caso particular de nuestro país, utilizaron la información obtenida en comunicaciones cifradas oficiales argentinas en beneficio de Inglaterra durante la guerra de Malvinas en 1982. Está claro que, cuando se trata de herramientas para la ciberdefensa, no se puede correr semejante riesgo. Es necesario contar con las capacidades para desarrollar, verificar y auditar su funcionamiento.

Capacidades necesarias

El segundo punto de fundamentación es que Argentina posee las capacidades necesarias para abordar esta problemática, como ya se ha demostrado en áreas tecnológicas de punta y por su vasto pasado de industrialización tecnológica y militar. Como bien indican Bianculli y Vercelli (2022), resulta importante no olvidar un primer momento de la informática en la Argentina. Se trata de la traducción de unos manuales por el ingeniero especialista y Capitán Naval Oscar A. Quihillalt en 1949, y el propio Sadosky unos años después. También se hace referencia al alquiler de tabuladoras de IBM para la Armada, en 1949, para la sección de Computadoras Mecánicas, dependiente de Estadística Naval (creada en 1946), además de la creación del Centro de Cómputos de la Dirección Nacional de Administración Naval en 1954, que fue equipado con tabuladoras Bull. No es la intención de este texto profundizar en esta cuestión, pero sí resulta importante hacer mención explícita en relación con el sector informático, tanto a nivel nacional como internacional, de los despliegues técnicos de primer nivel de las Fuerzas Armadas entre fines de la década de 1940 y mediados de 1955 (Bianculli y Vercelli, 2022).

En la actualidad, si nos referimos al desarrollo de tecnología informática, como puede ser el desarrollo de *software*, los abordajes desde la ciencia de datos o los algoritmos de inteligencia artificial y aprendizaje automático, Argentina posee sobradas y probadas capacidades que actualmente desarrolla. El sistema científico-tecnológico nacional está preparado y resuelve problemáticas de primer nivel mundial. Se nutre, además, de un sistema educativo masivo y de calidad en todos sus niveles. La educación pública argentina, sobre todo la educación superior, es un punto de apoyo fundamental para el sistema científico-tecnológico nacional, así como para el sector privado. Si en el país no existiese esta masa crítica estaríamos en problemas, ya que desarrollarla llevaría quizás décadas. Por lo tanto, la situación actual es una gran oportunidad.

Tecnología como destreza del trabajador

El tercer punto de fundamentación tiene que ver con entender a la tecnología no como un todo, sino como parte de un proceso social, es decir, la tecnología como medio para la producción y no como un fin en sí

misma. La tecnología no puede ser considerada únicamente desde su "aplicación", sino que es esencialmente la destreza del trabajador que la utiliza, la produce y la desarrolla (Dussel, 2014). Es necesario entender a la tecnología como un proceso vivo, que evoluciona junto con el sujeto que la utiliza, produciendo así una subjetividad productora y tecnológica.

Solo desarrollando la industria nacional se logra una apropiación y aprehensión necesaria de la tecnología. En el caso de la ciberdefensa, sin este desarrollo jamás tendremos las capacidades necesarias para la protección de nuestro ciberespacio, por más dinero que invirtiera el país en soluciones desarrolladas en el extranjero. Un caso excepcionalmente ilustrativo de esta situación lo podemos encontrar en el desarrollo de los algoritmos de inteligencia artificial. Estos algoritmos necesitan para su entrenamiento grandes cantidades de datos, experiencias pasadas de las cuales aprender. Analicemos algunos de estos algoritmos utilizados para la ciberdefensa. Por ejemplo, un algoritmo que clasifica tráfico de una red informática como benigno o malicioso: para entrenarlo habrá que utilizar grandes volúmenes de tráfico de red real con ciertas características, tanto de generalidades como de particularidades, para evitar el sesgo y sobre-entrenamiento. El *software* que pueda adquirirse en el mercado internacional utilizará algoritmos entrenados con tráfico de red de otras características diferentes de las que se pueden encontrar en las redes que se intentan proteger para la defensa nacional. En el fondo, no solo las arquitecturas y topologías de red dan constitución a un modelo de tráfico de red, sino también –y sobre todo– el comportamiento humano y organizacional detrás de los dispositivos que lo generan. Es decir, si no desarrollamos nuestros propios algoritmos, jamás podremos defender eficientemente nuestras redes.

Componentes y cooperación

Es conocida ya la propuesta del triángulo de Jorge Sábato como modelo de política científico-tecnológica para describir la cooperación intrínseca y necesaria entre el Estado, el sistema científico-tecnológico y el sector productivo. Es necesario defender esta propuesta ya que, aunque en materia de ciberseguridad y ciberdefensa pueda ser insuficiente, quizás haya que considerar seriamente cómo incorporar un cuarto nodo a este modelo: la comunidad.

El desarrollo de la comunidad –o de las comunidades– en el mundo del *hacking*[1] es realmente avanzado, a tal punto que muchos de los resultados relevantes en investigaciones de nivel mundial son presentados en eventos organizados por la misma comunidad. El mundo del desarrollo de *software*, en particular el vinculado al movimiento de *software* libre, se apoya firmemente sobre la comunidad misma que lo utiliza, evalúa, adapta y desarrolla. En el ámbito específico de la ciberseguridad esta dependencia se intensifica. No es el propósito de este texto abordar la temática en profundidad, pero sí entendemos que no es posible un desarrollo de la industria nacional para la ciberdefensa sin incorporar a las comunidades existentes.

Durante el año 2021, en nuestra participación en el grupo de trabajo de Concientización y Educación del Comité Nacional de Ciberseguridad, en representación del Ministerio de Defensa de la Nación, como parte de las actividades entrevistamos más de 30 organizaciones argentinas de la comunidad que están trabajando en la concientización y educación en materia de ciberseguridad y seguridad de la información. Es importante dimensionar y entender que los aportes de la comunidad se traducen directamente en producción de *software*, producción de documentación, incluso en identificación, clasificación y resolución de vulnerabilidades existentes.

Entendemos que cada uno de estos cuatro vértices –los tres de Sábato más la comunidad–deben asumir funciones y responsabilidades para el desarrollo de una potente industria nacional para la ciberdefensa.

Desde el Estado, esto ocurre a través de políticas públicas. Se debe impulsar no solo la producción científica y tecnológica, sino también la industria nacional. Se requiere una promoción tanto de la oferta como de la demanda. El Estado, a través de normativa específica, podría garantizar estándares de seguridad requeridos que alcanzaran a productos tecnológicos, sistemas de información y comunicación de utilización pública y privada. Podríamos asegurar el cuidado, la privacidad y la soberanía de los datos personales de todos los ciudadanos argentinos. Hay un deber importante también en torno a la normativa sobre las infraestructuras críticas de nuestro país (su identificación, clasificación y resguardo). Es responsabilidad del Estado garantizar que todos los servicios esenciales para la población y el normal desarrollo de la vida de sus ciudadanos estén debidamente protegidos. De este modo, identificando los activos críticos de información involucrados en estos procesos, se puede trabajar en su

1 Para nosotros la palabra *hacking* no está asociada a la criminalidad ni a la ciberdelincuencia, sino que está asociada a la investigación: un hacker investiga, mientras que un ciberdelincuente delinque.

protección, normando en favor de una industria nacional que asegure no solo la protección, sino también nuestra soberanía. Actualmente, como explican Moncaut, Baum y Robert (2022), la flamante Ley de Economía del Conocimiento parece más orientada a afianzar y favorecer un modelo exportador de capacidades –en las áreas de la llamada industria 4.0–, que a un entramado productivo local y un despliegue de proyectos públicos estructurantes que fomenten el fortalecimiento de trayectorias tecnológicas de alto potencial de crecimiento, como podría ser la industria nacional estratégica para la ciberdefensa.

En lo que respecta al sistema científico-tecnológico, existe la necesidad de potenciar las líneas de investigación, extensión y divulgación en todo lo que tenga que ver con seguridad de la información, ciberseguridad, ciberdefensa y seguridad informática. Reiteramos que, desde nuestra perspectiva, Argentina tiene las condiciones para profundizar estas líneas de investigación, soportadas además por la base del iceberg, que es el sistema público de educación. Sobre este mismo sistema educativo, financiado por la totalidad de la población nacional, se apoya la industria tecnológica en todas sus particularidades. Se trata de una industria nueva, sujeta a los vaivenes geopolíticos globales y que en nuestro país en particular aún debe definir su rumbo estratégico y normalizar su constitución, por ejemplo, en lo referido a la organización de los trabajadores informáticos (Moncaut, Baum y Robert, 2022), que son el gran capital que la compone, el muchas veces llamado "talento" humano que la diferencia de muchos otros países. En particular, con respecto a la ciberseguridad y la ciberdefensa, es necesario promover la integración de la industria tanto con el sector científico-tecnológico nacional como con las comunidades del área, y que se asuma el compromiso de desarrollar mejores capacidades nacionales en la materia. Es decir, fomentar una industria que crea en el talento nacional, que desarrolle sus productos aquí en la Argentina y para el crecimiento nacional. Hay en la industria de la ciberdefensa una oportunidad de ser exportadores en la materia, siempre y cuando hayamos desarrollado las capacidades nacionales. De lo contrario, sólo afianzaremos nuestra dependencia tecnológica. Vincular la industria a la comunidad de usuarios, comunicadores, colaboradores y desarrolladores es condición necesaria para desarrollar una industria nacional para la ciberdefensa de excelencia. Por último, hay que alentar a la comunidad a que continúe organizándose por sus propios medios, como lo viene haciendo. La organización comunitaria es la llave silenciosa que puede lograr que todo lo demás funcione.

Conclusión

Estamos convencidos de que, para proteger eficientemente los sistemas soberanos del ciberespacio nacional, es condición necesaria el desarrollo de una industria nacional para la ciberdefensa, con participación del sector productivo, con promoción estatal, fuertemente vinculada al sistema científico tecnológico, a las Fuerzas Armadas y a la comunidad de ciberseguridad.

Referencias

Bianculli, K. y Vercelli, A. (2022). Las historias de la informática argentina: una aproximación desde las alianzas socio-técnicas. En Vianna, M.; de Almeida Pereira, L. y Perold, C. (Org.). *Histórias da informática na América Latina: Reflexões e experiências (Argentina, Brasil e Chile)*. San Pablo: Paco Editorial.

Dussel, E. (2014). *16 Tesis de Economía Política*: interpretación filosófica. México: Siglo XXI Editores.

Miller, G. (11 de febrero de 2020). The Intelligence 'coup of de century'. *The Washington Post*. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Moncaut, N.; Baum, G. y Robert, V. (2022). ¿Hacia dónde se encamina la industria argentina de *software*? *Ciencia, Tecnología y Política*, *5*(8), 42-49.

Anexo
La inteligencia artificial aplicada a los sistemas informáticos del Estado

JOSÉ MARÍA CIFUENTES VILLANUEVA[1]

En ciertas ocasiones, el vertiginoso avance de la tecnología en estos tiempos llega al extremo de quitarnos la capacidad de sorpresa. El exceso de avances crea la percepción de que todo es posible y, por lo tanto, previsible. En esta línea de pensamiento pudimos observar, durante años, que la inteligencia artificial (IA) era un tema que llegaría algún día, casi como en una película de ficción en la cual los autos del futuro se conducen en forma autónoma por vías aéreas, pero creo que no advertimos que íbamos a encontrarnos con ella tan rápidamente. Por eso no nos sorprende su aparición intempestiva.

No obstante los desarrollos que se vienen realizando en todos los ámbitos, noviembre de 2022 marcó un hito en la evolución de la inteligencia artificial: OpenAI lanzó su aplicación ChatGPT. Se trata de un prototipo de inteligencia artificial programado especialmente para dialogar con personas a partir de un modelo de lenguaje ajustado, con técnicas de aprendizaje precargado y configurado para continuar aprendiendo según las conversaciones con los distintos usuarios.

La revolución tecnológica se dio, básicamente, a partir de la apertura del código de *software* de ChatGPT, que permitió la multiplicación de su uso en miles de aplicaciones nuevas con fines muy diversos. Entre ellos, podemos encontrar aplicaciones que permiten crear imágenes netamente realistas, leer grandes cantidades de páginas e interpretarlas en segundos, hasta armas de guerra que tienen la capacidad de elegir el objetivo y efectuar el disparo sin necesidad de contar con la aprobación humana.

---

1 Director del Departamento de Cibercrimen del Departamento Judicial Pergamino, Ministerio Público Fiscal de la provincia de Buenos Aires

La evolución es inevitable

Existen varios aspectos que debemos tener en cuenta a partir de esta evolución tecnológica de la que somos testigos. En primer lugar, el aspecto ético. Si bien el desarrollo de la inteligencia artificial demostró su valor para hacer frente a la pandemia generada por el COVID-19, al procesar grandes cantidades de datos en la carrera por encontrar una vacuna o un tratamiento adecuado, también permitió la contención de la propagación del virus a través de tecnologías de prueba, seguimiento y localización de focos virales. Esta contribución generó ciertos temores en lo relativo a la privacidad de las personas, el manejo de grandes volúmenes de datos y el efectivo uso de estos, más allá de las necesidades de seguimiento del virus particular.

Su intempestiva irrupción en la vida cotidiana nos permite identificar algunos dilemas éticos que pueden generarse, tales como posibles discriminaciones o sesgos de género con origen en representaciones estereotipadas, su utilización dentro de las instituciones del Estado, la cuestión derivada del derecho de propiedad intelectual, el derecho a la imagen o su aplicación en el ámbito comercial, entre otros.

En segundo lugar, el aspecto social. Aquí cabe consignar que el problema social que puede generar su implementación masiva estaría dado, en primer término, por las implicancias laborales que la inteligencia artificial puede generar, así como la necesidad de su regulación por parte del Estado argentino.

Y por último, en tercer lugar, el aspecto económico, derivado principalmente de las consecuencias generadas por un posible aumento vertiginoso de la tasa de desempleo.

¿Quién podrá controlar a la inteligencia artificial?

La interrogante que se nos genera cuando dejamos que un *software* decida en forma autónoma es: ¿podemos confiar en la tecnología algo tan propio del ser humano? Me refiero a la facultad humana de pensar y empatizar con el otro.

En este punto, el filósofo surcoreano Byung-Chul Han manifestó que "La inteligencia artificial no puede pensar porque no se le pone la carne de gallina. Le falta la dimensión afectivo-analógica, la emoción que los datos y la información no pueden comportar" (Byung-Chul, 2021, p. 54) y creo

que tiene razón en que la inteligencia artificial solo es un *software* (auqnue de lo más moderno) que puede efectuar operaciones lógicas similares a la de las personas, pero que carece de la capacidad de emocionarse y razonar tal como los seres humanos. Agrega: "La inteligencia artificial es apática, es decir, sin pathos, sin pasión. Sólo calcula" (ibíd., p. 56).

Allí radica la dificultad y necesidad del abordaje ético de la cuestión, porque la creación de proyectos de innovación tecnológica en el ámbito de la administración pública requiere de la concepción de una ideología profundamente humanista al momento de la configuración de los algoritmos que se inmiscuirán en datos sumamente sensibles de la población en general.

Administración de la cuestión pública en tiempos 4.0

Ahora bien, al margen de las cuestiones abstractas y las implicancias disruptivas de esta nueva tecnología, cabe reflexionar acerca de las implicancias prácticas y operativas que puede generar la utilización de las nuevas herramientas que nos proporciona la IA. Este espectro va desde la digitalización de los procesos administrativos hasta el uso de la inteligencia artificial como método para la realización de tareas simples, rutinarias y repetitivas en los distintos ámbitos del Estado moderno.

Cuando hablamos de digitalización de las operaciones del Estado tenemos que razonar que el Estado moderno recolecta cada vez mayor cantidad de datos de todo tipo, y por lo tanto debe almacenarlos y conservarlos como material probatorio futuro, utilizando para ello recursos informáticos muy costosos. Allí radica la importancia de planear una estrategia nacional de gobernanza de datos, ubicando a la información en el centro de un gobierno tecnológico respetuoso de las garantías constitucionales.

La *big data* y su relación con la toma de decisiones críticas

Desde hace décadas, el sector público y el sector privado recolectan y almacenan información de todo tipo (personal, bancaria, penal, tributaria, comercial, etc.), que administran según las regulaciones que surgen en las

distintas áreas e incumbencias. Sin embargo, aún carecemos de una estrategia nacional que no solo regule la utilización de la información acorde al estado de derecho imperante, tal como lo plantea la actual Ley Nacional de Protección de Datos Personales (Ley 25.326), sino que además utilice esos datos almacenados de forma tal que puedan conectarse entre sí, en la medida de lo posible con fines estratégicos. Esto puede ocurrir efectivamente en algunas áreas de la administración pública nacional, de las provincias o de los municipios, pero estos mismos ámbitos aún no comparten dicha información en forma automática.

En el sigo XXI podríamos afirmar que tomar decisiones estratégicas es administrar *big data*. Por lo tanto, de una correcta recopilación y análisis de la información se pueden derivar las grandes directivas relativas a la gestión de la cuestión pública. Para lograr dicho objetivo, es crítica la etapa de recopilación de la información. En este punto es clave definir y estandarizar los procesos de toma de datos, ya sea de forma humana o automática, porque este es uno de los grandes generadores de problemas futuros, como la duplicación de datos o errores de origen.

De esta forma, se debe garantizar consistencia y calidad de la información, para que permita la creación de modernos procesos de trabajo posibles de realizar. Luego, ya con la información recolectada de forma totalmente lícita, debemos crear el marco regulatorio necesario para comenzar a trabajar sobre ella, permitiendo, por un lado, una verdadera innovación de la relación de la ciudadanía en general con la administración pública y, por el otro, el comienzo de la interactuación de los sistemas programados con inteligencia artificial con los datos cargados a fin de generar informes, reportes y demás aplicaciones de utilidad.

El adiós a la burocracia eterna

Todo esto es interesante, pero debemos bajarlo a la realidad. ¿Es posible que el Estado argentino elabore y articule efectivamente una Estrategia Nacional de Gobernanza de Datos para la aplicación directa de la inteligencia artificial en la colaboración con la toma de decisiones críticas? No cabe duda de ello si se cuenta con la voluntad y la férrea decisión de robustecer los proyectos de innovación bajo cánones estrictamente éticos, junto con, por supuesto, la disposición de los fondos necesarios para llevar a cabo dicha tarea.

Si bien la optimización de carga inicial es un punto muy importante para trabajar, otro que se destaca es la posibilidad de compartir bases de datos con fines específicos regulados por ley para lograr una mayor eficiencia a la hora de la toma de decisiones, en las cuales el interés público se vea directamente involucrado.

Imaginemos por un instante que una fiscalía de la provincia de Buenos Aires pueda tener acceso a las bases de datos registrales del Estado nacional y a las investigaciones llevadas a cabo por una fiscalía de una provincia distinta a la hora de avanzar en un proceso penal concreto. Técnicamente es factible, pero no se pueden soslayar los riesgos asociados a dicha implementación. Si contar con una base de datos puntal es complicado, permitir que varias bases se conecten entre sí, en forma automática y desde diversas jurisdicciones, podría generar grandes inconvenientes si no se piensa y configura con los máximos estándares de seguridad, protegiendo a la ciudadanía en general de las posibles filtraciones y de la manipulación incorrecta de la información allí inserta.

Pensemos los efectos potenciadores que dicha interactuación podría brindarle al Estado nacional y a las provincias. Y ahora imaginemos a la inteligencia artificial asociada a dicho proceso. Obtenemos ventajas tales como la posibilidad de efectuar un control de expedientes administrativos, entrecruzamiento de datos con fines de investigación criminal y seguridad nacional, seguimiento de procesos de compra directa o licitación, identificación de infraestructuras informáticas críticas y gestión eficiente del expediente judicial, entre muchas otras. La enumeración de todas deviene una verdadera tarea imposible.

Aspectos de la regulación normativa de la inteligencia artificial

Como se puede observar, las implicancias técnicas no son las únicas a tener en cuenta. Y si bien una regulación legal de los avances tecnológicos siempre está sujeta a quedar rápidamente desactualizada, es necesario acordar políticas de uso común para evitar que esta revolución tecnológica genere más problemas que soluciones.

En este sentido, la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), reunida en París del 9 al 24 de noviembre de 2021, en su reunión número 41

aprobó la Recomendación sobre la Ética de la Inteligencia Artificial, por la cual recomendó que los Estados miembro apliquen de manera voluntaria sus disposiciones, mediante la adopción de las medidas adecuadas, en particular las medidas legislativas o de otra índole que puedan ser necesarias, de acuerdo con la práctica constitucional y las estructuras de gobierno de cada Estado, con el fin de dar efecto en sus respectivas jurisdicciones a los principios y normas enunciados en dicha recomendación, de conformidad con el derecho internacional, incluido, por supuesto, el derecho internacional de protección de los derechos humanos.

Asimismo, recomendó a los Estados miembro que hagan partícipes a todas las partes interesadas, incluidas las empresas, para asegurarse de que desempeñen sus respectivas funciones en la aplicación de la mencionada recomendación y que la difundan a las autoridades, organismos, organizaciones universitarias y de investigación, instituciones y organizaciones de los sectores público, privado y de la sociedad civil que participan en las tecnologías de la IA, para que su desarrollo y la utilización se guíe tanto por una investigación científica sólida como por un análisis y una evaluación éticos.

Esta recomendación mundial, si bien no es el único texto normativo global, marcó un norte para todos los Estados miembro. La República Argentina, mediante la Disposición 02/2023 de la Jefatura de Gabinete, adhirió a sus postulados y aprobó, en consecuencia, las Recomendaciones para una Inteligencia Artificial Fiable.

Comienzos de la regulación en nuestro país

La Disposición 02/2023 (Boletín Oficial, 2 de junio de 2023) busca ofrecer herramientas teóricas y prácticas para quienes forman parte del sector público, ya sea liderando proyectos de innovación, desarrollando tecnologías, adoptando tecnologías desarrolladas por otros equipos técnicos o proveedores, o formulando las especificaciones técnicas para esas adquisiciones. Distingue claramente los conceptos de responsabilidad y ejecución, estipulando que, cuando se contratan servicios tecnológicos (como la utilización de algoritmos), al proveedor se le transfiere la ejecución de distintas tareas, pero no la responsabilidad de su realización.

Es decir, la inteligencia artificial únicamente lleva a cabo una ejecución sin intención propia y de manera reactiva a una solicitud humana, quien decide programarla, entrenarla e implementarla con un destino de uso específico, con el fin de que ejecute distintas acciones. En consecuencia,

surge que un algoritmo no posee autodeterminación para tomar decisiones libremente, y por ende no se le pueden atribuir responsabilidades de las acciones que se ejecutan a través de dicho algoritmo. Dicho con otras palabras, para que una persona humana pueda ser jurídicamente responsable sobre las decisiones que tome la IA para realizar una o más acciones, debe existir discernimiento, intención y libertad. Por ello resulta importante establecer la concepción de las inteligencias artificiales como artificios, es decir, como tecnología, una cosa, un medio artificial para lograr objetivos humanos pero que no deben confundirse con una persona humana. Es decir, el algoritmo puede ejecutar, pero la decisión debe necesariamente recaer sobre la persona y, por lo tanto, también la responsabilidad.

Vemos que esta disposición comienza por delinear aspectos de la responsabilidad legal subyacentes al avance de la inteligencia artificial y termina por elaborar una verdadera guía de implementación de la IA desde el inicio del proyecto hasta su implementación en la práctica.

El abordaje de proyectos de innovación tecnológica

La flamante Disposición 02/2023 enumera exhaustivamente los principios éticos que se recomienda incorporar a todas las fases del diseño e implementación de un proyecto de inteligencia artificial. Entre ellos podemos encontrar los de proporcionalidad e inocuidad, seguridad y protección, equidad y no discriminación, sostenibilidad, derecho a la intimidad y protección de datos, supervisión y decisión humanas, transparencia y explicabilidad, responsabilidad y rendición de cuentas, sensibilización y educación, gobernanza y colaboración adaptativas de múltiples partes interesadas, crecimiento inclusivo, desarrollo sostenible y bienestar.

Esta disposición del Poder Ejecutivo Nacional recomienda conformar un equipo humano diverso y multidisciplinario antes de comenzar con el ciclo de la inteligencia artificial, para abordar los desafíos éticos, comprender las implicaciones sociales, priorizar resoluciones centradas en el usuario, evitar sesgos y discriminación y fomentar la innovación. De esta forma, luego podremos formularnos un interrogante muy interesante: ¿es excluyente el uso de inteligencia artificial para el problema que se quiere resolver? Decimos interesante porque desde el comienzo del presente capítulo ensalzamos las bondades de la tecnología en general y la IA en particular, pero siempre debemos recordar el punto de partida. ¿Es realmente necesario utilizarla?

En épocas en las que se impone el estudio de las implicancias prácticas que conllevará la aplicación de la IA, este interrogante debe guiar el accionar de la administración pública. Aquí cabe preguntarnos si es necesario permitir la interactuación automática de diversas bases de datos y si a dicho proceso podemos aplicarle los efectos potenciadores de la inteligencia artificial o no. Considero que debemos tomar la inteligencia artificial como una aliada de los intereses comunitarios en la medida que mejore sustancialmente el trabajo de la administración pública, redundando en beneficios palpables para los ciudadanos y ciudadanas. La innovación por la innovación misma carece de sentido si no es en beneficio de la vida social.

En un mundo que nos lleva a encerrarnos en nuestras pequeñas burbujas "inteligentes" debemos "*hackear*" la lógica del sistema para potenciar la vida en comunidad y fortalecer los lazos sociales reales.

Por último, la Disposición 02/23 divide en cuatro etapas el proceso de creación e implementación de los proyectos de innovación tecnológica: 1) diseño y modelado de datos; 2) verificación y/o validación; 3) implementación; y 4) operación y mantenimiento.

A modo de conclusión

Al inicio del presente capítulo nos preguntábamos si era posible que el Estado argentino elaborara y articulara efectivamente una estrategia nacional de gobernanza de datos para la aplicación directa de la inteligencia artificial en la colaboración de la toma de decisiones críticas. Al respecto cabe concluir, entonces, que ello es posible si se logran los consensos necesarios para llevar a cabo dicha decisión, como una política de Estado en la cual se deberá elaborar una estrategia donde se clarifiquen los diversos acuerdos y compromisos arribados para la elaboración de procesos de trabajo transparentes y democráticos, tales como la creación de una sólida interacción entre bases de datos digitales de interés nacional de acuerdo con la ya mencionada Ley Nacional de Protección de Datos Personales, que permita la creación de algoritmos de inteligencia artificial para su análisis y sistematización en la toma de decisiones críticas.

Referencias

Byung-Chul, H. (2021). *No-cosas. Quiebres del mundo de hoy*. Madrid: Editorial Taurus.

Disposición 2/2023 [Poder Ejecutivo Nacional]. Apruébanse las "Recomendaciones para una Inteligencia Artificial Fiable". 1 de junio de 2023.

Ley 25.326. Protección de los datos Personales. 30 de octubre de 2000.

UNESCO (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. Recuperado de: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa

Autoras y autores

(EN ORDEN ALFABÉTICO)

MARIELA CARDOZO

Es abogada y magister en Derecho Administrativo de la Economía por la Universidad Católica de Cuyo. Además, es doctora en Ciencias Jurídicas y Sociales por la Universidad de Mendoza. Publicó en editoriales de Argentina y México. En este último es Consejera de la Editorial Criminogénesis. Actualmente trabaja en la Dirección General de Asuntos Jurídicos del Ministerio de Defensa.

JOSÉ MARÍA CIFUENTES VILLANUEVA

Es abogado por la Universidad Católica Argentina. Tiene un posgrado en Cibercrimen y Evidencia Digital por la Universidad de Buenos Aires. Es director del Departamento de Cibercrimen del Ministerio Público Fiscal del Departamento Judicial Pergamino de la provincia Buenos Aires. Además, es referente de Investigación Digital de la Procuración General bonaerense. Es docente por concurso de la cátedra de Derecho Público, director de la Diplomatura Universitaria de Posgrado en Cibercrimen e Investigación Penal por Medios Digitales y secretario de la Cátedra Libre Nicolás Maquiavelo de la Universidad Nacional del Noroeste de la provincia de Buenos Aires. Asimismo, es speaker, *disertante y organizador de diversas charlas y capacitaciones relativas a las nuevas tecnologías y la investigación penal digital.*

JULIÁN DI CÉSARE

Es ingeniero Industrial, especialista en Aplicaciones Tecnológicas de la Energía Nuclear y magíster en Ciberdefensa y Ciberseguridad (tesis pendiente). Desarrolló tareas de análisis de seguridad y diseño termohidráulico y neutrónico en centrales nucleares de potencia. También de simulación y modelado de sistemas físicos. Actualmente, se desempeña como director de Protocolos y Asuntos Regulatorios de la Ciberdefensa en la Subsecretaría de Ciberdefensa del Ministerio de Defensa de la Nación.

DANIEL FEIPELER GÓMEZ

Desde 2004 vive en Tandil, provincia de Buenos Aires. Es informático de profesión y analista programador universitario. Estudió Ingeniería de Sistemas en la Facultad de Ciencias Exactas de la Universidad Nacional del Centro, en la Provincia de Buenos

Aires. Su interés profesional está en la ciberseguridad, la programación, el software *libre y la inteligencia artificial. Dirigió proyectos de investigación en la Universidad de la Defensa Nacional (UNDEF), donde ejerce como docente en el Instituto de Ciberdefensa de las Fuerzas Armadas (ICFFAA). Ha dictado materias sobre las temáticas de lenguajes y programación, análisis de* malware *y desarrollo seguro. Desde el año 2020 se desempeña como director de Políticas y Seguridad de la Información en la Subsecretaría de Ciberdefensa del Ministerio de Defensa de la Nación.*

ALDO FELICES

Es licenciado en Sistemas de Información, egresado de la Universidad Tecnológica Nacional – Facultad Regional Rosario. Fue docente en dicha universidad en la carrera de Análisis Universitario de Sistemas y en Ingeniería en Sistemas de Información. Ha dictado seminarios de Sistemas de Computación en la Licenciatura en Sistemas de la Universidad Nacional de Rosario (UNR). Tiene un posgrado de especialidad en Gestión Estratégica de Tecnología Informática de la Facultad de Ciencias Económicas y Estadísticas de la misma universidad, además de ser psicólogo egresado de la Universidad Nacional de Rosario y docente de la carrera de Psicología. Asimismo, es docente de la carrera de Psicología del Instituto Universitario Italiano de Rosario, donde también cursa el doctorado en Ciencias Biomédicas. Como profesional independiente, es titular desde 1991 de Kernel Informática, empresa dedicada al análisis, desarrollo e implementación de sistemas para cooperativas agropecuarias y acopios. Es socio de Madrygal SRL, empresa dedicada a seguridad informática y de la información.

OSCAR NISS

Es licenciado en Administración Pública, subsecretario de Ciberdefensa de la Nación desde 2019, miembro del Comité Nacional de Ciberseguridad y miembro de la Comisión Argentina en el Grupo de Trabajo de las Naciones Unidas sobre Paz y Seguridad en el Ciberespacio. Fue director general de Ciberdefensa en 2014-2015 y asesor TIC en la Honorable Cámara de Diputados de la Nación 2005-2013. Se desempeñó como profesor en la Facultad de la Defensa Nacional, la Escuela de Guerra Conjunta y la Universidad Nacional del Noroeste de la Provincia de Buenos Aires. Además, fue profesor invitado en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires, en la UADE y en otras universidades. También fue disertante en eventos nacionales e internacionales, además de miembro del Comité Ejecutivo y Comisión Directiva de la Cámara Argentina de Software y Servicios Informáticos (CESSI) del 2007 al 2013.

ARIEL VERCELLI

Es investigador del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), con lugar de trabajo en el Instituto de Humanidades y Ciencias Sociales (INHUS), unidad ejecutora de doble dependencia del CONICET y la Universidad Nacional de Mar del Plata (UNMDP). Es doctor en Ciencias Sociales y Humanas por la Universidad Nacional de Quilmes (UNQ), magíster en Ciencia Política y Sociología por FLACSO Argentina. A su vez, tiene posgrados en Informatización Nacional por la Agencia Coreana para las Oportunidades Digitales (KADO-NIA), en Derecho de Internet por Harvard Law School, en Propiedad Industrial por la Universidad de Buenos Aires (UBA) y en Derecho de Autor y Derechos Conexos por la UBA. Es escribano por la Universidad Nacional de Rosario (UNR) y abogado por la UNMdP. Realizó cursos de capacitación y actualización profesional en Perú (INICTEL-ITU), Costa Rica (ICE-ITU), Corea del Sur (NIPA) y la Organización Mundial de la Propiedad Intelectual (OMPI). Dictó cursos de posgrado en UNQ, UNMdP, UNSAM, UNTREF, UNS, CAICYT-CONICET y ECAE-PTN. Fue docente de grado en la UNMdP, FSOC-UBA y la FD-UNR.

“El ciclo evolutivo del ciberespacio propone las ideas centrales de un marco referencial de nivel estratégico, que contribuya en el diseño de políticas de gobierno para el ambiente cibernético”. Con esa intención este libro transcribe una serie de conferencias que giran en torno a la idea central acerca de la necesidad de tener una visión holística y completa de las distintas dimensiones que atraviesan al funcionamiento del ciberespacio, el desafío de las tecnologías disruptivas para la sociedad, su construcción discursiva, el debate acerca de sus aspectos soberanos, la necesidad de normativas legales y el devenir de una industria que consolide un desarrollo sostenible.

“Cómo se gobierna internet, cómo se despliegan y administran las redes de telecomunicaciones por las que discurren los datos, cuál es la dinámica de investigación, desarrollo y comercialización de hardware y software, cuánto la dependencia tecnológica o comercial condiciona los grados de soberanía ciberespacial, son interrogantes inevitables. Asegurarse el funcionamiento de cuotas o porciones del ciberespacio pasa a ser una necesidad para los estados si quieren mantener los niveles de funcionamiento adecuados y satisfacer los requerimientos y aspiraciones de sus ciudadanos, que cada vez más lo perciben como una herramienta i ndispensable de la vida cotidiana”.

Sergio Rossi