Estado abierto, Vol. 5, N.º 3, 2021, pp. 69-93
ISSN 2618-4362

Cybersecurity en la era exponencial: la política de Obama

Por *Andrés Nadur**

Resumen

El objetivo de este trabajo es señalar el impacto que la revolución tecnológica tiene en las agendas de los gobiernos a través del análisis de una política pública específica: el Plan de Acción de Ciberseguridad de la administración del expresidente estadounidense, Barack Obama. Los desafíos propios de esta era, en relación con la seguridad de las/os ciudadanas/os, tendrán un efecto cada vez mayor en el manejo de la gobernabilidad y, potencialmente, en la legitimidad de los gobiernos. Con el fin de dimensionar su amplio impacto, a continuación, se intenta abordar el contexto global signado por las nuevas amenazas y formas de cibercrimen. Seguidamente, se abordan los aspectos principales de esta política, su definición, objetivos, acciones, actores involucrados y resultados. Finalmente, se exponen algunas conclusiones acerca de la complejidad de la acción estatal y las transformaciones de la agenda pública a raíz de los nuevos desafíos que representa el rápido avance de la era exponencial.

Palabras clave

Estado, revolución tecnológica, era exponencial, ciberseguridad, gobernabilidad.

Abstract

The aim of this work is to stand out the impact that the technological revolution has had on governments' agendas by means of the analysis of a specific public policy, known as the Cybersecurity Action Plan of Obama's administration. The challenges associated to this era, in relation to citizens' security, will have a growing effect on governance management and, potentially, on government legitimacy. An analysis of the global context marked by new threats and different forms of cybercrime is carried out in order to dimension its wide impact. The analysis covers the main aspects

* Licenciado y profesor en Ciencia Política por la Universidad del Salvador. Aspirante a la carrera diplomática, ingresó como becario al Instituto del Servicio Exterior de la Nación en 2020.

andnadur@gmail.com

https://orcid.org/0000-0003-3064-3739

of the policy, its definition, objectives, actions, stakeholders and outcomes. Ultimately, the work shares some conclusions regarding the complexity of the policy-making process and the transformation in the public agenda as a result of the new challenges that the fast advance of the exponential era represents.

Key words

State, technological revolution, exponential era, cybersecurity, governance.

1. Introducción

La definición weberiana de Estado lo presenta como el conjunto de instituciones que detentan el monopolio de la violencia legítima —o coerción— en un determinado territorio. Según la perspectiva de gran parte de los filósofos contractualistas, el Estado se ha constituido con el fin principal de proveer a las/os ciudadanas/os de la seguridad necesaria para poder desarrollar plenamente las actividades sociales. La revolución tecnológica —llamada por algunas/os «cuarta revolución industrial»—, que surge a partir de la década del setenta y que redobla sus avances cada año, trae aparejadas múltiples ventajas para el desarrollo social, económico, político y cultural de las naciones, como también nuevas amenazas que desafían el objetivo principal por el cual el Estado ha sido constituido: la provisión de seguridad. Hoy en día, además de tener que atender las tradicionales formas de inseguridad y delito que amenazan la convivencia pacífica, el orden público, la seguridad nacional o los derechos de las/os ciudadanas/os, la agenda de los gobiernos se ve ampliada por las problemáticas que acarrean los cambios tecnológicos de la era exponencial.

Las nuevas formas de delito, facilitadas por la expansión de las plataformas y medios virtuales, nos han llevado a revisar los ámbitos de intervención del Estado. Mientras que la soberanía ha sido siempre pensada desde «lo territorial», el ciberespacio escapa a esa territorialidad, lo que da origen a toda una discusión jurídica acerca de hasta dónde debe intervenir la jurisdicción estatal en los espacios cibernéticos. Sin embargo, como ha dicho Del Carril:

> … si bien la tensión respecto del grado de intensidad de la intervención regulatoria del Estado en el ciberespacio es todavía una cuestión abierta, parece existir un cierto consenso en que es necesaria la presencia estatal en hechos y acciones que pueden afectar la seguridad individual, en especial en materia penal (2020, p. 74).

En el corto plazo, estos nuevos temas de la agenda de seguridad —que no solo constituyen una amenaza para las/os ciudadanas/os, sino también para el propio Estado— serán claves en la política de todos los gobiernos e impactarán cada vez más en las variables a tener en cuenta para medir la eficacia de la acción gubernamental. Por ende, puede resultar útil para los países en desarrollo observar cómo está incidiendo esta cuestión en la agenda de los gobiernos que se encuentran en etapas más avanzadas de la actual era tecnológica. Además, las problemáticas propias de este período tendrán un efecto cada vez mayor en los niveles de gobernabilidad y, potencialmente, en la legitimidad de los poderes del Estado. Siguiendo a Oszlak: «la globalización ha hecho más compleja la tarea de gobernar», a la vez que «… el riesgo informático se ha convertido en una función permanente de los gobiernos, y el test real de un desempeño efectivo será seguramente la capacidad de anticipar y contrarrestar la actividad de los ciberatacantes» (2019, p. 10). La eficacia del Estado en resolver problemas de seguridad individual y colectiva está en la raíz misma de su formación, pero la era exponencial desafía de diversos modos su *capacidad institucional*.

Este trabajo se propone estudiar un tema que se encuentra íntimamente relacionado con la agenda del Estado en la llamada era exponencial. Específicamente, interesa responder de qué manera Estados Unidos evaluó y manejó, durante la administración del presidente Barack Obama (2008-2016), las cuestiones que atañen a la seguridad nacional y la salvaguardia de los derechos individuales que pueden verse amenazados con el avance de las nuevas tecnologías. En este sentido, nos centraremos en conocer qué líneas de acción decidió seguir este gobierno para fortalecer lo que se conoce como *ciberseguridad*, a la luz de este ejemplo de política pública: el Plan de Acción de Ciberseguridad Nacional de los Estados Unidos (CNAP, por sus siglas en inglés).

En primer lugar, expondremos, a modo de ejemplo, algunas problemáticas de seguridad que vienen de la mano de la tecnología y que forman parte del contexto de la política pública en la era exponencial. Oszlak y O'Donnell (1976) sostienen que el análisis de la política estatal debe tener en cuenta diferentes contextos: a) el que atañe a la definición de la cuestión y a los actores que se movilizan en torno a ella, es decir, a la política estatal en sí misma; b) un segundo nivel de contexto definido por la «agenda de cuestiones»; y c) la estructura social como contexto de la agenda. Debido al límite de extensión de este trabajo, solo abordaremos el primero y el tercero de estos contextos. Resaltamos, con respecto a este punto, la complejidad y el cambio permanente que se da en la era digital.

Seguidamente, nos dedicaremos a analizar la política estatal de ciberseguridad —o *cybersecurity*— del presidente Barack Obama, cristalizada en el CNAP. Esto incluye el análisis del nacimiento de la cuestión, la toma de posición del Estado, los actores a favor y en contra de la iniciativa, la implementación de la política, las cristalizaciones institucionales a que dio lugar y, de manera genérica, los impactos que ha tenido.

A modo de conclusión, expondremos algunas reflexiones finales que se desprenden del análisis de este caso de política estatal y su relación con la capacidad institucional del Estado en la era exponencial.

2. El contexto global de la política de ciberseguridad

Estamos inmersos en lo que Marks (2017) llama «la era de la inseguridad digital». Es indudable que, en las últimas décadas, se ha avanzado exponencialmente en la producción, distribución y manejo de tecnologías de la información y la comunicación (TIC). A su vez, hemos presenciado el nacimiento de nuevos fenómenos tecnológicos (internet de las cosas, algoritmos, *big data*, *blockchains,* criptomonedas, impresiones 3D, inteligencia artificial y robótica). Todo ello suma nuevos temas a la agenda de los gobiernos y exige de su parte una toma de posición, ya que estos avances impactan en numerosos aspectos de la vida social. El tema resulta urgente ya que las mismas tecnologías que hoy sirven para lidiar con un problema que amenaza la seguridad nacional, como es la pandemia

del COVID-19, pueden ser las causantes de otros problemas graves de seguridad. La magnitud de estos cambios hace que nos preguntemos si los gobiernos están lo suficientemente preparados para enfrentar los desafíos de la era exponencial.

Cabe aclarar que la revolución tecnológica tiene una lógica de crecimiento propio muy potente, que goza de gran autonomía y escapa a cualquier posibilidad de querer impedirla. De este modo, vemos cómo, a lo largo de la historia, las tecnologías se van imponiendo: comienzan por invadir los sistemas de las sociedades más avanzadas y de allí se diseminan a los países en desarrollo. Por ende, la incorporación de las nuevas tecnologías se dará tarde o temprano en todos los ámbitos. Todo parece indicar que la inclusión de las TIC en la agenda de los gobiernos —y los riesgos que estas potencialmente implican para la ciudadanía— es un proceso inevitable. Es decir que aquellos Estados rezagados en la discusión de esta problemática deberían ponerse al día si no quieren que los nuevos desafíos los sorprendan «flojos de papeles»[1]. Lo que se observa, generalmente, es que los Estados reaccionan *a posteriori* de la aparición de los problemas. Esta lógica reactiva de la administración estatal lleva a que varios conflictos se desarrollen de manera desproporcionada hasta que los organismos públicos les dan respuesta —con enormes pérdidas en el ínterin—, o que, incluso, la gravedad de la problemática haya aumentado a niveles que dificultan su solución.

Sin dudas, es muy complejo dar cuenta de todas las amenazas que las nuevas tecnologías traen aparejadas. Se trata de un enorme abanico de asuntos que deberán ser parte de la agenda de seguridad de los gobiernos. Por un lado, están aquellas nuevas modalidades que se dan en el ámbito de viejas formas de crimen.

[1] Oscar Oszlak, en «La gestión pública en la "era exponencial": desafíos para los países emergentes» (2019), advierte sobre la necesidad de aumentar la capacidad de anticipación y preparación del Estado para enfrentar y adaptarse a los cambios de la nueva era tecnológica. En «Government for the future: reflection and visión for tomorrow's leaders» (Abramson *et al.*, 2018), Michael J. Keegan afirma que el mundo actual: «está plagado de incertidumbre (…). La creciente complejidad e interconexión de la sociedad de hoy aumenta el grado de lo desconocido. Lo que hace a la diferencia tanto para individuos como organizaciones es cómo pueden manejar este ambiente de incertidumbre, con riesgos que van desde lo financiero hasta lo operacional, pasando por lo reputacional. El modo de manejar esta incertidumbre es construir capacidad de gobierno para anticiparse y ser resiliente, a fin de prepararse para el futuro y sus efectos» (p. 140, traducido del original).

Es lógico que las TIC doten de nuevos recursos a los grupos criminales para que innoven al momento de cometer delitos tradicionales (secuestros virtuales; tráfico de armas, drogas y personas en la *deep web*; comunicaciones encriptadas; uso de explosivos manejados a distancia por grupos terroristas; etc.).

Por otro lado, las innovaciones tecnológicas posibilitan la aparición de nuevos delitos, es decir, de ilícitos que no podrían llevarse a cabo sin el recurso científico-técnico. Estos últimos, sin dudas, son los más complejos y los que aquí nos interesan, ya que comprenden el objetivo principal de la política de ciberseguridad. Mientras que los delitos tradicionales —a los que hoy se les agrega la complejidad de la tecnología—están mayormente incorporados en todas las agendas estatales, los nuevos delitos informáticos requieren de originales mecanismos de seguridad para prevenirlos y combatirlos, lo que amplía significativamente la agenda del Estado. Este tipo de delitos posibilita la circulación de miles de millones de dólares que van a parar a manos de los *ciberdelincuentes*. Según el informe *Cyber incidents and brench trends* de 2018 —uno de los mejores estudios sobre esta cuestión—, realizado por The Internet Society, el cibercrimen significó una pérdida anual de 45 mil millones de dólares (Pandasecurity, 2019).

En cuanto al caso específico de Estados Unidos, luego de analizar diferentes entrevistas realizadas al expresidente Barack Obama, podemos identificar cuáles son aquellas amenazas que preocupaban a su administración desde sus mismos inicios y que formaban parte del análisis del contexto que realizaba el gobierno estadounidense, punto de partida del Plan de Ciberseguridad que diseñaría posteriormente. Obama reconoció que había que «hacerse de un nuevo vocabulario para estar un paso delante de los cibercriminales» (The Obama White House, 2017). Este nuevo léxico incluía términos como espionaje cibernético, virus informáticos, *phishing*[2], *botnet*[3], *ransomware*[4], entre otros.

[2] Se conoce como *phishing* a la práctica por la cual, mediante correos electrónicos que fingen provenir de compañías o agencias oficiales, un estafador informático (*phisher*) engaña a su receptor con el fin de robarle información personal o confidencial para cometer otros delitos.

[3] Robots informáticos que operan como si fueran usuarios humanos.

[4] Se denomina *ransomware* a la operatoria de un programa dañino (o virus) que bloquea el acceso a ciertas partes o archivos de un programa y que exige del usuario el pago de una cierta suma para

Uno de los ciberdelitos de mayor crecimiento en Estados Unidos, en la primera década del presente siglo, fue el «robo de identidad». Esta forma de estafa, que puede dar origen a un sinfín de actos ilícitos, fue una de las principales preocupaciones dentro de la agenda de ciberseguridad de Barack Obama, ya que había significado miles de millones de dólares en pérdidas a la economía estadounidense en los años previos.

Proteger la seguridad de las transacciones comerciales se vuelve una política prioritaria en el contexto económico estadounidense, donde el *e-commerce* mueve ingentes cantidades de dinero. Según el índice mundial de comercio electrónico, Estados Unidos generó un producto de más de 500 mil millones de dólares en 2019 por ventas minoristas en internet[5], mientras que, a la llegada de Obama al Gobierno, esta cifra ascendía a 123 mil millones. Las estimaciones para este año, debido a que la pandemia de COVID-19 incrementó las ventas *online*, superan ampliamente las cifras anteriores. Cada vez son más frecuentes en cantidad e intensidad los llamados «ciberataques» a empresas e individuos. Los *hackers* han avanzado hacia redes de crimen organizado, lo que vuelve a la cuestión mucho más compleja. Ya no se trata de exempleados descontentos con una compañía a la que quieren perjudicar o de genios cibernéticos que buscan hacer dinero del secuestro de datos, la venta de antivirus o el tráfico de información. Hoy en día, existen redes de delincuencia que se dedican al delito informático de manera exclusiva. A esta amenaza, se suma el espionaje internacional en búsqueda de secretos de Estado o los llamados «espías industriales», quienes operan como verdaderas agencias de inteligencia al servicio de firmas que pretenden robar la propiedad intelectual de ciertos adelantos. En el ámbito empresarial, el robo de secretos industriales por parte de *hackers* es, actualmente, una de las mayores transferencias de riqueza (Marks, 2017).

En el ámbito de las finanzas, uno de los desafíos principales está dado por el nacimiento de las cadenas de bloques y criptomonedas, cuyo uso es cada vez

desbloquearlo. También se conoce a esta práctica como «secuestro de datos».

[5] Michael Keegan expresa que Estados Unidos ha visto afectados sus niveles de confianza en el gobierno, la cual viene decreciendo, como se mide en numerosas encuestas. Esta visión se deriva en parte de cómo las agencias federales se muestran inefectivas en el manejo de las amenazas de la era digital (Abramson *et al*., 2018).

más extendido. Esta nueva tecnología financiera escapa al control gubernamental. Actualmente: «se plantea que los gobiernos y las empresas deben colaborar en el fortalecimiento del liderazgo tecnológico y de mercado en este campo, sobre todo para resolver la potencial incompatibilidad, política y regulatoria, que puede restringir el crecimiento de esta economía digital basada en *blockchain*» (Oszlak, 2019, p. 14). El sistema de criptomonedas avanza rápidamente —mucho más que la legislación de los Estados en esta materia—, a la vez que genera lagunas en el mundo del derecho, así como en usuarias/os y organismos de regulación financiera.

En cuestiones de ataques cibernéticos, el riesgo no es solamente económico o financiero. La hipótesis de un posible *hackeo* de la campaña electoral de Hillary Clinton en las elecciones presidenciales de 2019 sirve para ilustrar la arista política del problema, que puede derivar en una pérdida de confianza de la ciudadanía. El mismo Obama lo sufrió personalmente cuando los sistemas de la campaña demócrata para la elección presidencial de 2008 fueron *hackeados*, de manera que se accedió a información confidencial, como archivos sobre posiciones políticas o planes de viajes del candidato[6].

En otro orden de cosas, los países dependen hoy de redes informáticas para la provisión de recursos estratégicos como agua, combustibles y electricidad. Este tipo de sistemas regulan el tráfico aéreo o el transporte público en las ciudades. Por este motivo, un ataque cibernético puede dejar aislada u oscurecida a una ciudad durante horas, provocar múltiples accidentes y sembrar el pánico.

En el campo militar, la existencia de estas amenazas cibernéticas genera más que preocupación, a sabiendas de que los sistemas de seguridad de las fuerzas armadas deben ser cada vez más sofisticados, a fin de no sufrir la intromisión de agentes externos que pueden ocasionar enormes pérdidas. Obama diría en su discurso del 29 de julio de 2009: «Nuestras redes militares y de defensa están bajo constante ataque» y «nuestra ventaja tecnológica es la clave del predominio militar norteamericano». Esto incluye la amenaza de ciberataques provenientes de grupos terroristas y de

[6] «Keep our country and the American people safe». Definición de la política de seguridad cibernética de Obama. Disponible en el sitio web de la Casa Blanca (www.obamawhitehouse.gov).

servicios de inteligencia exteriores. En 2008, numerosas computadoras del sistema de defensa estadounidense fueron infectadas por virus informáticos y, a pesar de que el ataque cibernético no pasó a mayores, obligó al aislamiento de miles de dispositivos electrónicos de las tropas americanas. Hoy un ataque terrorista es impensado sin el soporte de las nuevas tecnologías, que van desde comunicaciones encriptadas, pasando por dispositivos con GPS, hasta drones comandados a gran distancia.

Todos los ejemplos anteriores son solo una muestra del complejo escenario en el que se desarrolla la cuestión de la ciberseguridad, y se infiere de ello el enorme impacto que puede tener en la agenda estatal y en la evaluación de los niveles de capacidad institucional de los Estados.

3. Análisis del Plan de Acción de Ciberseguridad Nacional de la administración Obama

Luego de hacer una descripción general del contexto amenazante de la era digital, en el presente apartado expondremos el tratamiento del problema de la ciberseguridad en Estados Unidos, a la luz de la implementación de la política del presidente Barack Obama sobre esta cuestión: el Plan de Acción de Ciberseguridad Nacional (CNAP). Para un análisis ordenado de esta política, tomaremos el enfoque teórico elaborado por Oszlak y O'Donnell (1976), que entiende a la política estatal como «una *toma de posición* que intenta —o, más precisamente, dice intentar— alguna forma de resolución de la *cuestión*». (p. 13).

3.1 El nacimiento de la cuestión y la toma de posición del Estado

A poco de asumir su mandato, Barack Obama expuso su visión del contexto y los fundamentos que hacían necesaria una estrategia nacional en ciberseguridad, lo que definió como: «un momento transformacional, un momento en que un mundo interconectado se nos presenta, a la vez con grandes promesas, pero también grandes peligros». Otorgó a esta cuestión un lugar prioritario dentro de sus preocupaciones, por lo que llegó a afirmar que ninguno de los progresos que se proponía y: «… ninguno de los desafíos del siglo XXI, podrían satisfacerse

por completo, sin una buena infraestructura digital estadounidense, columna vertebral que apuntala la prosperidad económica y la fortaleza militar, así como un gobierno abierto y eficiente» (The Obama White House, 2017).

Toda política pública encuentra su inicio en la problematización de la cuestión: demandas y necesidades hay muchas, pero no todas son «problematizadas» de manera que se conviertan en objeto de una política pública. Existen numerosas razones por las cuales ciertas demandas o necesidades deciden «problematizarse», mientras otras se dejan de lado. En este proceso de problematización o formación de la agenda estatal, suelen intervenir diversos actores —sobre todo en las sociedades democráticas— como: clases, facciones de clase, organizaciones civiles, grupos de presión o individuos influyentes, quienes consideran que la demanda debe ser respondida desde la acción estatal y promueven, mediante distintos mecanismos, su incorporación a la agenda de problemas socialmente atendibles. Al respecto, cabe preguntarse en el inicio del análisis de una política pública, qué margen de maniobra o «capacidad de iniciación autónoma» tiene el Estado a la hora de fijar su agenda.

Como lo sugieren Oszlak y O'Donnell (1976): «en lo posible deberíamos encarar nuestros estudios analizando el período previo al surgimiento de la cuestión» (p. 13). Resulta útil, por tanto, analizar este momento previo junto el proceso a través del cual esta se convierte en una cuestión como tal. En el caso particular de la política de ciberseguridad estadounidense, es difícil rastrear desde cuándo forma parte de los objetivos de política estatal. Estados Unidos, como país desarrollado, posee una larga tradición en políticas de seguridad tecnológica. Escapa a los límites de este trabajo rastrear los antecedentes que en la materia han erigido otras administraciones anteriores al gobierno de Obama, ya que nos limitaremos a analizar el estado de la cuestión en los meses previos al lanzamiento del CNAP. Sin embargo, siguiendo a Abramson *et al.* (2018) podemos resumir que los primeros intentos de articular una política de ciberseguridad se dieron en la década de los noventa, en la etapa que estos autores llaman «de acción temprana» (*early action*). A partir de 2004, las acciones entraron en una fase de «expansión», que posibilitó pasar del nivel interno y descoordinado de los organismos del Estado, a una visión más amplia y de carácter nacional (es en este período que comienzan

a aparecer los *chief risk officers* en distintas agencias federales). A partir de 2014, los autores marcan el comienzo de una etapa de *institucionalización* tendiente a generar mayor control de los riesgos desde una perspectiva tecnocrática, que sigue los lineamientos de aquello que había funcionado dentro del sector privado, es decir, de las empresas de tecnología. En esta fase, a su vez, se propone un abordaje integral y articulado de la problemática de la ciberseguridad, a sabiendas de que la mayor interconexión hace que deficiencias de seguridad en un área del gobierno repercutan en los niveles de seguridad de otras.

El presidente Obama hizo mención de su Plan, por primera vez, en febrero de 2016. En este se proponía, en primera instancia, la revisión profunda de las redes del Gobierno estadounidense y la conformación de un nuevo organismo para analizar el estado de la cuestión en la administración pública de ese país. ¿Qué fue lo que llevó a que el Gobierno decidiera incorporar este problema en su agenda? En los últimos años se había registrado un importante aumento de *ciberataques* y filtraciones de datos, tanto de organismos públicos como de agencias privadas. En 2015 se conoció la vulneración de información personal de millones de empleados públicos, mediante el *hackeo* de la Oficina de Administración del Personal. «Estas ciberamenazas son uno de los peligros más urgentes para la seguridad económica y nacional de Estados Unidos» expresó Obama en esa oportunidad. Además, reconoció públicamente que algunas áreas de la administración pública usaban sistemas y códigos de los años sesenta, y que ningún éxito podía esperarse de este nivel de atraso.

En relación con las declaraciones anteriores, son importantes en la definición misma de la cuestión. La política de ciberseguridad fue planteada desde el comienzo por la administración Obama como una forma de «mantener seguro a nuestro pueblo». En un contexto de: «… después de la era digital que nos hace más vulnerables a la actividad cibernética maliciosa, debemos adaptarnos a esta amenaza nacional»[7]. Además de la definición de una cuestión, vemos en este discurso una clara toma de posición. El Gobierno reconocía la existencia de un hecho considerado una amenaza a la cual el Estado debe responder por el bien de la sociedad en su conjunto.

[7] «Keep our country and the American people safe». Definición de la política de seguridad cibernética de Obama. Disponible en el sitio web de la Casa Blanca (www.obamawhitehouse.gov).

La propuesta del CNAP debe leerse en el marco posterior a la aprobación, en 2015, de una Ley de Intercambio de Información sobre Ciberseguridad (CISA), que busca la colaboración de las empresas productoras de tecnologías y el Gobierno en materia de seguridad cibernética, aspecto que, como se verá más adelante, era fundamental para la puesta en práctica del Plan[8]. El proyecto de ley fue impulsado inicialmente por los demócratas, pero fue finalmente aprobado por amplia mayoría.

Es interesante analizar, a partir de este hecho, qué grupos se manifestaron a favor y cuáles en contra de esta política estatal. Esto se relaciona con lo que Oszlak y O'Donnell (1976) llaman la *capacidad de iniciación autónoma del Estado*, y la política estatal como *nudo* dentro del proceso de construcción social[9]. Para la sanción de la CISA, el Congreso recibió el apoyo de grupos de defensa, de la Cámara de Comercio de los Estados Unidos, la Asociación Nacional de Cable y Telecomunicaciones, y la Mesa Redonda de Servicios Financieros. Sin embargo, varias empresas importantes del mundo tecnológico (Google, Amazon, Cloudflare, Netflix, Facebook, Red Hat y Yahoo, entre otras) y asociaciones de empresarios —como la Asociación de la Industria de Computadoras y Comunicaciones— se mostraron opuestas a la promulgación de la ley. También se opusieron los grupos de defensa de los derechos digitales: Fight for the Future, Access, American Ciber Liberties Union y Electronic Frontier Foundation, entre otras, quienes encabezaron en su momento una protesta contra la CISA. La principal crítica de estos grupos sostenía que la ley significaba ampliar las posibilidades de vigilancia de parte del Gobierno sobre la ciudadanía, más que un sistema de protección. La misma red de apoyos y resistencias se movilizaría alrededor del CNAP. Vemos, a partir de este ejemplo, cómo diversos actores se relacionan en torno a una cuestión y accionan recursos

[8] La Ley de Intercambio de Información sobre la Ciberseguridad (CISA, por sus siglas en inglés) es una ley federal diseñada para mejorar la ciberseguridad en los Estados Unidos mediante un mayor intercambio de información sobre amenazas entre el gobierno estadounidense y las empresas de fabricaciones tecnológicas.

[9] Oszlak y O'Donnell (1976) sostienen que la política pública puede interpretarse como un *nudo* dentro del entramado social. A partir de la toma de posición —y posterior acción del Estado—, se van generando reacciones sociales que luego dan nacimiento a nuevos *nudos*, y estos, a su vez, repercuten en la política pública.

para que sea atendida o desestimada por el Estado, y, así, constituyen nuevos *nudos* dentro del proceso de construcción social que implica toda política pública.

En conclusión, el surgimiento de la cuestión bajo análisis no respondió a una demanda de la sociedad articulada a través de ciertas organizaciones civiles o grupos de presión, como suele ocurrir en otros casos (con respecto a la CISA, la mayoría de los grupos civiles involucrados se manifestaban en contra de la política estatal). Se trató más de la percepción de una amenaza a la seguridad nacional, lo que impulsó al Gobierno estadounidense a incorporar este tema de ciberseguridad en su agenda y, a pesar de encontrar numerosas resistencias en contra de su «intromisión», el Estado decidió continuar con la iniciativa.

La ciberseguridad es una cuestión que no puede faltar en el diagnóstico de un país desarrollado en la era exponencial y que obliga a los gobiernos a tomar posición y articular una serie de acciones formales para atender el problema. En el caso de estudio, la cuestión ya existía para cuando Obama llegó al Gobierno y, lejos de descartarla, decidió darle un alto nivel de prioridad en su agenda gubernamental, lo que requirió la movilización de una ingente cantidad de recursos. Esto, a la postre, demuestra la *capacidad de iniciación autónoma del Estado* en esta materia.

3.2 Implementación del CNAP

La administración Obama tomó en serio el problema de las amenazas cibernéticas desde el primer día: llevó a cabo una revisión de la cuestión, lanzó una política propia, erigió defensas y castigó a los actores más peligrosos del ciberespacio, lo que incluyó la imposición de sanciones a Corea del Norte y Rusia, así como la acusación a *hackers* que tenían vinculación con los gobiernos de China e Irán.

En 2016, Obama lanzó su Plan de Acción Nacional, presentado como el fruto de un esfuerzo mancomunado de siete años de trabajo, para el cual solicitó al Congreso la aprobación de una partida de 19 mil millones de dólares, que significaba un aumento del 35 % en esa materia. De ellos, 3 mil millones aproximadamente estarían destinados a modernizar la red de sistemas informáticos que usaban

las agencias del Gobierno. El objetivo, según lo definió el mismo Obama, era: «proveer a cada estadounidense de un nivel básico de seguridad en línea» (The Obama White House, 2016).

El Plan requería la inversión en infraestructura tecnológica como parte de la solución a las ciberamenazas. Asimismo, no existía una agencia centralizada encargada de la cuestión que contara con la información, la capacidad y la responsabilidad para afrontar el desafío de manera coordinada. En otras palabras, faltaban recursos materiales y mecanismos institucionales. Esto era parte del diagnóstico inicial de la administración Obama y se vería reflejado en varias aristas del CNAP.

En una primera etapa, el expresidente estadounidense convocó al Consejo de Seguridad Nacional (National Security Council) y al Consejo de Seguridad Interior (Homeland Security Council) para que llevaran a cabo una revisión exhaustiva de los esfuerzos realizados hasta el momento en materia de protección a la seguridad de la información federal y la infraestructura disponible en materia de comunicación del Gobierno. También lo hizo para solicitarles recomendaciones sobre las mejores formas de asegurar esos canales. La investigación inicial incluyó la consulta con especialistas académicas/os, universidades, representantes de la industria y de las asociaciones de defensa de los derechos civiles, así como a diferentes niveles dentro de la burocracia estatal, civil, militar y de los servicios de inteligencia.

Antes de que su programa fuera aprobado por el Congreso estadounidense, Obama había creado, en su voluntad de unificar y coordinar la estrategia de ciberseguridad, la figura del *Cibersecurity Coordinator*, un nuevo órgano cuya designación dependería directamente del presidente, y sería el encargado de asesorar al primer mandatario en materia de seguridad informática. Esto sirve para ilustrar de qué modo, como afirman Oszlak y O'Donnell (1976), las políticas estatales generan procesos internos al Estado mismo. El término *cristalizaciones institucionales* se refiere a la creación de aparatos burocráticos o la adjudicación de nuevas funciones a organismos preexistentes, que quedan formalmente encargados del tratamiento y de la eventual resolución de la cuestión. Estas incorporaciones suelen requerir el reacomodamiento «tanto horizontal como

vertical» de otras estructuras del Estado relacionadas con la cuestión. La nueva Alianza Nacional de Seguridad Cibernética —que incorporaba a las diferentes oficinas del Estado en materia de seguridad— era la otra *cristalización institucional* que debería articular con el coordinador de Ciberseguridad de la presidencia, y que sería miembro con amplios poderes dentro de la propia Alianza. También debían coordinar con él la Oficina de Gestión y Presupuesto del Estado y el Consejo Económico Nacional. Este nuevo ente se convirtió en un elemento condicionante de la política y de su definición, así como una variable interviniente del proceso político articulado en torno a la cuestión. Por ejemplo, la Oficina de Presupuesto sería la encargada de que las cuestiones de ciberseguridad tuvieran reservada una porción del presupuesto de cada uno de los entes públicos, según lo marcaran los lineamientos del coordinador.

Siguiendo con la evaluación de las cristalizaciones institucionales a las que el CNAP dio lugar, se contempló la creación de una comisión bipartidista (Commission on Enhancing National Cybersecurity) compuesta por doce miembros. Su fin era evaluar los desafíos a largo plazo que el país tenía en materia de ciberseguridad, la cual debía tener en cuenta al sector privado en la búsqueda de soluciones conjuntas. Basado en este espíritu, Obama nombró presidente de esa comisión a su antiguo asesor de Seguridad Nacional, Thomas Donilon, y le asignó la vicepresidencia al ex-CEO de la International Business Machines Corporation (IBM), Samuel Palmisano. Además, creó un Consejo de Privacidad Federal permanente, que reunía a las/os funcionarias/os de privacidad de todo el Gobierno para ayudar a garantizar la implementación de pautas federales más estratégicas y completas en esta materia. Una tercera cristalización institucional fue la creación del puesto de director federal de Seguridad de la Información, con el poder de impulsar cambios de manera coordinada en todas las áreas del Gobierno.

Pero los cambios institucionales también se dieron a nivel de instituciones ya existentes que vieron ampliadas o modificadas ciertas funciones originales. Según lo disponía el CNAP, el Departamento de Seguridad Nacional, la Administración de Servicios Generales y otras agencias federales aumentarían la disponibilidad de servicios compartidos en todo el gobierno en materia de TIC y ciberseguridad, con el objetivo de unificar los sistemas de seguridad e implementar opciones más eficientes, efectivas y sólidas.

En cuanto a sus objetivos declarados, el CNAP se propuso: «tomar acciones a corto plazo y fijar una estrategia a largo plazo para mejorar el nivel de conciencia en ciberseguridad y defensa, proteger la privacidad, mantener la seguridad pública, así como la seguridad económica y nacional, empoderando a los estadounidenses para que tengan un mayor control sobre su seguridad digital»[10]. Esto requería el esfuerzo conjunto del Gobierno, las empresas y los individuos.

Las medidas concretas del CNAP que se enumeran a continuación (se seleccionaron solo las consideradas más relevantes), dan cuenta de su importante magnitud y complejidad, así como de la ingente cantidad de recursos, la multiplicidad de actores involucrados y el nivel de coordinación que el plan requería para llevarse a la práctica.

Dentro de las acciones se encuentran, en primer lugar, la modernización de las tecnologías de información del Gobierno y la transformación de la forma en que este gestionaba la ciberseguridad. Esto se haría a través de un Fondo de Modernización de la Tecnología de la Información de más de 3 mil millones de dólares, usados para el retiro, reemplazo y modernización de tecnología informática heredada.

Con el objetivo de empoderar a las/os estadounidenses para asegurar sus cuentas en línea, se propuso ir más allá de las contraseñas y agregar una capa adicional de seguridad, como una huella digital o un código de uso único entregado por mensaje de texto. Como complemento de esta medida, se decidió que la Alianza Nacional de Seguridad Cibernética se asociara con firmas tecnológicas líderes —como Google, Facebook, Dropbox y Microsoft—, para facilitar que millones de usuarios aseguren sus cuentas en línea, y compañías de servicios financieros —como Mastercard, Visa, PayPal y Venmo—, para hacer más seguras las transacciones. En esta misma línea, se implementaron medidas para salvaguardar los datos personales en las transacciones en línea entre ciudadanas/os y el Gobierno, lo que incluía la adopción y el uso de pruebas de identidad efectivas, y métodos de autenticación multifactoriales sólidos.

[10] Estos objetivos están publicados en la «Fact sheet: Cybersecurity National Action Plan» disponible en el sitio web de la Casa Blanca durante la administración Obama (www.obamawhitehouse.gov).

Asimismo, el CNAP preveía el sostenimiento y perfeccionamiento de políticas anteriores, como la ampliación del sistema EINSTEIN y el Programa Continuo de Diagnóstico de Amenazas. En esta línea, se aumentó el número de equipos civiles de defensa cibernética —dependientes del Gobierno federal— a un total de cuarenta y ocho, y se reclutó a los mejores talentos en seguridad cibernética tanto del sector público como del privado. Estos equipos permanentes protegerían las redes, los sistemas y los datos de la administración pública, mediante la realización de pruebas de penetración y la búsqueda proactiva de intrusos, además de proporcionar respuesta a incidentes y experiencia en ingeniería de seguridad.

Como otra pata del Plan, se decidió apuntalar las medidas de concientización social a fin de prevenir el ciberdelito, para lo cual se previeron acciones en el ámbito educativo. En este contexto, se lanzó la «Iniciativa Nacional para la Educación en Ciberseguridad», que comprendía la reforma de programas educacionales a nivel escolar y universitario para incluir la problemática dentro de los centros de formación. Además, la Iniciativa fijaba el otorgamiento de becas de capacitación para profesionales que quisieran trabajar en el Gobierno en esta materia, así como el fortalecimiento de los centros de investigación en *cybersecurity*. Asimismo, surgió una «Campaña Nacional de Concienciación sobre Ciberseguridad» lanzada por la Alianza Nacional de Seguridad Cibernética, diseñada para proporcionar a las/os consumidoras/es información simple y procesable para protegerse en un mundo cada vez más digitalizado.

Con el fin de colaborar con la seguridad cibernética de las empresas privadas, se estableció un Centro Nacional para la Resiliencia de Ciberseguridad (otra cristalización institucional), organismo en el cual las empresas y las organizaciones podrían probar la seguridad de los sistemas, mediante simulacros de ciberataques.

Este ambicioso modelo de política estatal abarcaba muchas otras acciones de menor escala, desprendidas de las medidas centrales antes enumeradas. De alguna manera, un calibre tan amplio explica el poco impacto relativo de este conjunto de medidas, lo que abordaremos a continuación.

3.3 Evaluación de los impactos del CNAP

Cuesta identificar la correlación que existe entre la implementación de una determinada política y los cambios que se observan en el asunto en cuestión. Definir con qué criterio una política es exitosa —y a los ojos de quién— es una problemática que raramente encuentra acuerdo unánime. Tomaremos, para el análisis de los impactos del CNAP, las voces de algunos especialistas en ciberseguridad que han analizado la cuestión.

Algunos especialistas, como Joseph Marks (2017) y Taylor Armending (2017), han elogiado las intenciones del CNAP y los esfuerzos puestos en el programa de Obama. Sin embargo, han calificado los resultados como poco alentadores y limitados: «at the end, cyberspace won» (al final, ganó el ciberespacio) (Marks, 2017). La mayor crítica al sistema de *cybersecurity* de Obama se dio en ocasión del *hackeo* sufrido por la candidata demócrata Hillary Clinton —supuestamente por *hackers* rusos— en las elecciones que se disputaban al final del mandato de Obama, cuando el CNAP ya se encontraba en plena implementación. Siguiendo la misma línea argumental, Paul Rosenzweig, un experto en seguridad cibernética —exasesor del Departamento de Seguridad Interior de la administración Bush—, ha reconocido que Obama invirtió enormes recursos económicos e intelectuales en mejorar el aparato de seguridad estatal en relación con las ciberamenazas, pero que, a pesar de todo, no se llegó a una mejora sustantiva de la cuestión (Marks, 2017).

Otros expertos, como Tim Maurer, Jacob Olcott o Adam Segal, coinciden en que, en términos de instituciones para luchar contra el cibercrimen, Estados Unidos ha hecho avances durante la administración Obama. Sin embargo, en líneas generales, el entorno cibernético sigue siendo una amenaza difícil de prevenir. Incluso, Michael Daniel, el coordinador de ciberseguridad del presidente Obama, no se mostró del todo optimista en su balance final, al reconocer que «claramente se aumentó la capacidad, la conciencia y la seguridad en muchos aspectos, pero al mismo tiempo aumentó la vulnerabilidad en igual medida, ya que el panorama es más serio y más peligroso» (Marks, 2017).

Existieron, sin dudas, avances en cuestión de ciberseguridad. Algunos derivan directamente de la implementación del CNAP y otros de políticas relacionadas,

como el acuerdo firmado en 2015 con el Gobierno chino para combatir el *hackeo* comercial[11]. Dentro de las mejoras, se encuentra la implementación del «Sistema EINSTEIN 3» para detección y prevención de amenazas cibernéticas, que ahora protege a más del 90 % de las oficinas del Gobierno. El sistema de ciberseguridad de la Casa Blanca también fue mejorado. El Departamento de Defensa desarrolló un sistema independiente: el U.S. Cyber Command, dotado de capacidades defensivas y ofensivas, con más de 6000 agentes de seguridad informáticos. Por otro lado, el Departamento de Estado, llevó adelante la ofensiva externa, tratando de trabajar coordinadamente con otras naciones, en un intento mancomunado de regular el ciberespacio desde la óptica del derecho internacional. Asimismo, el Departamento del Tesoro desarrolló un paquete de sanciones similar al que la Casa Blanco utilizó contra los *hackers* rusos. En cuanto al sector privado, este adoptó ampliamente el marco de trabajo de ciberseguridad desarrollado por el National Institute of Standards and Technology, en el marco del CNAP.

A pesar de todos estos dispositivos, el gobierno de Obama sufrió la filtración de correspondencia de la Casa Blanca, el Departamento de Estado y los altos mandos de las Fuerzas Armadas, atribuida al accionar de *hackers* ligados al gobierno de Vladimir Putin. China, por su parte, fue acusada de obtener información personal de 20 millones de trabajadoras/es del Estado, a través de un ciberespionaje a la Oficina de Administración del Personal. Empresas como Sony, Target, JP Morgan Chase, Yahoo!, también sufrieron robo de datos de parte de supuestos *hackers* norcoreanos. En 2016, varias firmas sufrieron el bloqueo de su acceso a internet, entre las que se encontraban Netflix y el New York Times, por mencionar solo las más conocidas. Tampoco se registraron más bajos niveles de ciberataques a consumidores privados.

Hemos visto cómo uno de los frutos del CNAP fue el nacimiento de un conjunto de instituciones (cristalizaciones institucionales) que operan hasta el día de hoy en materia de ciberseguridad. Sin embargo, tal proliferación —producto de la complejidad del mismo Plan— conspiró contra uno de los principales

[11] En los meses posteriores al acuerdo, cayeron notablemente las denuncias de empresas que acusaban haber sido *hackeadas* por agentes de espionaje chinos en Estados Unidos. La compañía de ciberseguridad FireEye —que conduce investigaciones de corporaciones víctimas de espionaje cibernético— pasó de un promedio anual de 35 casos en los años anteriores al acuerdo a un promedio de 10 casos.

objetivos, que era facilitar la coordinación de políticas en torno a la cuestión de ciberseguridad.

Oszlak y O'Donnell (1976) plantean que si la implementación de una política estatal resulta inconsistente, esto puede explicarse por: a) la ambigüedad en la definición inicial de la cuestión; b) «la presencia, dentro del aparato estatal, de unidades con variable grado de autonomía, capaces de influir en diversas instancias del proceso, que entran en conflicto cuando debe definirse la posición del Estado frente a una cuestión social» (1976, p. 14); c) la toma de posición de otros actores afectados por la cuestión.

¿Cuáles fueron los principales escollos que encontró la política estatal del Gobierno estadounidense para mejorar sus rendimientos en la cuestión de ciberseguridad? Sin dudas, a partir de esta investigación, debemos inclinarnos por la tercera opción. A la presencia de actores amenazantes externos a Estados Unidos, debe sumársele la resistencia de muchas empresas de tecnología estadounidenses que se niegan a cooperar con el Gobierno a fin de contribuir a mejorar los sistemas de seguridad. Las empresas más adelantadas en cuestiones de informática se muestran reacias a compartir «sus secretos» con los entes estatales. El campo de la industria cibernética está mayormente gobernado por empresas privadas que gozan de un amplio margen de maniobra y poder, por lo que la capacidad que tiene el Gobierno para controlar a estos entes encuentra sus limitaciones[12]. Lo que para el Estado es una respuesta a un problema de seguridad nacional, para las empresas y ciertos grupos civiles es una forma de resignar libertades individuales en favor del Estado.

Como vemos, la definición misma de la cuestión es divergente, lo que dificulta la cooperación y hace que aparezcan nuevos *nudos* en la compleja trama de relaciones sociales que impactan en la política estatal. Esta puja de poder entre Estado y empresas tecnológicas puede verse desbalanceada en favor de estas como consecuencia de la pandemia, ya que las empresas que mayores beneficios

[12] Al respecto, los autores estudiados afirman que «el conjunto de políticas privadas y estatales se entrelaza en un complejo proceso social que, como veremos, hace difícil establecer con precisión qué proporción del cambio social observado puede ser atribuido a cada una» (Oszlak y O'Donnell, 1976, p. 16).

han obtenido este año son las industrias de software y las plataformas. Este es el caso de Amazon y Netflix, por nombrar a las más conocidas. Las incalculables sumas que están registrando estos actores privados, los dotará de recursos para continuar ganando autonomía frente al Estado, hasta llegar incluso a condicionar su accionar.

Asimismo, debemos resaltar que la dimensión sistémica (el contexto de la era exponencial) dificulta el éxito de la política de ciberseguridad —en Estados Unidos o en cualquier país—, ya que se trata de medidas que operan en un ambiente continuamente cambiante. «Las amenazas crecen y cambian más rápido que la habilidad del gobierno para lidiar con ellas» (Marks, 2017).

Como lo expresan Oszlak y O'Donnell, lo que llamamos: «impactos de políticas estatales son en realidad "contribuciones" —imputables al Estado— a complejos patrones de cambio de la sociedad global» (1976, p. 27). Esta frase sirve para poner en contexto las deficiencias de la política de ciberseguridad del gobierno de Obama. El programa de *cybersecurity* estadounidense refleja a las claras el carácter dinámico y cambiante de toda política estatal como una compleja construcción social, en la que interactúan actores con diferentes intereses.

En este contexto, medir el impacto del CNAP es una tarea que requiere de una estrategia de análisis muy minucioso, a fin de detectar cuáles son aquellos aspectos que han sido exitosos en la implementación de la política y aquellos que aún falta mejorar. Esto excede a las intenciones y alcances de este trabajo, pero, sin dudas, constituye una tarea interesante en el campo de estudio de las políticas públicas en la era exponencial.

4. Reflexiones finales

La agenda estatal, como sostienen Oszlak y Gantman (2006), se constituye de aquellas cuestiones problematizadas que llegan a suscitar la atención de las instituciones estatales. Si existe un Estado, es porque hay cuestiones a las que la ciudadanía no ha podido responder de manera alternativa. Sin dudas, las nuevas problemáticas en cuestiones de ciberseguridad difícilmente puedan ser

solucionadas por entes extraestatales, con lo cual, en este sentido, el Estado tiene un área que garantiza su subsistencia; aunque, también, pone a prueba su eficacia y capacidad.

Oszlak y O'Donnell (1976) han expuesto la tesis del *ciclo vital* de las cuestiones: toda cuestión tiene una *vida* que va desde su problematización —con la consecuente incorporación en la agenda del Estado— hasta su resolución —lo que implica su salida de la agenda—. Cabe preguntarse si es posible que en la era exponencial la cuestión de la ciberseguridad sea resuelta de manera definitiva para que desaparezca de la agenda estatal. En materia de *cybersecurity*, el avance tecnológico imparable en los tiempos que corren pareciera darle permanente combustible a una cuestión sobre la cual los Estados tienen poco margen para relajarse o desentenderse. Como lo expresa Marks (2017), «durante ocho años, el ciberespacio se mostró como el adversario más impredecible de la administración Obama, siempre girando en nuevas direcciones y asestando golpes donde menos se lo esperaban». Los resultandos de la lucha entre gobiernos y ciberatacantes demuestran que, estos últimos, siempre han estado un paso delante de la legislación y las políticas.

Ante esta cruda realidad, la cuestión de la ciberseguridad pareciera ser un claro ejemplo de «trabajo de Sísifo» para los gobiernos, lo que coopera para que la agenda en esta cuestión no pueda relajarse nunca y que la misma esté siempre latente. Cada medida puede evaluarse por separado para medir su nivel de eficacia en el punto específico que se proponían mejorar, pero todo lo que se haga en esta materia, comparado con el nivel de la amenaza, resultará escaso.

No puede prescindirse del análisis del contexto global —es decir, de los factores extrínsecos— de la política estatal. En este sentido, la era exponencial se manifiesta como una amenaza siempre cambiante y superadora, mientras los gobiernos van corriendo detrás de las cuestiones. Cuando intentan empezar a resolverlas, las nuevas fuerzas de la tecnología ya están abriendo otros frentes de batalla. Esto explica en gran medida la complejidad evidenciada en el diseño e implementación del CNAP, sus ambiciosos objetivos iniciales y los magros resultados obtenidos.

Cabe preguntarse si en caso de que las ciberamenazas dejen en evidencia a un Estado impotente a la hora de combatirlas, los niveles de legitimidad de los gobiernos no se verán perjudicados, con consecuentes cuestionamientos al sistema democrático. En la introducción de este trabajo, declaramos que mirar a los países más adelantados puede servirnos de ejemplo para observar qué cuestiones va imponiendo la era exponencial en la agenda de los gobiernos. Lo cierto es que, los bajos rendimientos de la política de ciberseguridad de la administración Obama, a pesar de los ingentes esfuerzos y recursos puestos en su implementación, nos generan la duda de si los gobiernos menos adelantados tienen serias posibilidades de hacer algo con respecto a la cuestión. Si aquellos países que cuentan con los recursos técnicos, humanos y económicos para darse a la tarea de hacer funcionar complejos sistemas de ciberseguridad, como es el caso de Estados Unidos, siguen estando enormemente expuestos a las amenazas provenientes del espacio cibernético, ¿qué queda para aquellos países carentes de tales recursos?

Con respecto al impacto limitado del CNAP, no podemos dejar de mencionar la resistencia que encontró tal política en un sector socioeconómico con enorme poder: las compañías tecnológicas, nudo cada vez más difícil de desatar. El ejemplo de la relación empresas-Estado, grafica lo dicho por Oszlak y O'Donnell: «aún en el caso en que el Estado inicia con gran autonomía una cuestión, las decisiones posteriores vinculadas a la misma (…) no dejarán de estar influidas por las posiciones adoptadas por otros actores» (1976, p. 16). Sin dudas, ante la gran *capacidad de iniciación autónoma* que mostró el gobierno de Barack Obama, la resistencia de otros actores sociales se manifestó igualmente fuerte. Este punto debe tenerse en cuenta en las futuras estrategias que se adopten para el tratamiento de la cuestión.

El análisis de la política pública en cuestión es un ejemplo ilustrativo sobre la complejidad de la acción estatal y las transformaciones de la agenda pública, a raíz de los nuevos desafíos que trae consigo el avance de la era exponencial.

Referencias bibliográficas

Abramson, M. A., Chenok, D. J. & Kamensky, J. M. (2018). *Government for the future: reflection and vision for tomorrow's leaders*. IBM Center for the Business of Government.

Armending, T. (31 de enero de 2017). Obama's cybersecurity legacy: good intentions, good efforts, limited results. *CSO*. https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html

BBC (13 de junio de 2018). Departamento de Justicia de Estados Unidos acusa a 12 miembros de la inteligencia rusa de hackear la campaña electoral de Hillary Clinton. *BBC*. https://www.bbc.com/mundo/noticias-internacional-44827846

BBC (14 de mayo de 2020). La economía y el coronavirus: los negocios ganadores y los sorpresivos perdedores durante la pandemia. *BBC*. https://www.bbc.com/mundo/noticias-52647431

Daniel, M., Scott, T. & Felten, E. (9 de febrero de 2016). The president's National Cybersecurity Plan: what you need to know. *Obama White House*. https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

EFEUSA (17 de febrero de 2016). Obama designa a antiguo asesor para encabezar comisión sobre ciberseguridad. *Agencia EFE*. https://www.efe.com/efe/usa/portada/obamadesigna-a-antiguo-asesor-para-encabezar-comision-sobre-ciberseguridad/50000064-2842872

El Universo (9 de febrero de 2016). Obama lanza plan de acción sobre ciberseguridad. https://www.eluniverso.com/noticias/2016/02/09/nota/5395348/barack-obama-lanza-plan-accion-sobre-ciberseguridad/

Freeman, J. (9 de febrero de 2016). President's Obama cybersecurity plan. *The Wall Street Journal*.

LINIO (s.f). Índice mundial de comercio electrónico.

Marks, J. (17 de enero de 2017). Obama's cyber legacy: he did (almost) everything right and it still turned out wrong. *Nextgov*. https://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almost-everything-right-and-it-still-turned-out-wrong/134612/

Obama White House (9 de febrero de 2019). *FACT SHEET: Cybersecurity*

National Action Plan. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Oszlak, O. (23-26 de abril de 2019). *La gestión pública en la «era exponencial»: desafíos para los países emergentes*. xv Conferencia anual INPAE, «Respuestas Latinoamericanas a los desafíos de la Administración Pública», Concepción, Chile.

Oszlak, O. y Gantman, E. (2007*)* La agenda estatal y sus tensiones: gobernabilidad, desarrollo y equidad. *Iberoamericana. Nordic Journal of Latin American and Caribbean Studies*, *37*(1), 79-110.

Oszlak, O. y O'Donnell, G. (1976). *Estado y políticas estatales en América Latina: hacia una estrategia de investigación*. CEDES/CLACSO, (4). http://repositorio.cedes.org/handle/123456789/3332

Panda Security (26 de julio de 2019). El coste del cibercrimen: 45 mil millones de dólares. https://www.pandasecurity.com/spain/mediacenter/seguridad/costes-del-cibercrimen/

Pearson, J. (30 de julio de 2015). Sending Congress all 6 million faxes protesting CISA will take months. *Vice*. https://www.vice.com/en/article/wnj3kx/sending-congress-all-6-million-faxes-protesting-cisa-will-take-months

Privacy, Cyber & Data Strategy Team (11 de febrero de 2016). President Obama announces Cybersecurity National Action Plan. *Alston & Bird*. https://www.alstonprivacy.com/president-obama-announces-cybersecurity-national-action-plan/

The Obama White House. (29 de mayo de 2009). *President Obama on Cybersecurity* [archivo de video]. YouTube. https://www.youtube.com/watch?v=wjfzyj4eyQM

The Obama White House. (17 de febrero de 2016). *The president speaks on the Cybersecurity National Action Plan* [archivo de video]. YouTube. https://www.youtube.com/watch?v=ZGFMZDQl9z0&ab_channel=TheObamaWhiteHouse

Cómo citar este artículo

Nadur, A. (2021). *Cybersecurity* en la era exponencial: la política de Obama. *Estado abierto. Revista sobre el Estado, la administración y las políticas públicas*, *5*(3), abril-julio, 69-93.