ISSN 0719-4110

CIEE
CENTRO DE INVESTIGACIÓN Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

CUADERNO DE TRABAJO Nº3-2023

GOBERNANZA DIGITAL Y CIBERSEGURIDAD: UN ANÁLISIS CONCEPTUAL Y RELACIONAL

Academia Nacional
de Estudios Políticos
y Estratégicos
www.anepe.cl

CUADERNOS DE TRABAJO es una publicación orientada a abordar temas vinculados a la Seguridad y Defensa a fin de contribuir a la formación de opinión en estas materias.

Los cuadernos están principalmente dirigidos a tomadores de decisiones y asesores del ámbito de la Defensa, altos oficiales de las Fuerzas Armadas, académicos y personas relacionadas con la comunidad de defensa en general.

Estos cuadernos son elaborados por investigadores, académicos y colaboradores del CIEE de la ANEPE, pero sus páginas se encuentran abiertas a todos quienes quieran contribuir al pensamiento y debate de estos temas.

Recordamos a los autores que el Cuaderno de Trabajo está comprometido con la publicación de artículos originales e inéditos que difundan conocimiento actualizado en materias de seguridad, defensa y ciencias sociales afines, con el fin de aportar y transferir, con el propósito fundamental de aportar al debate académico múltiples enfoques que enriquezcan el análisis, la reflexión y la interpretación en torno a los temas disciplinares propios de la seguridad, la defensa y las ciencias sociales.

Antes de imprimir este Cuaderno, piense en el medio ambiente.

CUADERNO DE TRABAJO DEL CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS es una publicación electrónica del Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos y está registrada bajo el **ISSN 0719-4110 Cuad. Trab., - Cent. Estud. Estratég.**
Dirección postal: Avda. Eliodoro Yáñez 2760, Providencia, Santiago, Chile.
Sitio Web www.anepe.cl. Teléfonos (+56 2) 2598 1000, correo electrónico ciee@anepe.cl

GOBERNANZA DIGITAL Y CIBERSEGURIDAD: UN ANÁLISIS CONCEPTUAL Y RELACIONAL

Pía Martabit Tellechea*

Resumen:

El desarrollo de una progresiva y masiva digitalización e hiperconectividad de la vida humana, así como en las actividades del ciberespacio, incentiva a que los gobiernos, impulsados por la idea de una buena gobernanza, migren sus servicios a las TIC, de manera parcial o total. Así las cosas, las actividades que se desarrollan en esta dimensión quedan más expuestas a ciberataques que, finalmente, afectan la calidad de entrega de servicios públicos que intentan ofrecer mayor eficiencia y elevado nivel de eficacia. Para esto, la necesidad de la buena gobernanza, total o parcialmente digitalizada, demanda de una robusta estructura de ciberseguridad. Este artículo busca comprender la compleja relación entre la buena gobernanza y la ciberseguridad.

Palabras clave: Ciberseguridad; gobernanza digital; gobernanza sector de seguridad; transformación digital.

DIGITAL GOVERNANCE AND CYBERSECURITY: A CONCEPTUAL AND RELATIONAL ANALYSIS.

Abstract:

The development of massive digitalization and hyperconnectivity of human life and its activities in cyberspace encourages governments, driven by the idea of good governance, to increasingly migrate their services to ICT, partially or totally, finding themselves increasingly more exposed to cyber attacks that affect the delivery of said public services that seek to improve in terms of efficiency and effectiveness. For this, the need for good governance, fully or partially digitalized, in all its complexity, undoubtedly requires robust cybersecurity. This article seeks to understand the complex relationship between good governance and cybersecurity.

Key words: Cybersecurity; digital governance; security sector governance; digital transformation.

* Cientista político de la Universidad del Desarrollo y magíster en Periodismo Mención Prensa Escrita de la Pontificia Universidad Católica de Chile, con estudios de diplomado en Seguridad Internacional y Ciberseguridad de la Universidad de Chile.

I. INTRODUCCIÓN

Gobernanza digital, e-government o gobierno digital constituyen conceptualizaciones que apuntan a la idea de mejorar la eficacia y eficiencia de las burocracias por medio de la digitalización y conectividad de los servicios y administración pública. También se le ha llamado a este proceso transformación digital. Esta iniciativa es la incorporación de Tecnologías de la Información y Comunicación (TIC) en el aparato público, buscando una mejor gestión del Estado, principalmente en la entrega de todos los servicios públicos que ofrece a su población. Una condición que abarca desde servicios básicos tangibles, como el agua, hasta intangibles, como la seguridad.

En este ámbito, la digitalización de servicios, sean públicos o privados, se encuentran en un terreno donde proliferan amenazas e inseguridades propiciado por la digitalización de toda, o una parte importante de las interacciones sociales. La conectividad a la red global de los servicios abre una ventana para que diversos actores, con diferentes niveles y capacidades de acceso, vulneren, exploten o expongan los sistemas, las herramientas y las aplicaciones informáticas de los servicios, afectando los principios que se establecen y las condiciones que permiten una buena gobernanza.

En cuanto a los servicios públicos, la digitalización de estos con el objetivo de perfeccionarlo, lo expone a inseguridades cibernéticas, alejándose de uno de sus principales roles del Estado: brindar seguridad.

Gobernanza, por su parte, es un concepto sumamente complejo, que reúne una diversa cantidad de variables y parámetros que afectan la capacidad que tienen las administraciones públicas para ofrecer una gran variedad de servicios de manera eficiente y eficaz. Se debe considerar que la soberanía y autonomía de los Estados, como también el desarrollo histórico, cultural, ideológico y político particular de estos, conlleva que no todos los Estados entreguen los mismos bienes y servicios de la misma forma y bajo las mismas normas.

“La conectividad a la red global de los servicios abre una ventana para que diversos actores, con diferentes niveles y capacidades de acceso, vulneren, exploten o expongan los sistemas, las herramientas y las aplicaciones informáticas de los servicios, afectando los principios que se establecen y las condiciones que permiten una buena gobernanza.”

En esta compleja circunstancia, la presencia de innumerables variables de gobernanza, se relaciona de manera intrincada con la seguridad. Cuando se integran estas dos conceptualizaciones a un ecosistema digital, es decir, al ciberespacio tanto como dimensión o bien como herramienta, su resultado será transitar por una red compleja de relaciones causales bidireccionales. Este vínculo genera la necesidad de precisar el significado de los fenómenos involucrados, en este caso de gobernanza digital, seguridad y ciberseguridad.

II. ¿Qué entendemos por gobernanza y gobernanza digital?

Gobernanza y burocracia son dos conceptos que apuntan a lo mismo, pero tienen diferentes características. Gobernanza se puede entender como “el proceso de toma de decisión colectiva e implementación de políticas, utilizada por diferentes niveles de la administración gubernamental para reflejar una preocupación más amplia por las normas y procesos relacionados con la entrega de bienes

públicos"[1]. Por otra parte, burocracia se puede entender como el "gobierno por funcionarios permanentes"[2]. Este último, sin embargo, posee un uso coloquial con percepción negativa desde su origen: ya en el siglo XVII y XVIII[3] se utilizaba "burocracia" como un sinónimo de gobierno ineficiente producto de excesivos procedimientos regulatorios, sostenido posteriormente en los siglos venideros por la proposición de la "Nueva Derecha" sobre la ineficiencia inherente del aparato estatal en comparación con los mercados[4].

Max Weber fue el primer economista, sociólogo e historiador en ver la burocracia en términos positivos[5] al comprender como inevitable el proceso de transición entre una administración del poder político de tipo feudal, gracias a la consolidación de las monarquías absolutas y, posteriormente, de los imperios contemporáneos hacia el aparato moderno de la administración, de manera institucionalizada y despersonalizada[6]. Francis Fukuyama reconoció los esfuerzos de Weber para definir la burocracia de manera positiva, con énfasis en los procedimientos, como clásicos e ideales, pero también como una definición de gobernanza[7]. Sin embargo, Fukuyama no separa estos conceptos, y define gobernanza como la habilidad del gobierno de hacer y ejecutar las reglas, entregar servicios, independientemente de lo democrático o no del gobierno[8]. Un gobierno democrático y uno autoritario puede tener buena gobernanza, de acuerdo a Fukuyama, independientemente de los mecanismos y formas de gobernar que los separa, como también de los objetivos concretos que cada gobierno particular persigue.

Por otro lado, Fukuyama llama a la burocracia weberiana como un parámetro óptimo al que los Estados debían aspirar para considerarse modernos. Este parámetro es el resultado de diez condiciones que se resumen en una administración del Estado profesional, organizada, competente, jerarquizada y meritocrática[9].

A pesar de los esfuerzos de Weber, muchos economistas posteriores continuaron argumentando la ineficiencia de las burocracias como una cualidad inherente a su esencia, y por consiguiente la del Estado[10]. A pesar de la reiterada prevalencia de esta idea, con o sin evidencia empírica, la persistencia del uso conceptual de burocracia para referirse a una deplorable gestión de los gobiernos ha hecho que la conceptualización de gobernanza se posicione como un concepto sustituto para hablar de buena agencia gubernamental o una burocracia eficiente.

Entonces, el concepto de gobernanza ha venido a reemplazar a la burocracia desde la década de los 90 en adelante, promocionado por diversos actores y organizaciones internacionales, en un esfuerzo de mejorar la eficiencia y eficacia de los variados servicios y bienes que provee

[1] BROWN, G. W. (ed.), et. al. Governance. Oxford Concise Dictionary of Politics & International Relations, cuarta edición. Oxford University Press, 2018. p.241.

[2] BROWN, G. W. (ed.), et. al. Bureaucracy. Oxford Concise Dictionary of Politics & International Relations, cuarta edición. Oxford University Press, 2018. pp. 59-60.

[3] *Ibid.*

[4] *Ibid.*

[5] *Ibid.*

[6] SAGER, F.; ROSSER, C. Weber, Wilson, and Hegel. Theories of Modern Bureaucracy. Public Administration Review, Vol.69, No.6, 2009. pp. 1136-1147. Disponible en:<http://www.jstor.org/stable/40469034>

[7] FUKUYAMA, Francis. What Is Governance? Center for Global Development (CGD) Working Paper 314, Washington DC, 2013. p. 1. Disponible en:<http://www.cgdev.org/content/publications/detail/1426906>.

[8] Ibid. p. 3.

[9] *Ibid.*

[10] BROWN, Op.Cit. p. 60.

el Estado a su población, además de incluir parámetros democráticos como características ideales de una buena gobernanza[11].

El desarrollo y masificación del concepto de gobernanza amplía la limitación normativa que carga la burocracia, siendo más que una mera crítica a una administración pública ineficiente. Para esto, la idea de gobernanza incluye a los privados en el aparato de agencia de los Estados al incluir la importancia de las redes que la administración pública genera con la sociedad civil, para bien o para mal[12]. Los actores no gubernamentales y su rol en la provisión de servicios y bienes públicos se encuentran dentro de la conceptualización de gobernanza[13].

Así como Weber, el Banco Mundial (BM) ha desarrollado medidas evaluativas de las seis dimensiones de gobernanza: rendición de cuentas (*accountability*); estabilidad política y ausencia de violencia; efectividad gubernamental; calidad regulatoria; Estado de derecho; y, control de corrupción[14]. El respeto por los derechos humanos es algo que Naciones Unidas (ONU) también determina como variable para evaluar la calidad de la gobernanza, que en definitiva se traduce en parámetros similares al del BM. Ambos organismos concluyen en que una buena gobernanza es "la transparencia, la integridad, la legalidad, las políticas sólidas, la participación, la rendición de cuentas, la capacidad de respuesta, y la ausencia de corrupción y malas prácticas"[15] en la administración pública.

Es necesario aclarar que una definición conceptual de gobernanza más amplia es aquella que se utiliza para hablar del ejercicio de gobernar cualquier institución. Se entiende por gobernanza como "las estructuras y procesos mediante los cuales una organización social (desde la familia hasta las empresas corporativas y las instituciones internacionales) se dirigen a sí misma, desde el control centralizado hasta la autorregulación"[16]. Esta definición resulta suficientemente amplia para ser aplicada a toda corporación e institución, entendiéndose como un "marco de reglas, relaciones, sistemas y procesos dentro y mediante los cuales se ejerce y controla la autoridad en las corporaciones"[17].

En definitiva, los parámetros de la ONU y del BM sobre gobernanza establecen una lista de condiciones para que la administración pública efectivamente logre sus objetivos, sin caer en los problemas asociados a la "mala burocracia". Por otro lado, podemos afirmar que los parámetros para evaluar la administración pública de un gobierno como "buena gobernanza" constituyen tanto procedimientos como características y objetivos del ejercicio tanto del poder ejecutivo como el legislativo y judicial, es decir, todo el aparato estatal.

Una crítica a estas formas de definir la gobernanza es que, desde el ejercicio e implementación, termina siendo tan amplia que parece que gobernanza se transforma en el ideal de la política misma[18]. Es más, el Instituto para la Calidad del Gobierno (QoG) de la Universidad de Gotemburgo ha reunido en una visualización

[11]cUNODC. What is good governance? Anti-Corruption Course, United Nations Office on Drugs and Crime, s.f. Disponible en:<https://www.unodc.org/e4j/zh/anti-corruption/module-2/key-issues/what-is-good-governance.htm>

[12] BROWN, Op. Cit. p. 241.

[13] *Ibid.*

[14] *Ibid.* p. 241.

[15] UNODC. Loc. cit.

[16] HÄNGGI, H., TANNER, F. Promoting Security Sector Governance. European Union Institute for Security Studies (EUISS), Promoting Security Sector Governance in the EU's Neighbourhood, 2005, pp. 11–26. Disponible en:<http://www.jstor.org/stable/resrep07029.5>

[17] GOVERNANCE INSTITUTE OF AUSTRALIA. What is governance? Governance Institute of Australia, Resources, s.f. Disponible en: <https://www.governanceinstitute.com.au/resources/what-is-governance/>

[18] UNODC. Loc. cit.

geográfica los distintos niveles de cumplimiento de gobernanza en los distintos países, donde reconoce 2.500 variables diferentes, ordenadas en 400 categorías, provenientes de diversos índices para poder abarcar las características (y las condiciones que las permiten) de una buena gobernanza[19]. De los numerosos índices que reúne el Instituto, sólo uno se relaciona directamente y explícitamente con gobernanza digital, que es el de "*e-government*", traducido al español como e-gobierno o gobierno electrónico (e-gob). La ONU presenta la siguiente definición para e-gob e incluye en ella la noción de gobernanza y gobernanza digital:

> "Se ha empleado gobierno electrónico para referirse a todo, desde "servicios gubernamentales en línea" hasta "intercambio electrónico de información y servicios con ciudadanos, empresas y otras ramas del gobierno". Tradicionalmente, el gobierno electrónico se ha considerado como el uso de las TICs para mejorar la eficiencia de las agencias gubernamentales y proporcionar servicios gubernamentales en línea. Posteriormente, el marco del gobierno electrónico se amplió para incluir el uso de las TICs por parte del gobierno para llevar a cabo una amplia gama de interacciones con ciudadanos y empresas, así como datos gubernamentales abiertos y el uso de las TICs para permitir la innovación en la gobernanza. Por tanto, el gobierno electrónico puede definirse como el uso de las TICs para prestar de manera más efectiva y eficiente servicios gubernamentales a ciudadanos y empresas. (...) A través de la innovación y el gobierno electrónico, los gobiernos de todo el mundo pueden ser más eficientes, proporcionar mejores servicios, responder a las demandas de transparencia y rendición de cuentas de los ciudadanos"[20].

A partir de esto, se entiende que las limitaciones conceptuales se van difuminando en la práctica en cuanto los procesos y prácticas del Estado se van digitalizando de acuerdo al desarrollo de las TICs y su aplicación en el mundo privado. Ahora bien, el e-gob se presenta como el estado de digitalización, mientras que gobernanza digital se entiende como la forma de accionar y ejercer las funciones públicas. Así es como el e-gob aporta a una buena gobernanza en general. Recogiendo alguna de las características del Banco Mundial y de la ONU sobre buena gobernanza, podemos plantear los siguientes beneficios que el e-gob aporta a este ideal:

1. Las TIC facilitan el acceso, almacenamiento y rapidez de la información promoviendo la transparencia y la rendición de cuentas.
2. La digitalización de la información de los ciudadanos permite mejorar su recopilación, procesamiento y análisis para entregar mejores políticas públicas.
3. Las TIC permiten la conectividad remota e inmediata, incentivando la participación.
4. La digitalización y disponibilidad en línea de procesos burocráticos (entendido como procesos administrativos de provisión de bienes y servicios públicos) permite hacer a los gobiernos más eficaces y eficientes.

Existen incontables ejemplos de aplicación de las TIC que sostienen estos puntos, pero quizás la prueba más emblemática se evidenció durante la pandemia del COVID-19 donde los Estados otorgaron "prioridad a la prestación de servicios en línea centrados en la salud, la educación, la protección social y, en algunos casos, la justicia"[21]. Según sostiene la última encuesta de e-gob de la ONU, "la expansión más notable en la prestación de servicios en línea se ha producido en el ámbito de la protección social; el número de países con portales nacionales que permiten a los usuarios solicitar prestaciones como

[19] DAHLBERG, Stefan; et. al. QoG World Map. The Quality of Government Basic Dataset, The Quality of Government Institute, University of Gothenburg, 2023. Disponible en: <https://worldmap.qog.gu.se/>

[20] ONU. UN E-Government Knowledgebase. United Nations (ONU), Department of Economic and Social Affairs, Division for Public Institutions and Digital Government, s.f. Disponible en: <https://publicadministration.un.org/egovkb/en-us/Overview>

[21] ONU. ONU. UN E-Government Survey 2022: The Future of Digital Government. United Nations, Department of Economic and Social Affairs. p.165-167. Disponible en: <https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf>

atención de maternidad, subsidios infantiles, pensiones, vivienda y subsidios de alimentación ha aumentado un 17% desde 2020"[22].

Por otro lado, las otras variables de buena gobernanza, definida por las organizaciones internacionales citadas, no resultan tan evidentemente relacionadas en lo que entendemos como e-gob. La calidad regulatoria, el Estado de derecho, la legalidad de los procesos, y el control de corrupción resultan variables de buena gobernanza que no se observan afectadas por la masificación del uso de TIC en el ejercicio burocrático. El Basel Institute on Governance (BIG) realizó un reporte de e-gob y prevención de la corrupción en 2017 donde buscaba responder si es que estos dos fenómenos de la administración pública tenían relación. El estudio reveló aclaraciones importantes sobre el e-gob que son necesarias exponer.

"La calidad regulatoria, el Estado de derecho, la legalidad de los procesos, y el control de corrupción resultan variables de buena gobernanza que no se observan afectadas por la masificación del uso de TIC en el ejercicio burocrático."

En primera instancia, el informe asegura que el e-gob es más que la digitalización de servicios, si no que "formas participativas de interacción entre gobierno y stakeholders no gubernamentales"[23]. Con esto encontramos una relación directa entre la variable de "participación". Además, el e-gob supone la inclusión de "análisis de datos usado para mejorar la generación, recolección, intercambio, agregación, combinación, análisis, acceso, búsqueda, y presentación de contenido digital, incluido para el desarrollo de servicios y aplicaciones" como "una parte integral de las estrategias modernizadoras de los gobiernos para crear valor público"[24]. Esta acotación aborda la variable de "políticas sólidas".

En segundo lugar, el reporte del BID aclara que el concepto de e-gob no es estático. Evoluciona y absorbe nuevos elementos. Así lo ha hecho, por ejemplo, "desde sus raíces, en la difusión de información hasta la funcionalidad transaccional y ampliada para incorporar aspectos de inclusión social"[25]. En otras palabras, no es solo compartir información con la sociedad civil, sino que también establecer condiciones para que esa transferencia sea equitativa para una población heterogénea, y una efectiva participación y comunicación en ambas direcciones. Así es como la gobernanza ha cambiado su enfoque de "centrado en personas" a "conducido por personas" donde "los ciudadanos y empresas determinan sus propias necesidades independiente de las autoridades y encuentran soluciones en asociación con los gobiernos" en vez de que las autoridades inviten a las personas a participar cuando lo estimen conveniente[26].

En definitiva, e-gob es la creación de un "ecosistema digital de gobierno donde interactúan los mismos gobiernos con organizaciones no gubernamentales, negocios y empresas, ciudadanos y sus asociaciones, e individuos, para producir, acceder y compartir datos, servicios y contenidos a través de dicha interacción"[27].

---

[22] *Ibid.*

[23] BASEL INSTITUTE ON GOVERNANCE. New perspectives in e-government and the prevention of corruption. Basel Institute on Governance, Working Paper 23, Julio 2017, p. 9. Disponible en: <https://baselgovernance.org/sites/default/files/2019-06/WP_23_web.pdf>

[24] *Ibid.* pp. 13-14.

[25] *Ibid.*

[26] *Ibid*. pp. 13-24.

[27] *Ibid.*

En cuanto a la corrupción, esta es definida por la ONU como "el uso indebido de cargos públicos, poder o autoridad para beneficio privado a través de diversos medios tales como: extorsión, soborno, nepotismo, tráfico de influencias, fraude, dinero rápido o malversación de fondos"[28]. El Banco Mundial amplía el entorno de corrupción "cuando agentes privados ofrecen activamente sobornos para eludir políticas y procesos públicos en busca de ventajas competitivas y ganancias"[29]. Ambas definiciones cubren cualquier tipo de abuso de influencia y poder entre sociedad civil y gobiernos, en ambas direcciones.

En cuanto a la relación, se presume que la conexión entre corrupción y e-gob está dada por la eliminación de los intercambios cara-a-cara con oficiales públicos al reducir o cesar las oportunidades para chantaje[30]. Por tanto, la premisa es que e-gob reduce el riesgo emanado de la toma de decisión discrecional al automatizar el trayecto digital[31]. Además, la aplicación de TIC facilita la variable de gobernanza de transparencia, como se mencionó, y la transparencia "ayuda a aumentar la confianza en el gobierno y reducir la corrupción"[32]. Así es como podemos asegurar que no se puede chantajear un sistema informático para corromperlo, pero sí se puede *hackear.* Sin embargo, el instituto Basel señala que "existe una fuerte correlación positiva entre el desarrollo del gobierno electrónico y el Índice de Percepción de la Corrupción (IPC) de Transparencia Internacional"[33].

"En cuanto a la variable de estabilidad política y ausencia de violencia, muchos expertos de diferentes especializaciones y nacionalidades han hecho eco de que una TIC, en particular, conocida como redes sociales (RR. SS.), ha contribuido fuertemente a la polarización política y por ende a la violencia dentro y fuera de la red."

En cuanto a la variable de estabilidad política y ausencia de violencia, muchos expertos de diferentes especializaciones y nacionalidades han hecho eco de que una TIC, en particular, conocida como redes sociales (RR. SS.), ha contribuido fuertemente a la polarización política y por ende a la violencia dentro y fuera de la red. Existe aún mucha discrepancia sobre cómo y cuánto se atribuye responsabilidad a las plataformas de RR. SS. y sus algoritmos por la polarización política[34] y la violencia que emana de esta.

Lo mencionado se debe principalmente a la complejidad de factores y variables que confluyen en el proceso de generación, propagación y asimilación de la información política que circula en los ecosistemas informáticos, cada uno con sus propias características, además de la complejidad que conlleva definir un único

[28] *Ibid*. p. 20.
[29] *Ibid.*
[30] *Ibid.* p. 13.
[31] *Ibid*. p. 9.
[32] *Ibid.*
[33] *Ibid*. p. 21.
[34] NYHAN, B., SETTLE, J., THORSON, E. et al. Like-minded sources on Facebook are prevalent but not polarizing. Nature 620, pp.137–144, 2023. Disponible en: <https://www.nature.com/articles/s41586-023-06297-w>; CENTOLA, D. Why Social Media Makes Us More Polarized and How to Fix It. Scientific American, Behavior, Opinion, 15/10/2020. Disponible en: <https://www.scientificamerican.com/article/why-social-media-makes-us-more-polarized-and-how-to-fix-it/>; HONG, S., HYOUNG KIM, S. Political polarization on twitter: Implications for the use of social media in digital governments. Government Information Quarterly, vol.33, issue 4, p.777-782. 2016. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0740624X16300375>

entendimiento de polarización política, en cada uno de los contextos políticos nacionales e internacionales donde esto ocurre[35]. En las décadas desde la masificación del internet, donde se advertía de una "ciberbalcanización" en 1996, hasta la actualidad, donde las plataformas de RR. SS. han sido responsabilizadas por crisis políticas violentas, los estudios no son concluyentes a nivel global[36].

Dicho lo anterior, el ecosistema que construyen las plataformas de RR. SS. no es el que es desarrollado, sostenido y regulado por un gobierno. Las RR. SS. son un espacio de comunicación bajo una empresa privada, en donde los individuos y las organizaciones interactúan entre sí y donde el gobierno es un usuario más al que se le solicita información, cumpliendo en parte lo que se pretende lograr con el e-gob[37].

Las RR. SS. son utilizadas por los gobiernos para poder incrementar la participación y la interacción con el público[38], siendo uno de los mecanismos más eficientes para compartir noticias y actualizaciones relacionadas a los servicios que entrega el gobierno y el e-gob[39]. El problema de esto es que el acceso a la información por medio de este tercer actor privado o ecosistema, creado a partir de datos, algoritmos y otras programaciones, puede distorsionar demandas y excluir a quienes no son usuarios o son usuarios inactivos[40]. Además, el ecosistema que configura estas plataformas no es uno representativo de la población a la cual el gobierno sirve, no solo por acceso desigual a estas plataformas, sino que también por la presencia de disímiles usuarios e información falsa.

En los últimos años ha aumentado dramáticamente la manipulación de información en diferentes plataformas digitales, ya sea a favor o en contra de los gobiernos, por obra de ellos o de terceros. De acuerdo a la ONG *Freedom House* "la manipulación de contenidos en línea contribuyó a un séptimo año consecutivo [2010-2017] de disminución general de la libertad en Internet, junto con un aumento de las interrupciones del servicio de Internet móvil y un aumento de los ataques físicos y técnicos contra defensores de los derechos humanos y medios independientes"[41]. Freedom House ejemplifica con el caso de Estados Unidos donde "el uso de "noticias falsas", cuentas "bot" automatizadas y otros métodos de manipulación" si bien no afectaron la libertad del ciberespacio, si evidenció una "perturbación por una proliferación de artículos periodísticos inventados, fuerte crítica partidista divisiva y acoso agresivo" en contexto de campañas políticas u otros procesos políticos[42]. En consecuencia, una creciente preocupación por este fenómeno está empujando a los gobiernos a regular y, en algunos casos, afectar efectivamente la libertad en el ciberespacio.

En sí mismas, "las tácticas de manipulación y desinformación jugaron un papel importante en las elecciones de al menos otros 17 países" durante el 2016, aseguró la ONG, "dañando la capacidad de los ciudadanos para elegir a

[35] BARBERÁ, P. Capítulo 3: "Social Media, Echo Chambers, and Political Polarization" En: PERSILY, N., TUCKER, J. A. (ed.). Social Media and Democracy: The State of the Field, Prospects for Reform. Cambridge University Press, SSRC Anxieties of Democracy, 2020, pp. 34–55. Disponible en: <https://www.cambridge.org/core/books/social-media-and-democracy/social-media-echo-chambers-and-political-polarization/333A5B4DE1B67EFF7876261118CCFE19>

[36] *Ibid.*

[37] ONU, Op. Cit. pp.165-167.

[38] *Ibid.* p. 92.

[39] *Ibid.* p. 106.

[40] *Ibid.* p. 120.

[41] KELLY, S., et. al. Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy. Freedom House, Report, 2017. Disponible en: <https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy>

[42] *Ibid.*

sus líderes basándose en noticias objetivas y debates auténticos"[43]. Es más, el monitoreo de la organización detectó que en 30 países los gobiernos emplearon "ejércitos de "formadores de opinión" para difundir las opiniones del gobierno, impulsar agendas particulares y contrarrestar las críticas del gobierno en las redes sociales"[44]. Este espacio también se ocupa para difundir opiniones que validan métodos antidemocráticos, sean partidarios del gobierno o de la oposición.

La presencia de gobiernos y administración pública en RR. SS. para mejorar la comunicación con la población, en la práctica, no es tan ideal como contribución a la buena gobernanza. "El despliegue de *bots*, productores de propaganda y medios de noticias falsos explotan las redes sociales y los algoritmos de búsqueda para garantizar una alta visibilidad y una integración perfecta con contenido confiable"[45], tanto en beneficio o en desmedro de las actividades y acciones de los gobiernos. Esto debido a que los bots son empleados para hacerse pasar por humanos en debates públicos y otras instancias de comunicación entre gobierno y sus *stakeholders*[46].

"La presencia de gobiernos y administración pública en RR. SS. para mejorar la comunicación con la población, en la práctica, no es tan ideal como contribución a la buena gobernanza."

Para 2019 Freedom House aseguró que "si bien las redes sociales en ocasiones han servido como campo de juego nivelado para el debate cívico, ahora se están inclinando peligrosamente hacia el "iliberalismo", exponiendo a los ciudadanos a una represión sin precedentes contra sus libertades fundamentales"[47]. Aunque para Fukuyama, y su interpretación de Weber, la buena gobernanza es independiente de las características de los regímenes, para la clasificación de la ONU y el Banco Mundial no, por lo que las redes sociales se toman más como una amenaza a la buena gobernanza debido a un importante uso de estas plataformas para consolidar autoritarismos por medio del control de narrativas y opinión pública como también para la supervigilancia masiva[48].

Ahora, podemos concluir que la gobernanza que emana de la transformación digital para la consolidación de un e-gob está dada principalmente porque las TIC permiten un tratamiento y manejo de los procesos administrativos más eficientes y eficaces, tal como lo hacen para todo proceso informático, sea dentro de un aparato público o privado.

En esta eficiencia y eficacia no es solo el acceso a estos procedimientos que facilitan la entrega de servicios públicos, como se observó en el proceso de digitalización durante la pandemia del *Covid*-19. También facilitan la captación de información de la población para generar mejores políticas públicas. La digitalización de portales para la solicitud de información pública, como también la digitalización de los datos que los gobiernos recopilan, favorecen la variable de gobernanza de transparencia, y con eso la rendición de cuentas. De esto emana la relación que existe entre el e-gob y la ausencia de corrupción ya que la automatización de los procesos burocráticos facilita la tentación de

[43] *Ibid.*
[44] *Ibid.*
[45] *Ibid.*
[46] I*bid.*
[47] SHAHBAZ, A., FUNK, A. Freedom on the Net 2019: The Crisis of Social Media. Freedom House, Report, 2019. Disponible en:<https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>
[48] *Ibid.*

manipular al administrador público por medio de sobornos.

Por otro lado, las variables de la gobernanza que resultan más ambiguas en su relación con el e-gob son la participación (que puede ser manipulada a favor o en contra del gobierno) y la ausencia de violencia (que puede incrementar, en algunos casos y condiciones, con la polarización de las RR. SS.).

Resulta, entonces, fundamental considerar que la manipulación de información e identidad presentes en las diversas plataformas digitales es una amenaza a la gobernanza, sin embargo, un excesivo control de estas también. Aquí reside el principal punto de discrepancia a la hora de encontrar una adecuada regulación a estas plataformas, donde se busca un equilibrio entre libertad y seguridad[49].

“La digitalización de procesos administrativos puede ayudar a generar mayores problemas de seguridad, sobre todo cuando no se poseen las condiciones de ciberseguridad necesarias”

Ahora bien, la transformación digital de los procesos burocráticos para alcanzar una buena gobernanza, o e-gob, podría presentar consideraciones diferentes cuando hablamos de un servicio público u otro. La digitalización de procesos administrativos puede ayudar a generar mayores problemas de seguridad, sobre todo cuando no se poseen las condiciones de ciberseguridad necesarias. Por otro lado, un incidente de ciberseguridad, como una filtración de datos sobre una administración corrupta, resulta en una acción de transparencia involuntaria, y una oportunidad para un mejoramiento hacia la gobernanza. En otros casos, en búsqueda de la ciberseguridad y también de la eficiencia y eficacia de los recursos públicos, la administración gubernamental terceriza servicios de TIC y, por ende, ciberseguridad, apelando a la confianza en los privados especializados, presentando mayores problemas de seguridad cibernética.

A continuación, se revisará en detalle lo que entendemos por seguridad, como servicio público, en relación a la gobernanza y el e-gob, del mismo modo cómo estas pueden afectar la ciberseguridad.

/II. ¿Cómo se relaciona gobernanza digital, seguridad y ciberseguridad?

La seguridad es uno de los servicios más esenciales e históricos que proporcionan los Estados. No solo para su propia población sino para sí mismo, en nombre de su población. La definición moderna de Estado es inseparable de la seguridad al poseer el monopolio del poder coercitivo como una función clave de este objetivo[50]. Sin seguridad no existe “la supervivencia de los agentes”[51], ni del Estado, ni del gobierno, ni de ninguno de los stakeholders con los que estos interactúan para entregar bienes y servicios públicos[52]. Además, lo que tradicionalmente significaba la seguridad estaba limitado al ejercicio de fuerza y violencia que ejercían los Estados para protegerse de fuerzas externas[53].

[49] MARTABIT, P. Seguridad versus libertad en el ciberespacio. Academia Nacional de Estudios Políticos y Estratégicos, Centro de Investigaciones y Estudios Estratégicos, Cuaderno de Trabajo N°9-2018. Disponible e: <https://www.publicacionesanepe.cl/index.php/cdt/article/view/902>

[50] HÄNGGI, Op. Cit. p.13.

[51] COLLINS, A. Introduction: What is Security Studies? En: COLLINS, A. (ed). Contemporary Security Studies (sixth edition). Oxford University Press, 2022. p. 1

[52] MARTABIT, P. Infraestructura crítica, usuarios y contenido: ¿Qué se busca proteger en el ciberespacio? Academia Nacional de Estudios Políticos y Estratégicos, Centro de Investigaciones y Estudios Estratégicos, Cuaderno de Trabajo N°9-2019. Disponible en: <https://www.publicacionesanepe.cl/index.php/cdt/article/view/875>

[53] KRAHMANN, E. “Conceptualizing Security Governance.” Cooperation and Conflict, vol. 38, no. 1, 2003, pp. 5–26. Disponible en: <http://www.jstor.org/stable/45083967>

Sin embargo, producto de la aparición y definición de nuevas amenazas emergentes, diversas y complejas, se ha ampliado hacia lo que se concibe como seguridad nacional. Los desastres medioambientales, las pandemias, la hambruna, y el crimen organizado son algunas de las problemáticas que se han ido incorporando como fenómenos que pueden amenazar la supervivencia de los agentes. Así es como "en el concepto de buena gobernanza del sector de la seguridad, la política de seguridad apunta a garantizar no sólo la seguridad del Estado sino también la seguridad del individuo"[54].

Esta expansión de la seguridad, para abarcar más elementos, hace indudablemente que la seguridad y la gobernanza se aproximen. Como el Stockholm International Peace Research Institute (SIPRI) señala, "cuando las instituciones se perciben como justas y eficaces, se respetan y rigen la forma en que interactúan las personas dentro de las sociedades. Sin embargo, cuando las instituciones se consideran ineficaces, excluyentes o corruptas, pueden generar agravios y conflictos"[55]. Es más, SIPRI asegura que "la inclusión y la construcción de instituciones efectivas y legítimas son fundamentales para prevenir recaídas en conflictos violentos y producir Estados y sociedades más resilientes" al ciclo de violencia que ocurre tras una crisis[56]. Esta condición se presenta porque una reforma institucional exitosa y sostenible, después de una crisis política violenta, restablece las funciones básicas de gobernanza y genera una prestación de servicios equitativa[57]. La buena gobernanza permite la consolidación de la paz y, por ende, de la seguridad. "Los sectores de seguridad y justicia mal gobernados suelen ser factores de inseguridad, criminalidad y violencia"[58].

Encontramos que las variables de legalidad y Estado de derecho, corrupción y transparencia de la gobernanza son las que sostienen esta correlación mencionada. La lógica es una de tipo circular, donde la falta de seguridad eficaz no permite una correcta gobernanza, y que la falta de esta alimenta mayor inseguridad. Esta perspectiva se relaciona con la seguridad de la población y no de la estructura y aparato estatal y gubernamental. El cambio de paradigma para el siglo XXI es que cada vez más son los "individuos y grupos sociales que necesitan ser protegidos en lugar del Estado, cuya disfuncionalidad es a menudo la causa principal de la inseguridad"[59]. Esa disfuncionalidad apela a una mala gobernanza.

"... cuando analizamos la seguridad desde la gobernanza, nos referimos a las instituciones que entregan este servicio público de seguridad."

Entonces, cuando analizamos la seguridad desde la gobernanza, nos referimos a las instituciones que entregan este servicio público de seguridad. Se entiende como sector de seguridad a "todas las instituciones estatales que tienen un mandato formal de garantizar la seguridad del Estado y sus ciudadanos de actos de violencia y coerción, como las fuerzas armadas, las policías, gendarmería, servicios de inteligencia, control fronterizo, como también las instituciones judiciales y penales"[60].

[55] KLOPFER, F., et. al. Introduction To Cybersecurity Governance – A Tool For Members Of Parliament. DCAF Geneva Centre for Security Sector Governance, Publication, s.f. p.5. Disponible en: <https://www.dcaf.ch/introduction-cybersecurity-governance>

[55] SIPRI. Peace and development: Governance and Society. Stockholm International Peace Research Institute. S.f. Disponible en: <https://www.sipri.org/research/peace-and-development/governance-and-society>

[56] *Ibid.*

[57] *Ibid.*

[58] *Ibid.*

[59] HÄNGGI, Op. Cit. pp.11–13.

[60] *Ibid.*

Además se incluyen las "autoridades civiles elegidas y debidamente designadas responsables de la gestión y el control de las fuerzas de seguridad, como el gobierno ejecutivo, los ministerios pertinentes (...), el parlamento y sus comités especializados"[61]. Considerando las definiciones amplias de seguridad dado por el creciente número de conflictos violentos internos, también "el poder judicial y los ministerios de justicia, los servicios de investigación y procesamiento penal, los regímenes penitenciarios, los defensores y las comisiones de derechos humanos deben considerarse partes integrantes del sector de seguridad"[62]. Se suman a esta lista a los actores no gubernamentales y sociedad civil como las empresas de seguridad privada, los medios de comunicación, las instituciones de investigación y las ONG[63].

En la actualidad, se habla de buena gobernanza democrática del sector de seguridad cuando existen los siguientes contrapesos a las instituciones estatales que poseen el monopolio exclusivo de la fuerza o violencia física para cumplir seguridad[64]: Marco legal y constitucional; control civil; rendición de cuentas; control parlamentario; control judicial; control público. Por ende, se entiende que "un sector de seguridad puede considerarse disfuncional si no proporciona seguridad al Estado y a su gente o, peor aún, si es causa de inseguridad"[65], afectando directamente en la legitimidad de este uso de la fuerza. Esto es una mala gobernanza en el sector de seguridad.

Ahora bien, dado el desarrollo de TIC y cómo estas han permeado toda actividad humana, resulta necesario entender cómo el sector de seguridad y su buena gobernanza se ve impactado. En el último informe de e-gob de la ONU (2022), que mide la efectividad del e-gob en la entrega de servicios públicos, esta señala que:

> "El [e-gob] ha llegado a un punto crítico. Ya no es una herramienta independiente o auxiliar, ni representa una panacea para las deficiencias o ineficiencias del gobierno; debe verse como un aspecto integral y completamente integrado del funcionamiento físico de las instituciones públicas y la prestación de servicios. El desarrollo digital es inexorable, y la inacción o la acción equivocada pueden ser costosas (...) y profundizar los riesgos (en particular los relacionados con cuestiones de ciberseguridad y privacidad). (...) Los individuos y las empresas pueden cada vez más interactuar con instituciones públicas a través de plataformas en línea, obtener información sobre la legislación relacionada con la libertad de información y acceder a contenidos y datos públicos. (...) Perseguir la transformación digital sin el apoyo institucional, los fondos, las regulaciones, las políticas y las estrategias adecuadas puede provocar pérdidas de empleo, aumento de la desigualdad y problemas de seguridad y privacidad de los datos"[66].

La relación entre TIC y gobernanza es compleja como ya hemos evidenciado, y aún más cuando incorporamos la variable de seguridad. Las TIC pueden ser implementadas para mejorar la seguridad de la población, pero también puede generar mayores inseguridades, ya sea cuando un gobierno autoritario persigue a la población a través de estas TIC o cuando los gobiernos democráticos no tienen las debidas medidas de ciberseguridad para protegerse de agentes maliciosos externos, exponiendo datos personales sensibles que pueden ser explotados para amenazar a las personas.

Un ejemplo de esta relación compleja la podemos ver cuando se habla de la supervigilancia masiva que permiten las TIs. El uso del monitoreo de actividad en línea como la amplia presencia de cámaras de televigilancia, por un lado, permiten crear modelos predictivos para hacer más eficiente y efectiva la entrega de seguridad[67].

[61] *Ibid.*
[62] *Ibid.* p. 14.
[63] *Ibid.*
[64] *Ibid.* p.15.
[65] *Ibid.* p.16.
[66] ONU. Op. Cit. pp. xxiv - xxix.
[67] *Ibid.* pp. 104 - 108.

El problema de la supervigilancia masiva en la práctica es que podría permitir la persecución política por medio del deterioro de la privacidad, invitando al abuso de poder y, a la larga, a una deslegitimación del sector de seguridad.

Por otro lado, si estos sistemas de vigilancia para la seguridad no tienen la debida seguridad informática, pueden estar expuestos a ser explotados por terceros por medio de ciberataques. Se ha señalado como una buena gobernanza al sector de seguridad una que apela a pesos y contrapesos para no abusar de los poderes entregados para cumplir el objetivo de seguridad. Llevado a la ciberseguridad, a mayor cantidad de datos que recopila el Estado para mejorar la gobernanza y a mayor digitalización de sus plataformas, más es la exposición de que estas se vean vulneradas y explotados por agentes de amenazas.

Las TIC no son cajas negras impenetrables, sino que un mal uso o abuso afectan la gobernanza y la seguridad. El "interior" de estas TICs pueden ser manipulados por terceros maliciosos, presentar vulnerabilidades "de fábrica", no tener la adecuada mantención u otros problemas que resultan en una falla de los sistemas y, por ende, en la paralización o afectación de los servicios públicos.

La definición de ciberseguridad entregada por IBM es toda acción que tiene como objetivo "proteger los sistemas, aplicaciones, dispositivos informáticos, datos confidenciales y activos financieros de individuos y organizaciones" contra varios incidentes[68]. Esta protección se entiende, de acuerdo a la normativa de estandarización internacional ISO/IEC 27000 como la preservación de la confidencialidad, la integridad y la disponibilidad[69] de la información, tanto de la infraestructura que constituye un sistema como también el contenido o los datos que se almacenan y comparten. Es por esto que cualquier incidente o acción que tenga el poder interrumpir (contrario a la disponibilidad), dañar y destruir (contrarios a la integridad) se constituye una afectación a la ciberseguridad. Por otro lado, la filtración de datos (contrario a la confidencialidad) también se constituye como un incidente de este tipo.

"Las TIC no son cajas negras impenetrables, sino que un mal uso o abuso afectan la gobernanza y la seguridad."

Como se mencionó, en la definición del concepto de e-gob, la legislación en ciberseguridad se establece como un marco institucional y normativo fundamental para entregar servicios públicos y la participación en línea[70]. Además, es importante la literalidad o alfabetismo digital para que el e-gob pueda ser de igual acceso para todo segmento de la población[71]. De esta forma "comprender y aplicar principios básicos de ciberseguridad, con énfasis en reconocer actividades cibercriminales, desinformación, y noticias falsas" permite una efectiva y correcta entrega de los servicios que entrega el e-gob[72].

Las campañas de alfabetismo digital, recomendadas por la ONU, no solo deben concentrarse en informar que ciertos servicios públicos se encuentran disponibles en línea, sino que también deben generar concientización y correcto uso de las TIC para generar confianza y legitimidad en las plataformas, ya que la

[68] IBM. What is cybersecurity? IBM Security QRadar, s.f. Disponible en: <https://www.ibm.com/topics/cybersecurity#:~:text=Cybersecurity%20aims%20to%20protect%20individuals,attacks%2C%20and%20everything%20in%20between.>

[69] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000:2018(en) Information technology, Security techniques, Information security management systems, Overview and vocabulary. Disponible en: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

[70] ONU. Op. Cit. p. 50.

[71] *Ibid.* p. 134.

[72] *Ibid.*

exclusión digital está perpetuada por ignorancia y desconfianza en las tecnologías[73]. Además, las actividades maliciosas en el ciberespacio socavan la confianza digital hacia y entre los gobiernos[74]. Un Estado y su gobierno que no asegure sus sistemas digitales generan la erosión en la confianza del poder de las instituciones para garantizar el servicio público de seguridad.

Ahora bien, la cibergobernanza digital entendida como la buena gobernanza en el ciberespacio para la entrega de seguridad informática, es decir, la capacidad del Estado de proveer de seguridad informática, posee dificultades particulares por las características del espacio que constituye. El ciberespacio como ecosistema posee una composición particular donde diversos actores son propietarios de las distintas partes del todo, además que la anonimidad es una característica casi innata del ciberespacio[75]. En estas circunstancias, los gobiernos que buscan establecer un e-gob deben, necesariamente, involucrar a actores privados en la entrega de los servicios públicos digitales. Para esto, los gobiernos están efectivamente cediendo control sobre la administración de los datos a terceros, lo que requiere de un alto nivel de fe y confianza en que los proveedores de servicios TIC puedan cumplir con las reglas y regulación de manejo de datos, sin afectar el nivel de seguridad[76].

La difuminación de la frontera, entre lo público y lo privado, cuando hablamos de servicios digitalizados está dado porque los agentes gubernamentales suelen contratar servicios TIC a actores privados. Resulta más eficiente y eficaz con los recursos públicos externalizar la producción de hardware y software al mercado. Sin embargo, el panorama actual sobre amenazas hace necesario que la ciberseguridad sea una condición importante a considerar en la relación pública-privada para el e-gob. Un 27% de la filtración de datos ocurre por medio de la cadena de suministro, es decir por medio de un proveedor de la organización afectada[77].

“La inoperatividad de cualquier servicio público es un grave problema de seguridad. Sin embargo, cuando hablamos de e-gob los parámetros especiales de buena gobernanza para el sector de seguridad se hacen más necesarios.”

La mitad de estos ocurre por medio de proveedores de softwares[78]. Para obtener ciberseguridad en e-gob, es importante considerar la capacidad que tiene la administración pública para exigir a las empresas de las TIC, y sus sistemas de ciberseguridad, parámetros adecuados para lograr esta misma seguridad. En un 25% de los incidentes que resultaron en filtración de datos dejaron inoperativos los sistemas[79].

La inoperatividad de cualquier servicio público es un grave problema de seguridad. Sin embargo, cuando hablamos de e-gob los parámetros especiales de buena gobernanza para el sector de seguridad se hacen más necesarios. Una empresa que entrega servicios TIC al sector de seguridad debe ser entendida como parte de este sector y por ende demostrar responsabilidad frente al sector público. En este ámbito, “sectores de gobierno como defensa

[73] *Ibid.*

[74] Ibid. p. 179.

[75] MARTABIT, P. (2019). Atribuciones en el ciberespacio: Piedra tope en el Derecho Internacional. Academia Nacional de Estudios Políticos y Estratégicos, Centro de Investigaciones y Estudios Estratégicos, Cuaderno de Trabajo N°14-2019. Disponible en: <https://www.publicacionesanepe.cl/index.php/cdt/article/view/870>.

[76] ONU. Op. Cit. p. 179.

[77] IBM SECURITY. Cost of a Data Breach Report 2023. IBM, s.f. p. 32. Disponible en: <https://www.ibm.com/reports/data-breach>

[78] *Ibid.*

[79] *Ibid.* p. 31.

(...) y justicia tienen una baja tolerancia al riesgo y al error"[80] en relación a la digitalización de sus servicios y administración interna, en cuanto lidian con el mandato más importante del Estado, la seguridad. "Un pequeño error operativo o una filtración de datos pueden causar daños que tengan un impacto negativo a largo plazo"[81].

Un incidente en los sistemas informáticos y de comunicaciones del sector seguridad permite la filtración de información que puede ser explotada por un actor de amenaza para realizar un ataque o constituir una amenaza mayor al estar mejor informada de la capacidad y situación de la fuerza del sector. Otro elemento importante que consolida la buena gobernanza en el sector de seguridad es la confianza. Cuando los actores dentro del sector no confían los unos con los otros, la desconfianza ralentiza la colaboración y,, por consecuencia, hace menos eficiente la provisión de seguridad. Cuando las empresas de TIC del sector no logran cumplir con el mandato de seguridad, estas no solo pierden la confianza de las instituciones públicas que le confirieron el servicio o el bien, sino que provocan la desconfianza en este último.

Nada de esto es un aporte a la buena gobernanza del sector. Así lo concluyen los variados reportes del *Geneva Centre for Security Sector Governance* (abreviado como DCAF por su nombre original Democratic Control of Armed Forces). La gobernanza de ciberseguridad, según el DCAF, es cuando "la ciberseguridad debe esforzarse por crear un espacio en línea seguro para todos"[82]. Para lograrlo, asevera el DCAF, "la política de ciberseguridad debe abarcar una serie de cuestiones, que van desde proteger la integridad del Estado y garantizar los derechos humanos de las personas hasta hacer cumplir la ley y prevenir los delitos cometidos en el ciberespacio o a través de él"[83]. Así también, la buena gobernanza de ciberseguridad tiene el desafío en que los roles y las responsabilidades de los diferentes actores suele no estar claramente definida en los marcos normativos[84]. Como muchos servicios esenciales de ciberseguridad son propiedad de actores privados, el Estado depende de una activa cooperación de estos para mantener sus redes y servicios TIC seguros[85].

"Por eso una buena estrategia de ciberseguridad, e inclusive de ciberdefensa, será una que incluya principios de gobernanza, como la inclusividad, la transparencia y la responsabilidad."

Las preguntas que se hace la DCAF para construir un marco regulatorio que propicie la buena gobernanza de ciberseguridad son: ¿Quién controla y quién es responsable por una infraestructura segura o por un contenido en línea seguro? ¿Qué deberes o privilegios se derivan de esta responsabilidad?[86]. Esto es importante porque la seguridad nacional, debido a la información sensible que se maneja en las comunicaciones del sector de seguridad, dependerá cada vez más de los actores privados con cada proceso de e-gob. En consecuencia, no es necesariamente costos, ya que al incentivar la "cooperación y compromiso de los diferentes stakeholders" para una robusta comunidad de confianza en ciberseguridad, se puede aprovechar lo "efectivo y eficiente" de involucrar al sector de seguridad en el e-gob[87].

[80] ONU. Op. Cit. p. 179.
[81] Ibid.
[82] KLOPFER. Op. Cit. p. 5.
[83] *Ibid.*
[84] *Ibid.*
[85] Ibid.
[86] *Ibid.*
[87] *Ibid.*

La consolidación de una comunidad de ciberseguridad es vital, ya que estas pueden consolidar el hábito de compartir información para prevenir y detectar ciber-incidentes[88]. Por eso una buena estrategia de ciberseguridad, e inclusive de ciberdefensa, será una que incluya principios de gobernanza, como la inclusividad, la transparencia y la responsabilidad[89]. Estos valores son aquellos que permiten la generación de confianza en cualquier comunidad.

Uno de los desafíos que plantea el DCAF es que normalmente a los mecanismos de control y supervisión de la gobernanza de ciberseguridad, entre los diversos actores, le falta claridad debido a la compleja mezcla de actores estatales y no estatales involucrados en los ejercicios de la ciberseguridad de las TIC[90]. Además, la buena gobernanza del e-gob con buena ciberseguridad es compleja en tanto los actores privados involucrados no son solo actores nacionales que se encuentran sujetos a las legislaciones y normativas nacionales; un elevado número de ellos suelen ser empresas multinacionales no sujetas a la jurisdicción nacional de un Estado particular[91].

Entre las recomendaciones que tanto la ONU como el DCAF sugieren, Chile las ha desarrollado o se encuentran en desarrollo. Una política nacional de ciberseguridad, legislación sobre la protección a la infraestructura crítica y la protección de datos personales, además de un plan de transformación digital. El DCAF inclusive destaca al Comité Interministerial de Ciberseguridad de Chile como una buena práctica de la cooperación del sector privado[92]. Sin embargo, "los factores principales de vulnerabilidad en ciberseguridad vienen del error humano y de las fallas técnicas" producto de que son los "usuarios de internet no informados que hacen click en los links equivocados la causa más frecuente de ciber incidentes"[93].

"Se estima que un 74% de los incidentes de ciberseguridad son producidos por error y mal uso humano, incluido ataques que utilizan ingeniería social, es decir la explotación de los espacios de ignorancia de las personas."

Se estima que un 74% de los incidentes de ciberseguridad son producidos por error y mal uso humano, incluido ataques que utilizan ingeniería social, es decir la explotación de los espacios de ignorancia de las personas[94]. Por eso no es solo importante una legislación adecuada, sino también la construcción de una cultura de ciberseguridad donde todo el sector de seguridad se encuentre capacitado en prácticas de ciberseguridad en actividades tan mundanas como el uso de correo electrónico. Según un informe, más del 76% de los ataques a la administración pública que ocupan ingeniería social, o la manipulación del usuario, son por medio del uso del correo electrónico institucional[95].

[89] Ibid.

[89] Ibid. p. 6.

[90] Ibid.

[91] DCAF. Guide to Good Governance in Cybersecurity. DCAF Geneva Centre for Security Sector Governance, 2021. p. 12. Disponible en: <https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_EN_Jan2022.pdf>

[92] Ibid. p. 70.

[93] KLOPFER, Op. Cit. p. 6.

[94] VERIZON. 2023 Data Breach Investigations Report. Business Resources and Industry Insights, Data Breach Investigations Report, 2023. Disponible en: <https://www.verizon.com/business/resources/reports/dbir/>

[95] VERIZON. 2023 Data Breach Investigations Report: Public Sector Snapshot. 2023. p.5. Disponible en: <https://www.verizon.com/business/resources/T86a/reports/2023-dbir-public-sector-snapshot.pdf>

Por otro lado, más de un 68% de los incidentes son motivados por actores externos que buscan una ganancia económica[96], más que política [97] Así es como los esfuerzos de la DCAF de entregar buenas prácticas para una buena "ciber higiene"[98] tienen más importancia cuando entendemos el factor humano en la ciberseguridad del e-gob.

IV. Conclusión

No se concibe una correcta gobernanza digital, con adecuado nivel de ciberseguridad, sin una adecuada gobernanza en el sector de seguridad. Tanto por la importancia que se le da al individuo como a la sociedad civil, especialmente a las empresas privadas de TIC, pero también por los principios que persigue. Los principios democráticos como la libertad y la privacidad son valores fundamentales para evitar abusos de las TIC por actores privados y públicos por igual. La explotación de las TIC por parte de gobiernos no democráticos no es un ejercicio de buena gobernanza digital. Por otro lado, la eficiencia y la eficacia en la administración pública se logran con mayores niveles de e-gob, pero esta también debe cumplir con los otros principios de gobernanza. Las amenazas en el ciberespacio no discriminan entre la naturaleza de los actores, por lo que una mala práctica de un individuo podría traer graves consecuencias a la seguridad. Es por esto que la consolidación de una comunidad de ciberseguridad público-privada, tanto nacional como internacional, resulta fundamental.

Se infiere entonces que, en el entorno del ciberespacio, el uso de plataformas digitales; la ignorancia de los usuarios; la falta de competencia de los agentes sobre buenas y seguras prácticas en ciberseguridad, se han situado como puntos determinantes en esta enredada interrelación. En efecto, la explotación de los espacios digitales, producto de la ignorancia de los usuarios, tanto fuera como dentro de la administración pública, constituye el factor principal de inseguridad en esta dimensión.

Conviniendo que la seguridad de las personas y la sociedad constituye un servicio fundamental del Estado, la ciberseguridad se ha convertido en una actividad fundamental, requiriendo para tal efecto de educación y capacitación, principalmente para el sector de la administración pública responsables de la seguridad de la nación. Una apropiada educación y capacitación de ciberseguridad es primordial en tanto la mayor amenaza a los sistemas en línea, y por ende al e-gob, son el factor y error humano. La inclusión de toda la sociedad civil y las instituciones gubernamentales en la normalización de buenas prácticas es aún un punto pendiente por avanzar.

[96] Ibid.

[97] Ibid. p. 7.

[98] BABIC, V., BRATIC, A. Guidebook on Staying Safe Online Cyber Hygiene for Public Institutions and SMEs. DCAF, Geneva Centre for Security Sector Governance, Octubre 2022. Disponible en: <https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookStayingSafeOnline_CyberHygiene_EN_web_Jan2023.pdf>

BIBLIOGRAFÍA

BABIC, V., BRATIC, A. Guidebook on Staying Safe Online Cyber Hygiene for Public Institutions and SMEs. DCAF, Geneva Centre for Security Sector Governance, Octubre 2022. Disponible en: <https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookStayingSafeOnline_CyberHygiene_EN_web_Jan2023.pdf>

BARBERÁ, P. Capítulo 3: "Social Media, Echo Chambers, and Political Polarization" En: PERSILY, N., TUCKER, J. A. (ed.). Social Media and Democracy: The State of the Field, Prospects for Reform. Cambridge University Press, SSRC Anxieties of Democracy, 2020, pp. 34–55. Disponible en: <https://www.cambridge.org/core/books/social-media-and-democracy/social-media-echo-chambers-and-political-polarization/333A5B4DE1B67EFF7876261118CCFE19>

BASEL INSTITUTE ON GOVERNANCE. New perspectives in e-government and the prevention of corruption. Basel Institute on Governance, Working Paper 23, Julio 2017, p. 9. Disponible en: <https://baselgovernance.org/sites/default/files/2019-06/WP_23_web.pdf>

BROWN, G. W. (ed.), et. al. Bureaucracy. Oxford Concise Dictionary of Politics & International Relations, cuarta edición. Oxford University Press, 2018. pp. 59-60.

BROWN, G. W. (ed.), et. al. Governance. Oxford Concise Dictionary of Politics & International Relations, cuarta edición. Oxford University Press, 2018. p. 241.

CENTOLA, D. Why Social Media Makes Us More Polarized and How to Fix It. Scientific American, Behavior, Opinion, 15/10/2020. Disponible en: <https://www.scientificamerican.com/article/why-social-media-makes-us-more-polarized-and-how-to-fix-it/>

COLLINS, A. Introduction: What is Security Studies? En: COLLINS, A. (ed). Contemporary Security Studies (sixth edition). Oxford University Press, 2022. p. 1.

DAHLBERG, Stefan; et. al. QoG World Map. The Quality of Government Basic Dataset, The Quality of Government Institute, University of Gothenburg, 2023. Disponible en: <https://worldmap.qog.gu.se/>

DCAF. Guide to Good Governance in Cybersecurity. DCAF Geneva Centre for Security Sector Governance, 2021. p. 12. Disponible en: <https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_EN_Jan2022.pdf>

FUKUYAMA, Francis. What Is Governance? Center for Global Development (CGD) Working Paper 314, Washington DC, 2013. p. 1. Disponible en: <http://www.cgdev.org/content/publications/detail/1426906>.

GOVERNANCE INSTITUTE OF AUSTRALIA. What is governance? Governance Institute of Australia, Resources, s.f. Disponible en: <https://www.governanceinstitute.com.au/resources/what-is-governance/>

HÄNGGI, H., TANNER, F. Promoting Security Sector Governance. European Union Institute for Security Studies (EUISS), Promoting Security Sector Governance in the EU's Neighbourhood, 2005. Disponible en: <http://www.jstor.org/stable/resrep07029.5>

HONG, S., HYOUNG KIM, S. Political polarization on twitter: Implications for the use of social media in digital governments. Government Information Quarterly, vol.33, issue 4, p.777-782. 2016. Disponible en:< https://www.sciencedirect.com/science/article/pii/S0740624X16300375>

IBM SECURITY. Cost of a Data Breach Report 2023. IBM, s.f. p. 32. Disponible en:<https://www.ibm.com/reports/data-breach>

IBM. What is cybersecurity? IBM Security QRadar, s.f. Disponible en: <https://www.ibm.com/topics/cybersecurity#:~:text=Cybersecurity%20aims%20to%20protect%20individuals,attacks%2C%20and%20everything%20in%20between.>

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000:2018 (en) Information technology, Security techniques, Information security management systems, Overview and vocabulary. Disponible en: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

KELLY, S., et. al. Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy. Freedom House, Report, 2017. Disponible en:<https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy>

KLOPFER, F., et. al. Introduction To Cybersecurity Governance – A Tool For Members Of Parliament. DCAF Geneva Centre for Security Sector Governance, Publication, s.f. p. 5. Disponible en:<https://www.dcaf.ch/introduction-cybersecurity-governance>

KRAHMANN, E. "Conceptualizing Security Governance." Cooperation and Conflict, vol. 38, no. 1, 2003, p. 5–26. Disponible en: <http://www.jstor.org/stable/45083967>

MARTABIT, P. (2019). Atribuciones en el ciberespacio: Piedra tope en el Derecho Internacional. Academia Nacional de Estudios Políticos y Estratégicos, Centro de Investigaciones y Estudios Estratégicos, Cuaderno de Trabajo N°14-2019. Disponible en: <https://www.publicacionesanepe.cl/index.php/cdt/article/view/870>.

MARTABIT, P. Infraestructura crítica, usuarios y contenido: ¿Qué se busca proteger en el ciberespacio? Academia Nacional de Estudios Políticos y Estratégicos, Centro de Investigaciones y Estudios Estratégicos, Cuaderno de Trabajo N°9-2019. Disponible en: <https://www.publicacionesanepe.cl/index.php/cdt/article/view/875>

MARTABIT, P. Seguridad versus libertad en el ciberespacio. Academia Nacional de Estudios Políticos y Estratégicos, Centro de Investigaciones y Estudios Estratégicos, Cuaderno de Trabajo N°9-2018. Disponible e: <https://www.publicacionesanepe.cl/index.php/cdt/article/view/902>

NYHAN, B., SETTLE, J., THORSON, E. et al. Like-minded sources on Facebook are prevalent but not polarizing. Nature 620, pp.137–144, 2023. Disponible en: <https://www.nature.com/articles/s41586-023-06297-w>

ONU. UN E-Government Knowledgebase. United Nations (ONU), Department of Economic and Social Affairs, Division for Public Institutions and Digital Government, s.f. Disponible en: <https://publicadministration.un.org/egovkb/en-us/Overview>

ONU. UN E-Government Survey 2022: The Future of Digital Government. United Nations, Department of Economic and Social Affairs. Disponible en: <https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf>

SAGER, F.; ROSSER, C. Weber, Wilson, and Hegel: Theories of Modern Bureaucracy. Public Administration Review, Vol.69, No.6, 2009. pp.1136 - 1147. Disponible en: <http://www.jstor.org/stable/40469034>

SHAHBAZ, A., FUNK, A. Freedom on the Net 2019: The Crisis of Social Media. Freedom House, Report, 2019. Disponible en: <https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>

SIPRI. Peace and development: Governance and Society. Stockholm International Peace Research Institute. S.f. Disponible en: <https://www.sipri.org/research/peace-and-development/governance-and-society>

UNODC. What is good governance? Anti-Corruption Course, United Nations Office on Drugs and Crime, s.f. Disponible en: <https://www.unodc.org/e4j/zh/anti-corruption/module-2/key-issues/what-is-good-governance.htm>

VERIZON. 2023 Data Breach Investigations Report: Public Sector Snapshot. 2023. p. 5. Disponible en: <https://www.verizon.com/business/resources/T86a/reports/2023-dbir-public-sector-snapshot.pdf>

VERIZON. 2023 Data Breach Investigations Report. Business Resources and Industry Insights, Data Breach Investigations Report, 2023. Disponible en: <https://www.verizon.com/business/resources/reports/dbir/>


CENTRO DE INVESTIGACIÓN Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL