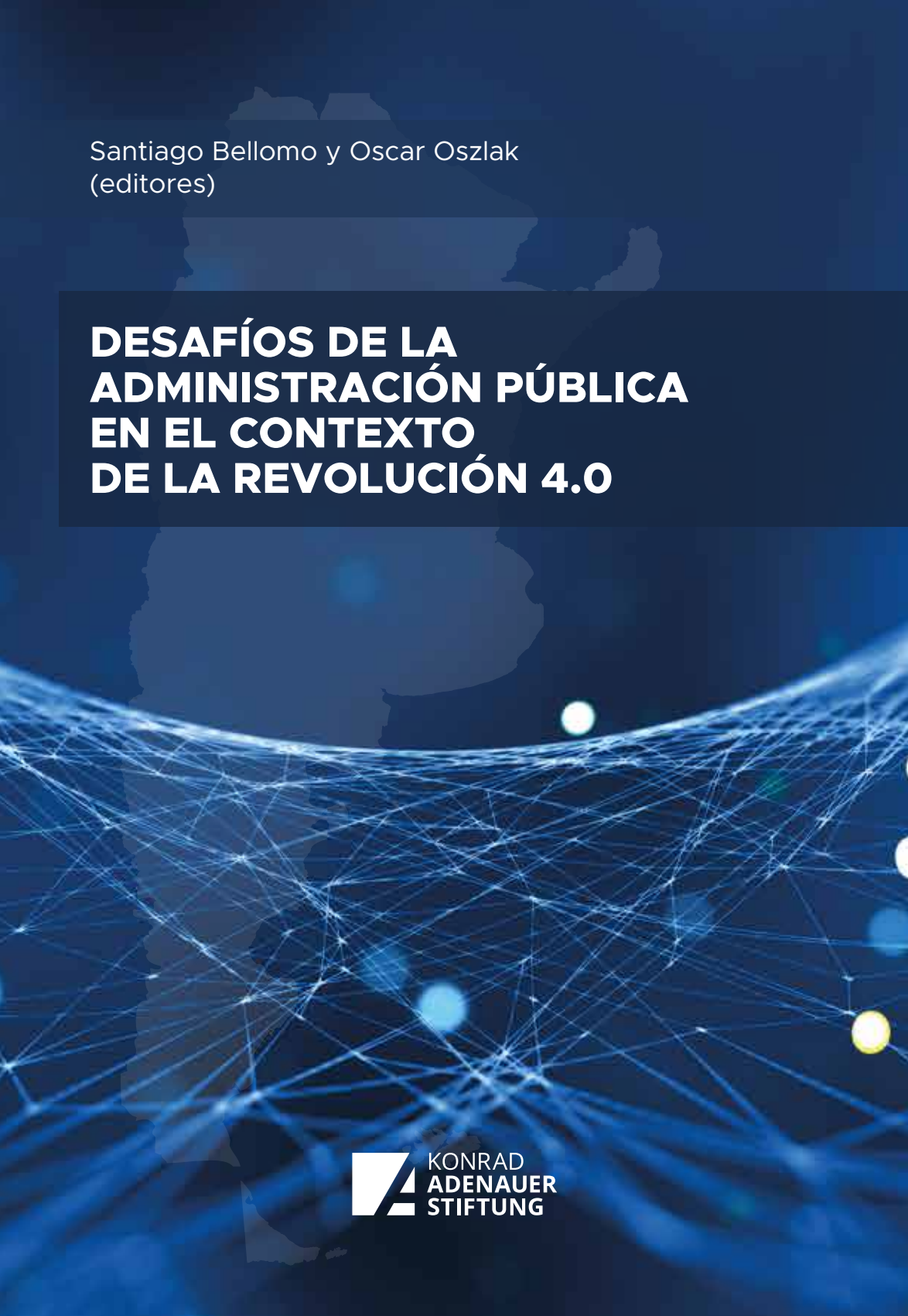
Santiago Bellomo y Oscar Oszlak
(editores)

DESAFÍOS DE LA ADMINISTRACIÓN PÚBLICA EN EL CONTEXTO DE LA REVOLUCIÓN 4.0



KONRAD ADENAUER STIFTUNG

Desafíos de la administración pública en el contexto de la Revolución 4.0

Editores:
Santiago Bellomo y Oscar Oszlak

KONRAD ADENAUER STIFTUNG

Desafíos de la administración pública en el contexto de la Revolución 4.0 / Oscar Oszlak ... [et al.] ; editado por Santiago Bellomo ; Oscar Oszlak. - 1a ed. - Ciudad Autónoma de Buenos Aires : Konrad Adenauer Stiftung, 2020.
327 p. ; 23 x 16 cm.

ISBN 978-987-1285-86-0

1. Inclusión Digital. I. Oszlak, Oscar, ed. II. Bellomo, Santiago, ed.
CDD 351.02854678

Suipacha 1175, Piso 3
C1008AAW
Ciudad de Buenos Aires
República Argentina
Tel: (54-11) 4326-2552
www.kas.de/argentina
info.buenosaires@kas.de

ISBN: 978-987-1285-86-0

Noviembre 2020

Índice

El *back office* de la transformación digital en la administración pública

Prólogo

El trabajo que nos complace presentar aborda los retos que enfrenta la administración pública en tiempos de la revolución 4.0, entendida como una transformación sin precedentes, que excede lo tecnológico y representa un cambio cultural profundo que atraviesa todas las esferas de la actividad humana.

A partir de dos ángulos diferentes y complementarios, estas páginas constituyen un exhaustivo recorrido por diversos aspectos de la transformación digital y cómo esta impacta e interpela a las dependencias estatales en general.

El primero, concerniente a problemas generados por la transformación digital surgidos por fuera de la gestión pública, pero que requieren su intervención, incluye temas como el rol del Estado como regulador, proveedor de servicios, promotor de la innovación y garante de la seguridad ciudadana, la brecha digital de género, la soberanía en un mundo convergente y la gobernanza de internet.

El otro, relacionado con problemas que se generan «puertas adentro» como producto de la transformación digital, incursiona en el diseño de modelos de gobernanza superadores de las herencias burocráticas y verticalistas, el rol de los recursos humanos, el uso del *big data* y las relaciones entre tecnología, política y sociedad.

Las innovaciones siempre influyen en nuestra vida cotidiana. Desde la Fundación Konrad Adenauer, difundimos e implementamos innovaciones que tengan una repercusión positiva sobre la democracia,

la libertad y el bienestar de los ciudadanos. La transformación digital representa, sin duda, una innovación imprescindible que nos brinda herramientas para optimizar los procesos democráticos.

Olaf Jacob
REPRESENTANTE DE LA
FUNDACIÓN KONRAD ADENAUER
EN LA ARGENTINA

Introducción

Santiago Tomás Bellomo

La cuestión de la transformación digital se ha vuelto un tópico de tratamiento obligatorio en las más diversas especialidades, a raíz de la magnitud de su impacto, la extensión de su alcance y la vertiginosidad de su ritmo. Podemos afirmar, sin temor a equivocarnos, que ha conformado un *Zeitgeist,* un determinado «espíritu de la época». El nuestro es un tiempo de interconexión global de máquinas y de personas, de disponibilidad de datos en dimensiones astronómicas, de capacidades para su aprovechamiento inéditas y de automatización, *customización* y digitalización creciente, fenómenos que se han convertido en variables significativas de nuestra vida. La revolución 4.0 que los designa es mucho más que una revolución tecnológica: abarca un cambio cultural profundo que teje nuevos modos de concebir las relaciones sociales y organizacionales, y perfila nuevas identidades y patrones de comportamiento. Su incidencia define estándares más exigentes para medir la calidad de experiencias y el nivel de los servicios. Por supuesto, su acción también genera externalidades negativas vinculadas con nuevos tipos de criminalidad, incremento de la exclusión digital o ampliación de brechas de género.

En el umbral de esta transformación, las organizaciones asimilan un nuevo «imperativo de adaptación». Es preciso ajustarse a los criterios vigentes para asegurar supervivencia y aceptación social. El

dominio público no escapa a este imperativo, aun cuando su velocidad de reacción y capacidad de acomodación pudieran ser menores a las de su contraparte privada. Las administraciones gubernamentales apelan con creciente regularidad a la jerga 4.0 para describir su agenda de gestión y orientar sus comunicaciones internas y externas. El uso de conceptos tales como *big data*, *blockchain*, *machine learning*, *IA*, *IOT*, inunda las conversaciones públicas, así como los títulos de congresos y *papers* de la especialidad. No se trata exclusivamente de una moda. Esta efervescencia pone en evidencia los esfuerzos que realizan sus protagonistas para aprehender cuestiones de difícil asimilación y gran impacto. Por su misma naturaleza, la transformación digital constituye un fenómeno a la vez extraño y familiar. Extraño, en tanto comprende mecanismos y patrones de funcionamiento incomprensibles para quienes no somos tecnólogos. Familiar, en cuanto sus impactos y alcances se experimentan cotidianamente de innumerables maneras.

El presente libro constituye el resultado de un esfuerzo colectivo orientado a facilitar esta tarea de asimilación. Aspira a ofrecer nociones introductorias sobre las distintas dimensiones de la transformación digital y el modo en que afectan o interpelan a las administraciones públicas. No se trata, por tanto, de un libro sobre tecnología ni sobre administración pública. Antes bien, intenta ubicarse en el difuso espacio en que conviven ambos universos, para ofrecer una descripción suficientemente equilibrada y exhaustiva sobre aquellos aspectos a los que más atención corresponde prestar en virtud de su importancia estratégica o necesidad.

El impacto de la revolución 4.0 afecta a la administración pública desde dos ángulos diferentes y complementarios. Por un lado, la interpela a partir de la generación de nuevas situaciones, problemas y desafíos que surgen con motivo del avance de la transformación digital en campos externos a la gestión pública, pero que demandan su

intervención directa o indirecta. Dado que se trata de desafíos que surgen *ad extra* de las administraciones, podemos identificarlos bajo la denominación de ***front desk* de la transformación digital**. Como contrapartida, los organismos y dependencias del Estado también deben asimilar las prácticas y avances de la revolución 4.0 que mejor contribuyan al cumplimiento de su misión. Por tratarse de un esfuerzo realizado «puertas adentro», cabe agruparlos bajo el nombre de ***back office* de la transformación digital.**

1. El *front desk* de la transformación digital en las administraciones públicas

Este primer nivel involucra a los organismos o entes públicos en sus diferentes roles y responsabilidades. Cuatro, en particular, son especialmente interpelados en el marco de la transformación digital que ocurre «puertas afuera» de las administraciones públicas: el rol de la regulación, la provisión de servicios, la promoción de la innovación y el aseguramiento de derechos.

Un ejemplo relativo al rol regulatorio tiene que ver con el surgimiento de las criptomonedas y su utilización para transacciones corrientes. Por tratarse de monedas digitales, su comportamiento no se ajusta totalmente a la dinámica tradicional de intercambio financiero. Es preciso modificar o crear normativas para regular su utilización. Algo similar ocurre con las *fintech*, empresas de tecnología financiera, que se valen de las novedosas transformaciones digitales para ofrecer servicios que, en algunos casos, no operan sobre la base de la bancarización.

La revolución 4.0 también demanda adecuaciones en una misión esencial de las administraciones y organismos públicos: la prestación de servicios. Un ejemplo reciente ilustra este impacto: con el advenimiento de la pandemia COVID-19, los gobiernos provinciales

debieron realizar ingentes esfuerzos para intentar asegurar la continuidad escolar a través de mediaciones digitales de enseñanza. No resultaba suficiente ejercer potestad regulatoria declarando la exigencia de continuidad. En las escuelas de gestión pública, la responsabilidad abarcaba también el aseguramiento efectivo de esta continuidad a través de la generación de condiciones tecnológicas y didácticas adecuadas. Esto implica garantizar niveles suficientes de conectividad, provisión de herramientas y contenidos digitales de enseñanza, entre otras condiciones necesarias.

La transformación digital no es un *commodity* que se importa al modo de un «enlatado». Más allá de que ese sea el caso para algunos insumos en particular, el proceso supone un esfuerzo colectivo de incorporación de conocimientos y habilidades técnicas y sociales, de asimilación de lenguajes y conductas, de adaptación de tecnologías existentes a contextos para los cuales no fueron creadas o de desarrollo de soluciones nuevas *customizadas*. Estos esfuerzos, y otros que podrían añadirse, integran lo que habitualmente llamamos «innovación». La innovación no sucede por ósmosis o efecto contagio. Debe ser promovida, y su promoción también es responsabilidad de las administraciones y organismos públicos. Desde esta óptica, por ejemplo, el estímulo para el estudio de ciertas carreras, el financiamiento de proyectos de transferencia tecnológica en universidades, la creación de incentivos para el desarrollo de *start-ups*, aceleradoras o laboratorios de innovación, constituyen mecanismos necesarios para asegurar una cultura de mejora y actualización permanente.

Oscar Oszlak se concentra en el análisis de estas tres primeras responsabilidades del Estado en el capítulo titulado, precisamente, **«El Estado como regulador, proveedor de servicios y promotor de la innovación»**. Con su característico rigor académico y excelente pluma, describe exhaustivamente los impactos de la era exponencial en

la administración pública y las responsabilidades que conlleva. Esto le permite identificar roles y enunciar algunos lineamientos para iluminar el diseño de un proyecto de transformación. Además, destaca la retroalimentación necesaria que debe existir entre el mencionado proceso y la generación de un Estado abierto, en el que se consolide la transparencia y se potencie la democracia participativa.

Las organizaciones públicas también deben asegurar el respeto de los derechos básicos y fundamentales de la ciudadanía. La revolución 4.0 puede generar directa o indirectamente externalidades negativas que pongan en riesgo estos derechos. Es el caso, por ejemplo, del derecho a la privacidad. Los fenómenos de invasión de la intimidad se vuelven recurrentes y pueden llegar a extremos en que se vulneran derechos constitucionales. Esto sucede, por ejemplo, cuando se viralizan contenidos falsos que afectan gravemente el honor de las personas o se generan perjuicios importantes en su vida personal o profesional. La transformación digital también puede acelerar o potenciar delitos informáticos que afecten a la seguridad jurídica, económica o, incluso, física. Las administraciones públicas están obligadas a extremar recaudos y adquirir nuevas destrezas en orden al combate de cibercrimen.

Enrique del Carril ofrece una descripción detallada sobre los desafíos que interpelan al Estado en materia de protección ciudadana en su capítulo **«El Estado como garante de seguridad del ciudadano individual. Desafíos vinculados con el cibercrimen y el ciberdelito. Desafíos normativos y ejecutivos».** A partir de su experiencia como director del Cuerpo de Investigaciones Judiciales, describe las limitaciones que ofrecen los actuales instrumentos normativos para determinar los alcances de la intervención del Estado en el ciberespacio, toda vez que constituye un ámbito híbrido, que no es ni enteramente privado ni propiamente público. Además, la ausencia de ubicación geográfica dificulta la identificación de responsabilidades y competencias.

Ante circunstancias de tráfico de pornografía infantil o que pongan en riesgo la vida o integridad de las personas, el Estado debe actuar, pero es preciso definir los modos y criterios de su potestad de intervención. Del Carril ofrece valiosas orientaciones en esa dirección, y enfatiza la necesidad de contar no solo con nueva legislación, sino también con nuevos gestores políticos que sepan aplicarla adecuadamente en contextos de creciente complejidad.

Sol Gastaldi, especialista en cuestiones de defensa, considera las implicancias de la transformación digital, no ya desde el punto de vista del aseguramiento de los derechos de la ciudadanía, sino de la preservación de la soberanía y el territorio. El título de su capítulo es sugerente: **«La soberanía en un mundo convergente. Apuntes para entender los dilemas para la seguridad y defensa»**, e ilustra bien la intención de la autora de describir las amenazas al Estado en un contexto definido no ya según el paradigma de la globalización, sino según el paradigma de la convergencia. En este marco, señala que el fenómeno de transformación digital conlleva una profunda modificación de las relaciones entre soberanía y territorio, e invita a seguir ajustando las políticas de seguridad y defensa al componente ciberespacial, para poder enfrentar los riesgos y amenazas de dicho entorno.

A los derechos vinculados con la preservación de la integridad individual y la seguridad nacional se suman los relacionados con la equidad de acceso a la tecnología y la consecuente posibilidad de participación ciudadana en la transformación digital. Ana Basco y Paula Garnero, especialistas del Banco Interamericano de Desarrollo, presentan los resultados de sus investigaciones a partir de la consulta a 20.000 latinoamericanos/as en 18 países de la región, y analizan el impacto del mundo digital en sus vidas, focalizando su atención en la cuestión de l**a brecha digital de género en América Latina.** El capítulo analiza los niveles de penetración de la tecnología, la adquisición de

hábitos digitales, la percepción sobre el impacto de la automatización en el empleo, la inserción de los niños en los procesos de transformación digital, así como el nivel de penetración del comercio electrónico en el entorno regional. Este análisis global permite la identificación de brechas de género en cada uno de los aspectos e induce la propuesta final de algunos interrogantes cuya respuesta debe iluminar la acción de los gobiernos y las políticas de Estado.

Un párrafo aparte merece la discusión relativa a la declaración de internet como «derecho humano de tercera generación» y la responsabilidad consecuente de asegurar niveles de inclusión digital de la población. Los datos revelan por sí solos los fundamentos de este interés. Según estudios recientes (We are Social, 2020), el 67% de la población mundial cuenta con dispositivos móviles (esta proporción era del 50% cinco años atrás), y la tasa de crecimiento anual es de 2,5%. Este crecimiento no parece tan notable como el de la conectividad a internet, que abarca a más de 4,5 mil millones de personas, lo que significa que 6 de cada 10 personas cuentan con acceso a la red. El número se incrementó en casi 300 millones de usuarios en un solo año. La presencia creciente de teléfonos móviles y el acceso a conectividad explican que casi la mitad de la población mundial sea usuaria activa de redes sociales, y que esta tasa esté creciendo a un ritmo sostenido de aproximadamente el 10% interanual desde 2016.

Los números globales tienden a ser un poco más elevados cuando se considera la situación del continente americano, aun con sus disparidades endémicas. Si el promedio mundial de conexión diaria a internet es de 6,43 horas, América Latina lleva la delantera. En Filipinas, las horas de uso por habitante superan las 9,45. Países como Colombia, Brasil, Argentina o México integran el *top ten* mundial de ciudadanos con mayor promedio de consumo diario. El uso de redes sociales en estos países no los ubica en los primeros lugares, pero todos cuentan

con más del 80% de usuarios activos, que llegan al 95% para el caso de la Argentina. Todas estas cifras ilustran un aspecto parcial del fenómeno de la transformación digital. Dan cuenta de las condiciones en que se despliega, así como de su notable alcance e incidencia.

Ante este panorama de extensión geométrica progresiva del acceso a internet, resulta indispensable que los Estados acuerden un modelo para su gobernanza. Agustina Callegari, senior manager en la Internet Society, aporta un interesante capítulo, titulado precisamente **«La gobernanza de internet en Argentina: espacios multisectoriales, desafíos y recomendaciones».** Sus párrafos ofrecen una descripción bien documentada sobre los esfuerzos realizados por nuestro país y por la comunidad internacional para consolidar ámbitos de discusión y acuerdo en torno al gobierno del ciberespacio. En este esfuerzo descriptivo, no deja de señalar las limitaciones y aprendizajes adquiridos en cada instancia y con cada modelo implementado, y detalla el estado de situación actual, puntualizando los principales debates y desafíos a sortear en el nivel local, regional y global.

2. El *back office* de la transformación digital en las administraciones públicas

A los desafíos que la transformación digital genera *ad extra*, que hemos denominado *front desk*, corresponde sumar aquellos que surgen en el *back office*. Estos remiten a las condiciones que deben generarse puertas adentro de los organismos y dependencias del Estado para que puedan responder adecuadamente a los desafíos externos. Existe una variedad amplia de condiciones necesarias. Cabe destacar aquellas que –en función de la experiencia local e internacional– resultan más relevantes por su importancia estratégica o impacto relativo.

Bárbara Ubaldi, jefa adjunta de la División Reforma del Sector Público y jefa del Equipo de Gobierno Digital y Datos Abiertos de la OCDE, ofrece una síntesis muy precisa y bien caracterizada sobre las distintas dimensiones que abarca la transformación digital de las organizaciones públicas. A partir de su vasta experiencia internacional, enfatiza la importancia central de la definición de un modelo de gobernanza que contribuya a superar las naturales desarticulaciones que acompañan el diseño y la gestión de políticas públicas. Sin una gobernanza adecuada, los procesos de transformación digital tienden a constituir fenómenos voluntaristas aislados, de escaso impacto o frágil continuidad. También destaca los criterios rectores que deben orientar los procesos de transformación, que identifica bajo los principios «digital desde el diseño», «apertura por defecto», «orientación al ciudadano», «gobierno como plataforma», «proactividad», «gobierno basado en datos». En su conjunto, el capítulo constituye una referencia obligada para comprender de manera holística los desafíos que deben enfrentar las administraciones para llevar adelante la transformación de su *back office*.

En orden a su implementación efectiva, la transformación digital abarca la progresiva digitalización de procesos, cuyo síntoma visible es la «despapelización», pero cuya naturaleza no es identificable con el mero reemplazo del papel físico por el formulario electrónico. Eduardo Martelli, experto en implementación de transformaciones digitales en la administración pública y exsecretario de Modernización Administrativa, traduce su experiencia tanto en escala jurisdiccional como nacional en **«Aprendizajes y recomendaciones para una efectiva transformación digital»**. En su capítulo, ofrece una identificación de los objetivos centrales que deben orientar el desarrollo de los procesos de innovación pública, describe las diferencias entre desburocratización, agilización y simplificación, e intenta desmitificar varios

prejuicios o supuestos erróneos cuya incidencia suele afectar el desarrollo de transformaciones efectivas.

Por su parte, Diego Pando y Eduardo Poggi, académicos reconocidos en el campo de la administración pública, ofrecen una interesante reflexión sobre el lugar que cabe asignar a los **«Datos masivos para la toma de decisiones públicas: aportes para un debate imprescindible».** El capítulo tiene la virtud de introducir de manera clara y sencilla a la comprensión de un desafío tan complejo como el uso del *big data* en la administración pública. Además de describir el fenómeno de la analítica de datos y el paradigma de la política basada en datos (*data driven policies*), identifican impactos potenciales y reseñan experiencias regionales concretas que contribuyen a visualizar el alcance de la transformación pretendida.

Los aspectos «duros» de la transformación del *back office* no son suficientes si no se acompañan de un trabajo en las dimensiones «blandas», generalmente vinculadas con la gestión de recursos humanos y el cambio cultural. Pablo Legorburu, exsecretario de Empleo Público de la Nación, acomete en su capítulo la desafiante tarea de identificar los principales desafíos que deben resolver las administraciones públicas. En un primer apartado, procurar generar conciencia sobre los desafíos que entrañan para la transformación digital la dimensión y conformación de la administración pública, el marco jurídico laboral y la idiosincrasia cultural. Estos elementos determinan el entorno en que se desarrolla la gestión de los recursos humanos y tienen fuerte incidencia en la promoción de cambios en la dinámica institucional. Luego de describir las bases y componentes de lo que denomina una «estrategia integral de gestión del empleo público» (que, según el autor, constituyen un marco de referencia de los programas, proyectos e iniciativas para el fortalecimiento y jerarquización del servicio público), se aportan lineamientos y recomendaciones sobre algunos

aspectos relevantes de la gestión de los recursos humanos. Ellos aspiran a ser de utilidad para responder a algunos de los desafíos planteados en el primer apartado.

Finalmente, y como requisito transversal subyacente a todo el proceso de transformación, se ofrece una reflexión relativa a los aspectos éticos vinculados con el desarrollo tecnológico en general y su aplicación particular al campo de la administración pública. Martín Parselis, académico experto en la materia, propone una profunda y original aportación relativa a la **«Ética y gobernanza tecnológica en la era de la complejidad».** El capítulo recorre, en rigurosa y clara síntesis, los aspectos filosóficos centrales que enmarcan la relación del hombre con la tecnología, con sus correspondientes señales de extrañamiento y familiaridad. Aporta claves para comprender la relación entre tecnología, política y sociedad, al tiempo que enfatiza la necesidad de una nueva ética, toda vez que la cuestión de la tecnología involucra un problema de gestión de los bienes comunes o *commons*. Ofrece, además, reflexiones relativas al rol del Estado en la gestión de la innovación, y recomendaciones valiosas para orientar el diseño de políticas públicas sobre la base de ejemplos concretos.

Pese a la variedad y cantidad de dimensiones analizadas, resulta innegable que la transformación digital de las administraciones públicas constituye un fenómeno de tal complejidad y magnitud que no puede ser adecuadamente aprehendido mediante un único y limitado acercamiento. Algunas cuestiones han sido explícitamente omitidas en función de su alto grado de especificidad o de la dificultad para el acceso a datos ciertos. Es el caso, por ejemplo, de los impactos de la transformación en dependencias o reparticiones específicas vinculadas con la gestión de la salud, la educación, la economía o el trabajo. En otros casos, temas centrales asociados usualmente a la digitalización han sido incorporados transversalmente, como contenidos de otros

capítulos. Es lo que sucede, por ejemplo, con el abordaje de la cuestión del cambio cultural (inserta en el capítulo sobre gestión de los recursos humanos), o el análisis del paradigma del gobierno abierto y la correspondiente exigencia de transparencia, temas tratados en el capítulo vinculado a los roles del Estado.

En su conjunto, la propuesta goza de suficiente equilibrio y afán comprehensivo, y resultará de especial interés para un público instruido, aunque no especializado. Sacarán especial provecho de su lectura los funcionarios públicos de distintas dependencias y niveles, así como legisladores, formadores de opinión y estudiantes de disciplinas directa o indirectamente vinculadas con la administración pública. A efectos de asegurar el resultado, cada especialista ha realizado un gran esfuerzo para emplear un lenguaje sencillo y amigable, sin resignar por ello rigor o profundidad, acompañando la explicación teórica con ejemplos y recomendaciones prácticas. Cada uno de ellos merece un especial agradecimiento y felicitación por la tarea cumplida. Especial consideración y reconocimiento cabe otorgar a Oscar Oszlak, quien, además de hacer su contribución académica con un capítulo correspondiente, acompañó la producción general de cada autor con una lectura atenta y pródiga en recomendaciones y valoraciones de gran pertinencia y utilidad.

Finalmente, resulta necesario agradecer a la Fundación Konrad Adenauer, por hacer posible la producción de esta publicación en condiciones de especial respeto por la diversidad de opiniones y compromiso con la calidad académica integral de la publicación.

SANTIAGO BELLOMO. Doctor, licenciado y profesor en Filosofía y licenciado en Administración y Gestión de la Educación. Su especialización profesional se concentra en la gestión y planeamiento educativos en diversos niveles del sistema.

Entre sus antecedentes, se destacan sus actuaciones como subsecretario del Instituto Nacional de la Administración Pública de la República Argentina, director de Educación del Ministerio de Energía y Minería de la Nación, gerente de Educación de la Fundación YPF y secretario académico de la Universidad Católica Argentina. Actualmente desarrolla tareas de docencia, investigación y gestión en la Universidad Austral y desarrolla consultoría especializada en materia de capacitación y educación en organizaciones públicas y privadas, con especial énfasis en transformación digital.

Es especialista en cuestiones vinculadas con la educación digital, la educación para el desarrollo sustentable y filosofía de la psicología y la educación. Participa regularmente como miembro evaluador en proyectos de investigación, así como en diversos comités académicos de escuelas e institutos educativos, además de ser autor de numerosos artículos de su especialidad.

El *front desk* de la transformación digital en la administración pública

CAPÍTULO 1

El Estado como regulador, proveedor de servicios y promotor de la innovación

Oscar Oszlak

La primera y segunda revoluciones industriales, que dieron nacimiento a las eras del vapor y la electricidad, duraron, en total, aproximadamente, dos siglos. La tercera revolución, llamada científico-tecnológica o de la informática, se inició en las últimas dos décadas del siglo XX y duró poco más de un cuarto de siglo. Cuando en 2006 fue formalmente reconocida a través de una declaración de la Unión Europea, ya se estaba gestando una cuarta revolución. Una nueva era en la que convergían tecnologías digitales, físicas y biológicas, que en su despliegue y combinación anticipaban cambios radicales en el mundo y en las relaciones humanas tal como las conocemos. En muy pocos años, esta revolución 4.0 ha creado sistemas ciber-físicos en los que se combinan dispositivos y aplicaciones basados en computación avanzada, nanotecnología, internet de las cosas, sensores y comunicación digitalizada, entre otras innovaciones.

Hasta ahora, a pesar de los cambios científicos y tecnológicos que se fueron sucediendo a través de la historia, era posible reconocer la vigencia de ciertas pautas de organización y funcionamiento

de nuestras sociedades, que se venían reproduciendo desde tiempos remotos: la fisonomía de las ciudades, las reglas de sociabilidad, los modos de intercambio de bienes y servicios, el ejercicio de artes y oficios, la atención de la salud, las modalidades de enseñanza-aprendizaje, de producción y apreciación artística o de disfrute del ocio. Por supuesto, todos estos aspectos de la actividad humana sufrieron cambios, pero fueron graduales y siempre fue posible observar su introducción e impacto incremental a través de las sucesivas generaciones.

Hoy, en cambio –y probablemente mucho más en un futuro próximo–, este proceso de cambio disruptivo puede hacer irreconocibles muchos de esos rasgos que caracterizaron nuestra vida y lazos sociales durante siglos. Hemos ingresado en una era exponencial y desconocemos adónde puede conducir un proceso de innovación que es, a la vez, indefinido e ilimitado. No habría que descartar que, en un futuro no muy lejano, debamos seguir numerando revoluciones industriales a intervalos cada vez más breves.

Entre muchos otros impactos generados por esta nueva era exponencial, sobresalen las exigencias que plantea la velocidad de estos cambios a la capacidad institucional del Estado para absorberlos, procesarlos y enfrentar sus consecuencias. Idealmente, como principal instancia de articulación de relaciones sociales, el Estado puede ser visto como el tejido conjuntivo que sostiene y facilita la existencia y vínculos de una comunidad. Materialmente, el Estado constituye el aparato institucional en el que una sociedad decide concentrar el poder y los recursos que aseguren su gobernabilidad y promuevan un desarrollo humano justo y sostenible, en beneficio del conjunto de sus habitantes. Vista desde cualquiera de estos dos planos, su actuación resulta crucial para asegurar la vigencia de reglas de juego que hagan previsibles los intercambios y las

transacciones, el cumplimiento de las normas, el desarrollo de las fuerzas productivas y la distribución equitativa del producto social. Para cumplir este rol, el Estado interviene prácticamente en todas las esferas de la actividad socioeconómica y política, estableciendo derechos y obligaciones, produciendo bienes, prestando servicios, promoviendo iniciativas, invirtiendo recursos o regulando comportamientos. Y en cada uno de estos planos y ámbitos de actuación, sus instituciones deben contar con capacidades de gestión acordes con el volumen, calidad y complejidad de los respectivos servicios y prestaciones.

Si esas reglas se ven radicalmente alteradas por cambios abruptos en las pautas de interacción, organización y funcionamiento de la sociedad, a raíz de una disrupción tecnológica sin precedentes como la actual, todo el aparato institucional del Estado pasa a necesitar otras capacidades y recursos, solo para adaptarse al nuevo ritmo que impone el proceso de innovación tecnológica, y así seguir cumpliendo su papel como regulador, proveedor de servicios e incluso, promotor de la innovación. Este es el tema a desarrollar en este capítulo, en el que analizaré los desafíos que enfrenta la gestión pública ante el cambio exponencial de la cuarta revolución industrial.

Para ello, luego de una breve introducción sobre la disrupción tecnológica de esta nueva era y sus impactos, fundamentaré la necesidad de una intervención estatal activa frente a la innovación, especificando las cuestiones centrales de la agenda estatal que se ven afectadas por el proceso de innovación. Luego examinaré los diferentes roles que puede asumir el Estado según la naturaleza de las tecnologías involucradas, para ofrecer, finalmente, un panorama sobre las políticas que están adoptando los gobiernos en esta materia, particularmente en los países que lideran la innovación tecnológica.

1. La era exponencial y su impacto sobre la gestión pública

El mundo actual asiste a transformaciones simultáneas en el tiempo cuyo impacto no tiene precedentes. Cambios demográficos, desplazamientos en el poder económico mundial, urbanización en gran escala, escasez de recursos naturales, cambio climático y pandemias de alcance global no solo coinciden temporalmente, sino que se manifiestan con una intensidad y alcance inéditos. Sin embargo, esta lista parcial no incluye todavía cambios aún más dramáticos, que no sólo están ocurriendo, sino que previsiblemente tendrán mucho mayor impacto en un futuro próximo. Me refiero a las innovaciones que caracterizan el desarrollo de la tecnología, la digitalización y la ciencia, ámbitos en los que las transformaciones han adquirido un ritmo exponencial. Entre ellas se destacan enormes avances en la electrónica, la comunicación, la inteligencia artificial, la robótica y otras disciplinas, cuyo acelerado ritmo de desarrollo es notoriamente superior a la capacidad de adaptación de las personas e instituciones y, por lo tanto, le otorgan al proceso de cambio un carácter disruptivo.

Los gobiernos y organizaciones del sector público se encuentran en el epicentro de esta «tormenta perfecta» y deben replantearse qué significa gestionar en una era disruptiva. Para colmo, deben hacerlo al tiempo en que deben recuperar la confianza pública, cuya declinación se advierte en casi todas partes. En un contexto de crecientes expectativas y demandas sociales, pero también de magros recursos fiscales, los gobiernos deben tratar de prestar servicios a sus ciudadanos, moderando las inevitables tensiones entre las cuestiones de gobernabilidad, desarrollo y equidad que componen el núcleo problemático central de la agenda estatal.

Hasta cierto punto, las innovaciones de esta era exponencial les permiten aprovechar las posibilidades que ofrecen las nuevas tecnologías en áreas tales como TIC, internet de las cosas, automatización, criptomonedas o impresiones 3D. Pero al mismo tiempo, muchas de estas innovaciones pueden crear importantes desafíos y amenazas, en aspectos tales como la ciberseguridad, la invasión de la privacidad, la desigualdad social, la complejidad regulatoria o los impactos sobre el mundo del trabajo. En todos ellos, el Estado cumple un rol insustituible, tanto para promover la innovación tecnológica como para resguardar a sus ciudadanos de las propias acechanzas que ese desarrollo genera.

La pandemia desatada por el virus COVID-19 ha provisto una magnífica ilustración de las caras opuestas, positiva y negativa, que muestra la disrupción tecnológica, auténtico Jano bifronte. Su cara amable se ha manifestado en la posibilidad de enfrentar y resolver múltiples problemas logísticos, sanitarios, financieros y de seguridad generados por la pandemia. De no haber dispuesto los gobiernos del arsenal tecnológico de la era exponencial, el manejo de esa crisis múltiple habría sido mucho menos eficaz, ya que una variedad de innovaciones jugaron un papel crucial en esa gestión. Plataformas gubernamentales de trámites a distancia permitieron a centenares de miles de personas imprimir al instante, o subir a teléfonos celulares, permisos que habilitaban la circulación de quienes estaban eximidos del aislamiento obligatorio. Otras plataformas hicieron posible, en más de cincuenta países, realizar transferencias de dinero a millones de familias socialmente vulnerables para asistirlas en la emergencia. Esta solución tecnológica, conocida como G2P (*government to people transfers*), puede aplicarse hoy para efectivizar salarios públicos, becas, pensiones, subsidios o transferencias no condicionadas a los pobres.

Pero hay muchos más ejemplos. Las impresiones 3D fueron utilizadas para imprimir, en el hogar y la industria, máscaras, respiradores,

hisopados para testeo y otros insumos médicos. También se utilizó esta tecnología para imprimir, en tiempo récord, salas completas de aislamiento incorporadas a dos hospitales construidos en China en diez días. En varios países incorporaron cadenas de bloques o *blockchain* para ayudar a resolver problemas generados por la pandemia (v.g., plataformas basadas en *blockchain* que permiten a los usuarios rastrear la demanda y cadenas de suministro de implementos médicos o la trazabilidad en la distribución de alimentos). También se ha utilizado *bitcoin* y *blockchain* para recaudar dinero y efectuar donaciones destinadas a víctimas del virus. Y hasta se ha fabricado un lavamanos inteligente que incorpora visión computarizada y tecnología de internet de las cosas, para ayudar a la gente a realizar un lavado de manos más eficaz.

En Túnez y Singapur, robots policiales fueron utilizados para controlar el confinamiento y en España se utilizaron drones para patrullar las calles y enviar mensajes a la población. En otros países se emplearon robots para el control remoto de los infectados por el COVID-19. En Israel, las aplicaciones móviles geolocalizaron y advirtieron a los usuarios haber estado en contacto con infectados o los alertaron sobre posibles focos de infección a evitar en sus recorridos; o sea, una suerte de GPS anti-coronavirus. Por su parte, la inteligencia artificial y el *big data* permitieron a decenas de laboratorios predecir cuáles de las drogas existentes, o nuevas moléculas que simulan drogas, tenían posibilidades de tratar más eficazmente el virus, con lo cual redujeron notablemente los tiempos de investigación a unos pocos meses, cuando normalmente puede demandar una década producir una nueva vacuna, a un costo muy superior. Como última ilustración, cito el caso de China y otros países asiáticos, donde durante la pandemia se utilizó reconocimiento facial y cámaras térmicas para detectar infectados.

Sin embargo, el rostro preocupante de Jano apareció en los fundados temores de que el férreo control social que, en mayor o menor medida, el Estado ejerció durante la pandemia, se mantuviera una vez que la vida cotidiana retornara a la normalidad. El despliegue tecnológico de China, en tal sentido, constituyó el primer experimento social masivo de la historia en que, desde el Estado, se logró escudriñar a fondo en la vida íntima de los ciudadanos. Con el atendible argumento de que las autoridades velaban por la salud pública, el gobierno les exigió –en extendidas zonas del país– utilizar en sus teléfonos celulares un software que decide quiénes deben permanecer en cuarentena o pueden transportarse en subterráneos, circular por shoppings o lugares públicos. No se sabía, a ciencia cierta, cómo clasificaba el sistema a la gente, lo que causó temor y desconcierto entre aquellos obligados a aislarse sin saber por qué.

Human Rights Watch ha señalado que la crisis del coronavirus pasó a ser un hito crucial en la historia de la vigilancia masiva de la población, al abrir la posibilidad de un fisgoneo computarizado que hace posible una completa trazabilidad de los movimientos de cada persona. Muchos analistas han advertido sobre el riesgo de que, una vez pasada la pandemia, estas innovaciones sean utilizadas para un mayor control ciudadano –tanto en China como en países que nadie tildaría como autoritarios–, lo cual entrañaría un serio peligro para la gobernabilidad democrática.

De hecho, en América Latina, la mayoría de los gobiernos adoptaron medidas que tendieron a restringir una serie de derechos que los ciudadanos, hasta la emergencia generada por la pandemia, tenían garantizados por las respectivas constituciones nacionales. Algunos limitaron la libertad individual de circulación, reunión y manifestación, en tanto la mayoría de los países establecieron el aislamiento obligatorio en los hogares y, en varios casos, el toque de queda. El estado de excepción también se manifestó en otros avances sobre los derechos cívicos,

como la restricción del acceso ciudadano a la información pública o la prórroga indefinida de respuesta, por parte del Estado, a las consultas o pedidos de los ciudadanos. Medidas de endurecimiento en el accionar de las fuerzas armadas o de seguridad, de inmunidad frente a sus excesos, de ciberpatrullaje para el control de opositores, de suspensión de la actividad parlamentaria y de concesión de superpoderes al Poder Ejecutivo completaron un panorama ciertamente preocupante.

La tecnología no es más que una herramienta que abre nuevas oportunidades para que los gobiernos adquieran mayor capacidad y sean más eficientes. Pero al amplificar de modo exponencial el poder de los datos, su impacto sobre el bienestar de las sociedades y sobre la naturaleza del régimen político pasa a depender del uso de ese poder. A lo largo de toda la historia de la humanidad, la coerción, el dinero o la ideología han sido empleados como instrumentos de dominación y sojuzgamiento; hoy, la información –como recurso de poder– también puede serlo. En términos potenciales, la acelerada evolución de estas herramientas informativas hace posible utilizarlas –y ya hay suficiente evidencia de ello– para marginar poblaciones discriminadas en virtud de una «decisión logarítmica», para «guiar» las decisiones de consumidores y votantes a partir del conocimiento de sus gustos y preferencias, o para perseguir y encarcelar a opositores políticos.

2. Fundamentos de la intervención estatal frente a la innovación

La actuación de los gobiernos ante a una de las mayores crisis de la historia, como ha sido enfrentar los desafíos del virus COVID-19, fue una inesperada escenificación del futuro. De pronto, la paralización de la actividad productiva aceleró la adopción del teletrabajo, una modalidad ocupacional que venía creciendo muy lentamente como opción

al trabajo presencial y, entre muchas otras, pasó a ser irreemplazable como herramienta de educación virtual. La geolocalización, cámaras térmicas, reconocimiento facial, telediagnósticos y tratamientos a distancia impulsaron avances gigantescos en la atención médica. Drones y robots se convirtieron en presencias más familiares del paisaje urbano. Todas estas innovaciones demostraron, bien a las claras, que el mundo ya incursionó en una nueva era.

Sin embargo, el campo de estudios sobre la gestión pública no ha explorado todavía suficientemente los impactos que la aceleración del cambio tecnológico tendrá sobre la actuación del Estado y la resolución de las cuestiones de la agenda social. Tampoco los gobiernos, al menos en los países más rezagados, parecen haber asumido la responsabilidad de anticiparlos y de evaluar su futuro impacto sobre su gestión. Por ejemplo, los generados por el surgimiento de cuestiones sociales inéditas que exigirán la asunción de nuevos roles y funciones; la consecuente modificación requerida en el perfil y composición de los elencos de funcionarios; la digitalización de procesos administrativos a través de sistemas y aplicaciones revolucionarios; o la atención de mayores demandas de participación ciudadana en la gestión estatal en la medida en que se difunda el Estado abierto como modelo institucional para la gestión pública.

Ante este inminente escenario, este capítulo intenta alertar acerca de la necesidad de aumentar la capacidad de anticipación y preparación del Estado para enfrentar y adaptarse a estos cambios. Para ello, examina algunos de los mecanismos y acciones que están poniendo en marcha los países que marchan a la vanguardia en la innovación tecnológica.

Hay al menos tres razones que justifican esta preocupación. Una es que, librado a su propia dinámica, el cambio tecnológico en ciernes producirá seguramente transformaciones profundas sobre la estructura de poder de los países, la producción e intercambio de bienes y servicios en

el orden nacional e internacional y, por lo tanto, la propia naturaleza del capitalismo como modo de organización social. Se requiere, por lo tanto, un Estado con capacidad preventiva y reactiva para enfrentar y conducir este proceso, sin disuadir la innovación tecnológica puesta al servicio de la producción de bienes y servicios de interés colectivo.

La segunda razón, de especial importancia para los países emergentes, es la posibilidad cierta de que, frente a la aceleración del cambio tecnológico, se ensanche la brecha entre los países que lideran este proceso y aquellos que ni siquiera contemplan por ahora la inminencia y magnitud de sus impactos. Está ampliamente demostrado que el desarrollo económico y social de los países está estrechamente correlacionado con su esfuerzo de generación e incorporación de conocimientos científico-tecnológicos (C&T) a sus procesos productivos. Por lo tanto, es altamente probable que aquellos que queden rezagados en la adquisición de capacidades institucionales de sus Estados para lidiar con esos cambios tecnológicos serán más débiles y se verán más subordinados a los países líderes.

La tercera razón es, principalmente, ética. Si el Estado no está capacitado para comprender los riesgos que trae aparejado el desarrollo e implantación de ciertas innovaciones tecnológicas, así como de regular sus deletéreas consecuencias, la sociedad puede verse expuesta a la voracidad de empresas y emprendedores para los cuales las consideraciones éticas o morales no cuentan y priman solo los criterios puramente mercantiles que inspiran la producción de los bienes o servicios que vuelcan al mercado. Esto puede ocurrir con muchos nuevos desarrollos en el campo de la ingeniería biomédica, la logística del transporte, la robótica en la educación, las plataformas de redes sociales, la ciberseguridad, etcétera.

Por lo tanto, para que las cosas ocurran de uno u otro modo, hay un actor social insustituible a la hora de propiciar, conducir, regular o

impedir que se produzcan los impactos y consecuencias sociales negativas del cambio tecnológico en ciernes. Ese actor es el Estado. Su papel resulta crucial para que el poder combinado de la industria y el *establishment* científico-tecnológico pueda encauzarse en una dirección que aproveche las ventajas de la innovación y evite sus negativas consecuencias sobre el bienestar e interés general de la sociedad. Sólo el Estado, con el activo involucramiento de la ciudadanía y las organizaciones sociales, puede poner freno a los excesos de un transformismo tecnológico sin cauces, sin valores, que sólo obedece a los despiadados principios del mercado o al ciego traspaso de fronteras de una ciencia que olvida que el conocimiento debe ser puesto, en primer lugar, al servicio del ser humano. Sólo el Estado puede evitar que su capacidad de intervención social se vea superada por la velocidad del cambio tecnológico, para lo cual debe conseguir que sus instituciones prevean la direccionalidad de esos cambios y adquieran las herramientas de gestión necesarias para adoptar a tiempo las políticas públicas e implementar las regulaciones que permitan controlar su ritmo y dirección. Sólo el Estado puede impedir que la tecnología ahonde la desigualdad social o incremente la dependencia tecnológica frente a los países líderes y las poderosas empresas globalizadas que controlan el mercado de la ciencia y la innovación. Sólo el Estado puede proteger a los ciudadanos de la vulneración a su privacidad en una sociedad digitalizada, de los crecientes ataques del ciberterrorismo, de la manipulación informativa, del desempleo tecnológico por sustitución robótica o de las caprichosas decisiones adoptadas por arte de algoritmos inhumanos.

Pero quienes gobiernan también pueden ser artífices –inconscientes, involuntarios o deliberados– de los peores escenarios imaginables. Pueden ser cómplices activos de las fuerzas incontroladas del mercado o la ciencia. Pueden utilizar las innovaciones tecnológicas para ejercer el más férreo y despótico control social, haciendo añicos los valores

e instituciones de la democracia. O, simplemente, pueden ignorar las señales y tendencias que ya pueden advertirse, y seguir gestionando «como de costumbre», haciendo caso omiso de los procesos en curso, con lo cual condenarían a sus sociedades a situaciones de miseria y dependencia inimaginables.

De todo esto trata este capítulo, es decir, de lo que deberían hacer los Estados en países menos desarrollados para enfrentar los desafíos de una era exponencial que avanza a un ritmo vertiginoso, que tras las promesas de un futuro mundo feliz, oculta graves amenazas para el bienestar de la sociedad humana.

2.a. Cuestiones centrales de la agenda estatal

Las ciencias sociales han reflexionado bastante acerca de si capitalismo y democracia pueden funcionar en el contexto de economías subdesarrolladas, en las que el Estado ha tenido un papel protagónico en la inversión y en la dirección de la economía, en tanto las clases capitalistas han florecido a su amparo a través de esquemas que implicaron importantes transferencias regresivas de ingresos y riqueza. La literatura también ha puesto en discusión si la democracia es compatible con la equidad social, es decir, si puede asegurar la vigencia de mecanismos de representación, participación ciudadana y, más genéricamente, gobernabilidad, a través de los cuales pueden prosperar y satisfacerse demandas por una distribución más justa del producto social. Finalmente, la literatura analiza si el capitalismo «social», «renano» o «con rostro humano» puede florecer bajo condiciones de ajuste estructural extremo, apertura irrestricta, endeudamiento externo crónico e insuficiente intervención del Estado.

En el trasfondo de esta ecuación, lo que se plantea es el grado de congruencia entre tres cuestiones que, históricamente, no sólo han

dado contenido básico a la agenda del Estado, sino que en su mutuo despliegue han generado tensiones permanentes en el modelo de organización de las sociedades de América Latina. Me refiero a las cuestiones de la gobernabilidad, el desarrollo y la equidad, que son precisamente las que compondrían un modelo de organización social sintetizable como «capitalismo social y democrático». Es decir, una fórmula donde *capitalismo* es un modo de desarrollo, *social* implica un modo de redistribución equitativa del excedente económico y *democrático* refleja un modo de gobernabilidad.

No es trivial que el «sustantivo» de la fórmula sea el capitalismo y lo «social» y «democrático» su adjetivación. Como modo de organización social, el capitalismo presupone la vigencia de reglas y condiciones que, por una parte, viabilicen su funcionamiento «técnico» y, por otra, impidan su eventual desestabilización. Las primeras se relacionan con la creación de un «orden» que, inscripto en múltiples facetas de la interacción social, generen un contexto propicio a la actividad económica propia de un sistema capitalista. Las segundas se vinculan con la adopción de políticas y la puesta en marcha de programas de acción orientados a paliar los costos sociales que se originan cuando el capitalismo, librado a su propia dinámica, agrava las condiciones de precarización y vulnerabilidad de extensos sectores pauperizados, lo que genera no sólo situaciones de inequidad, sino también potenciales focos de violencia y explosión social que conspiran contra la gobernabilidad.

Por eso, el papel del Estado abarca esos tres planos, ya que no existe progreso económico duradero sin orden, ni orden estable sin mínima equidad social. La agenda del Estado nacional se constituyó, históricamente, al compás de sus intentos por resolver los problemas sociales suscitados en torno a estas tres grandes cuestiones. La acción estatal se concentró, primero, en la resolución de las múltiples

manifestaciones de desorden que acompañaron los procesos de organización nacional, incluyendo las derivadas de los enfrentamientos armados, la inseguridad jurídica, la precariedad administrativa, la irregularidad de las finanzas y muchas otras. Poco a poco, estas funciones fueron desplazadas en importancia por las tareas de creación de la infraestructura física que facilitó el gran despegue económico de los países; la promoción de la inmigración y la capacitación de la fuerza de trabajo, que generaron los recursos humanos incorporados a la actividad productiva; o la modernización de la gestión fiscal y financiera, que procuró los recursos que permitieron acelerar el tiempo histórico del progreso nacional.

Al menos para América Latina, el Estado, visto como conjunto institucional, fue el actor clave en este proceso de construcción social, en el que simultáneamente a su constitución como aparato, promovía la conformación de una identidad nacional, de relaciones de producción, de un mercado, de clases sociales y de una ciudadanía política. No casualmente, la estatitad, su constitución definitiva como Estado, coincidió con la gradual conformación de un modo de organización social capitalista. Su agenda, a la vez, se convertía en un terreno de lucha por la atención de los problemas que planteaba el desarrollo del capitalismo y los roles que iba asumiendo fueron, en gran medida, producto de un verdadero proceso de «expropiación social».

Con el crecimiento económico se agudizaron las tensiones sociales, al advertirse que el costo del progreso económico recaía fundamentalmente sobre los sectores populares, cuyo descontento crecía al ritmo de sus expectativas frustradas de mejoramiento económico y ascenso social. La agenda estatal comenzó entonces a engrosarse con diferentes manifestaciones de lo que dio en llamarse «la cuestión social» o, en términos más actuales, la equidad distributiva. Ello alentó en la región movimientos contestatarios, revoluciones, golpes de Estado y

otras formas de inestabilidad social que pusieron en jaque la gobernabilidad de los países.

De este modo, el Estado se fue transfigurando. Fue gendarme, represor y organizador en el plano de sus funciones estrictamente ordenadoras; empresario, subsidiador y promotor en el plano del desarrollo; benefactor, empleador y protector de derechos en el plano de la equidad social. La compleja convivencia de estos roles se prolongó durante la mayor parte del siglo XX y, en la mayoría de las experiencias de la región, acabó configurando un aparato burocrático pesado e inmanejable.

Pasaré por alto, en esta síntesis histórica, los factores que contribuyeron a deslegitimar al Estado, luego de profundas crisis (precio del petróleo en los años setenta, *default* de la deuda externa a partir de 1982, auge del neoliberalismo y del Consenso de Washington, crisis de 2001 y Gran Recesión de 2008) y de cómo todo ello influyó en los procesos de reforma del Estado, tanto en el plano ideológico como en el de la acción. Sólo destacaré que desde fines de los ochenta y durante toda la década del 90, la mayoría de los países del mundo se embarcó en programas de reforma más o menos ambiciosos, cuyo rasgo principal fue la reducción del aparato estatal a través de políticas de desregulación, descentralización, privatización, tercerización y achicamiento de las dotaciones de personal. El Banco Mundial las englobó en la común denominación de «reformas de primera generación», previendo que una «segunda generación» de reformas acometería la tarea de mejorar el aparato institucional remanente, lo cual, en los hechos, sigue estando en buena medida pendiente o inconcluso.

Los resultados de estas reformas en América Latina fueron magros y no llegaron a generar progresos significativos en las capacidades estatales disponibles para promover un desarrollo sostenible, mejorar la equidad social o fortalecer la gobernabilidad democrática. Sus

componentes centrales fueron a menudo contradictorios, sobre todo cuando se pretendió introducir un mismo tipo de medidas en contextos muy diferentes, sin evaluar sus eventuales contradicciones. Y a pesar de que luego del descrédito del neoliberalismo el Estado «regresó» y logró algunos progresos desde el punto de vista de la inclusión social, las relaciones entre gobernabilidad, desarrollo y equidad continuaron mostrando profundas tensiones.

Se deduce de este análisis que pese a los interregnos en que el mercado intentó sustituir al Estado como articulador fundamental de las relaciones socioeconómicas, la organización social «Estado-céntrica» continúa siendo una marca identitaria de la mayoría de los países latinoamericanos. Un rasgo que al tiempo que destaca la centralidad del Estado y muestra la fuerte dependencia de la economía y la sociedad civil respecto de su intervención, pone crudamente de manifiesto sus límites. Es decir, un Estado a menudo capturado por poderosos intereses económicos, que debe operar con recursos escasos, en sociedades profundamente desiguales, con sistemas productivos dependientes de los avatares económicos y financieros de un mundo globalizado y, por lo tanto, con escasa capacidad de adoptar políticas relativamente autónomas.

Si esta interpretación resulta aceptable y la relacionamos con el tema central de este trabajo, al que ahora regresaremos, surgen algunos interrogantes inquietantes. ¿Serán los Estados de la región capaces de enfrentar, orientar y conducir el proceso de innovación tecnológica de la era exponencial? ¿Dispondrán de los instrumentos y los recursos necesarios para aprovechar las ventajas de ese proceso e impedir o mitigar sus efectos perniciosos? En definitiva, ¿podrán las diferentes innovaciones de esta nueva era tecnológica contribuir en los países latinoamericanos a consolidar la gobernabilidad, promover el desarrollo y mejorar la equidad?

2.b. Rol del Estado frente al desarrollo tecnológico exponencial

La aceleración del cambio tecnológico puede generar grandes beneficios, pero, también, perjuicios irreparables: mayor desigualdad social, pérdida de la privacidad, disrupción en el mundo del trabajo, asfixiante control social, pautas culturales aberrantes, entre otras consecuencias negativas. Cuando el acelerador se activa y la velocidad se vuelve incontrolable, es necesario accionar el embrague para cambiar el ritmo de la marcha. El Estado es, a veces, el único actor social capaz de cumplir ese doble rol: actuar como acelerador, promoviendo el proceso de innovación tecnológica, pero, al mismo tiempo, actuar como embrague, para reorientar y regular su marcha.

Como promotor, puede afectar recursos a través de la inversión o subsidio directo a actividades de I&D, a la formación de recursos humanos o a la creación de instituciones y centros de investigación públicos o mixtos. También puede habilitar nuevos emprendimientos (*startups*) o suscribir acuerdos con organismos multilaterales para la canalización de financiamiento o el desarrollo de proyectos multinacionales. Si bien el grado de incertidumbre que rodea al proceso decisorio estatal con relación al rol promotor es alto, lo es quizás más todavía cuando actúa como regulador.

Es que la velocidad del cambio tecnológico es tal, que no permite evaluar claramente sus beneficios frente a sus posibles perjuicios. Consideremos, por ejemplo, el caso de las criptomonedas, cuyas posibilidades y promesas llevaron a numerosos países a invertir e innovar en este campo tecnológico. Así, gobiernos de varias naciones ya han adoptado medidas para reducir o eliminar restricciones regulatorias para las industrias que desarrollan estas tecnologías. Existe bastante consenso en considerar que las mismas constituirán la próxima

frontera de una economía soportada por internet. Pero para otros, las promesas de *bitcoin* y *blockchain* son ejemplos de puro «solucionismo»: responden a la cultura elitista y la perspectiva *tech*-céntrica de la tecnología disruptiva propia de las *startups*. Además, su estructura descentralizada con tecnología de encriptación asegura completa privacidad al usuario y es vulnerable a usos ilícitos, tanto para el lavado de dinero como para la financiación de actividades terroristas. Para colmo, su utilización puede ser contraria a los objetivos de los Estados nacionales, especialmente a raíz de la aparición de Libra, criptomoneda de Facebook, que generó la reacción de decisores políticos en todo el mundo por el poder que así demuestran las grandes corporaciones para pasar por encima de toda forma de regulación estatal.

Consideremos, como otro ejemplo, la robótica. Es indiscutible que las innovaciones en este campo producen enormes beneficios por sus múltiples aplicaciones. Pero también suponen enormes desafíos, no sólo para los responsables de adoptar políticas públicas, sino también para los líderes empresarios, la comunidad jurídica, las instituciones académicas y la ciudadanía, en tanto los robots se vayan incorporando progresivamente a la vida social. Sus impactos sobre el mundo del trabajo ya comienzan a percibirse. La robótica militar y sexual despierta enormes inquietudes y ya desvela a los reguladores. En un caso, por sus consecuencias para una renovada carrera armamentista. En el otro, por los impactos sobre la ética, la salud y la cultura de una práctica que roza el terreno del delito.

Además de promotor y regulador, el Estado es también proveedor de servicios, tal vez su rol esencial. Y en este papel, la tecnología de la era actual puede ser una aliada o, como en las otras modalidades de intervención, una fuente de dificultades. En 2011, Tim O'Reilly acuñó el término *government as a platform*, con el que destacó la capacidad del gobierno para transformar profundamente la provisión de servicios

públicos. Para algunos, se trataba simplemente de un sendero hacia mejores prestaciones. Pero otros lo consideraron como la ruptura definitiva de los compartimentos organizacionales; como una caja de herramientas para los funcionarios públicos; como una plataforma abierta a ser construida; como una nueva infraestructura pública; como sinónimo de coproducción; y como una estrategia para facilitar nuevas instituciones más adecuadas para la era digital.

Metafóricamente, en lugar de observar a la administración pública como una máquina expendedora en la que el ciudadano (contribuyente-usuario) coloca una «moneda» (impuesto) en la «ranura» para obtener una prestación (educación de sus hijos, seguridad vial), comienza a ser vista como una plataforma de servicios personalizados. En la medida en que el desarrollo de *software* se fue trasladando crecientemente hacia la nube, las plataformas crecieron como medio más rápido de proveer una funcionalidad más amplia y novedosa. En tal sentido, el desarrollo de plataformas, por contraposición al desarrollo de servicios estandarizados, se está convirtiendo en la próxima frontera. Esta posibilidad es consecuencia de los enormes progresos producidos en las TIC y en otros desarrollos en el campo del *big data* y la IA.

Las plataformas permiten a las agencias gubernamentales evitar la creación de sistemas monolíticos, cuyo mantenimiento requiere personal altamente especializado y escaso, y cuyas soluciones se transforman en compartimentos estancos. Así, hoy es posible construir microservicios, o sea, funciones basadas en componentes pequeños e independientes, que pueden accederse a través de interfaces de programación de aplicaciones (APIs), tales como verificación de domicilio o registro de avisos de vencimiento, que con un único desarrollo pueden distribuirse a través de múltiples productos. De realizarse debidamente, el proceso permite a los organismos públicos ganar en velocidad, capacidad de respuesta y oferta de servicios que interoperan efectivamente.

El enfoque de plataforma también puede complementar en los gobiernos el desarrollo customizado de *software*. Cuando en los equipos TIC de un gobierno se difunde la noticia de que se han creado microservicios disponibles en una plataforma, los desarrolladores pueden utilizarlos para construir productos customizados, en lugar de escribir un nuevo código fuente, lo cual muestra la versatilidad de estos sistemas.

De hecho, algo parecido ocurre con los portales gubernamentales, donde los ciudadanos y empresas pueden acceder a un enorme número de servicios, como realizar trámites a distancia, obtener información, solicitar turnos, pagar multas o plantear quejas y demandas en línea. Si bien diferentes en su naturaleza y por lo general gratuitos, estos servicios han simplificado enormemente la relación entre Estado y sociedad, al tiempo que han mejorado la transparencia de la gestión pública y abierto mayores posibilidades de colaboración y participación ciudadana en la gestión pública. Las predicciones son coincidentes en el sentido de que esta tendencia tendrá efectos mucho más profundos, en la medida en que el desarrollo de las TIC atraviese nuevas fronteras.

Menciono, por ejemplo, el caso de la llamada «Carpeta del Ciudadano», una aplicación crecientemente adoptada sobre todo por gobiernos municipales, que sirve como «ventanilla única» o punto único de acceso a toda la información relevante que puede consultar un ciudadano en su vinculación con la administración pública (v.g., registros de datos personales, impuestos pagados, recibos, multas, turnos, solicitudes, quejas), posibilitado por las técnicas de interoperabilidad e integralidad, adoptadas cada vez más extendidamente por los gobiernos. Las posibilidades de este canal interactivo podrían aumentar de modo drástico si, además, la carpeta ciudadana contuviera informaciones personalizadas de interés para los usuarios: por ejemplo,

oportunidades laborales frente a situaciones de desempleo, historias clínicas a partir de datos disponibles en centros de salud, certificaciones educativas, créditos para la vivienda disponibles y tantas otras como la imaginación y la tecnología lo permitieran.

Naturalmente, la contrapartida de innovaciones semejantes es la capacidad institucional del Estado para desarrollar y poner a disposición de la ciudadanía este tipo de servicio. Esa capacidad depende de numerosos factores: a) el esfuerzo de desarrollo tecnológico que pueda desplegar o la promoción de este proceso a través de la regulación del mercado, el financiamiento estatal o los emprendimientos de colaboración público-privada; b) el reclutamiento y los programas de formación y capacitación de personal responsable de alimentar y actualizar, en forma permanente, los datos volcados a las carpetas, que responda a la vez a las consultas y propuestas ciudadanas; c) la protección de los datos de los usuarios a través de legislación y los controles ejercidos sobre los grandes oligopolios que dominan el mercado de la información y las redes sociales.

Si bien la transformación digital se ha convertido en una tendencia imparable, el viraje hacia el desarrollo de plataformas exige todavía un importante cambio de mentalidad. Las agencias gubernamentales deben conocer primero sus ventajas para luego empezar a desarrollarlas. En los países emergentes, se requiere, además, tomar conciencia de que la reorientación del gasto hacia este tipo de infraestructura puede suponer enormes ahorros de recursos en el mediano y largo plazos. A veces, las inversiones iniciales pueden disuadir la adopción de esta estrategia.

Por otra parte, en los países en desarrollo existen, al menos, otros tres desafíos que deben enfrentar sus gobiernos para avanzar en sus procesos de digitalización. Uno es considerar internet como un bien público global, promoviendo su expansión para ampliar sus economías

de escala, la creación de redes y las externalidades positivas, sea indirectamente a través de la regulación del mercado de oferentes privados o, directamente, a través de la inversión pública en infraestructura y esquemas colaborativos público-privados.

Un segundo desafío es asumir el firme compromiso de fortalecer la ciberseguridad frente al riesgo cierto de que los sistemas informáticos sean hackeados. Está comprobado que el riesgo cibernético está creciendo para las organizaciones en general y los gobiernos en particular, en la medida en que los ciberataques aumentan en volumen, intensidad y sofisticación. El riesgo no es solamente financiero; también entraña la posibilidad de pérdida de confianza ciudadana, además de distraer la atención de la gestión respecto de otros temas prioritarios.

El tercer desafío exige adoptar una estrategia que conduzca al reemplazo de los llamados «legados informáticos» (*legacy systems*), es decir, tecnologías, sistemas o aplicaciones computacionales que han pasado de moda pero aún se encuentran en uso y plantean serios dilemas a los responsables de la gestión pública. Quienes dedican ingentes recursos presupuestarios y personal a mantener *hardware* y *software* obsoletos deben considerar rápidos cambios en esa dirección, ya que la tecnología está disponible y las ventajas de hacerlo son indudables. Además, las plataformas sin soporte sobre las que corren pueden incrementar los riesgos de ciberataques y, por su inflexibilidad, no permiten modificar procesos adaptados a las herramientas de IA.

Si bien los países más avanzados están lejos de haber resuelto estos tres desafíos, su importancia es particularmente elevada en los más rezagados. Tampoco son los únicos desafíos a afrontar. Sólo me propuse ilustrar la naturaleza de las capacidades que deberán adquirir los Estados para aprovechar las posibilidades y controlar los efectos

perversos de estos desarrollos. También son necesarios consensos regionales para impulsar la rezagada economía digital en América Latina, en comparación con Europa o Asia. Y a pesar de que se registran algunas experiencias exitosas en el país, para cerrar la brecha digital existente se necesitan mecanismos de coordinación más eficaces, que promuevan un mercado regional más competitivo y sostenido que en la actualidad, eviten la duplicación de actividades y la descoordinación entre iniciativas.

La integración digital de la región requiere, entre otras cosas, homogeneizar los marcos legales, regulatorios y de mercado de las economías nacionales para generar mayor confianza, ampliar los circuitos comerciales y potenciar el intercambio de bienes y servicios comercializados a través de plataformas digitales. Una mayor homogeneidad de los marcos institucionales tendería a derribar las barreras que impiden o dificultan el comercio transfronterizo. Por supuesto, también será necesario mejorar la infraestructura digital con conectividad de alta calidad, aumentar la confianza de los inversores y estimular el uso del comercio electrónico entre los más de 600 millones de consumidores de América Latina.

Uno de los mayores desafíos es crear autoridades supranacionales en la región, con capacidad de articular eficazmente el mercado digital. Los esfuerzos realizados en los diferentes bloques de integración subregionales no han tenido éxito en promover una visión común y una agenda que incluya prioridades, objetivos, metas, recursos, mecanismos de gobernanza y un cronograma acordado. Y si bien las distintas asociaciones regionales y subregionales han planteado cuestiones vinculadas con la economía digital, no han conseguido acordar mecanismos de coordinación orientados a concretar esa agenda común ni movilizar suficientes recursos financieros y humanos destinados a gestionar tal agenda.

2.c. Estado abierto y capacidades institucionales

Una de las innovaciones más recientes, que promete transformar la naturaleza de la gestión pública y, por lo tanto, mejorar la capacidad institucional del Estado, es el enfoque de gobierno abierto. En 2009, al asumir su primer mandato, el presidente Barack Obama anunció que el suyo sería un gobierno transparente, participativo y colaborativo, lo que estableció los pilares de una filosofía de gestión estatal llamada a tener amplia repercusión en todo el mundo[1]. La idea de un gobierno abierto (*open government*) no era nueva, pero reafirmaba una concepción acerca de cómo gobernar y de cuál es el rol que juegan el gobierno y los ciudadanos en la gestión pública y en sus resultados.

El veloz desarrollo de las TIC había producido una verdadera revolución, multiplicando sus aplicaciones. La posibilidad de compartir información, la interoperabilidad entre sistemas, los diseños centrados en el usuario y las infinitas oportunidades de colaboración a través de internet habían abierto nuevas y variadas modalidades de interacción social, que podían modificar velozmente la cultura de la gestión pública.

El razonamiento implícito en la noción de gobierno abierto era que: 1) la tecnología disponible permite una fluida comunicación e interacción de doble vía entre gobierno y ciudadanía; 2) el gobierno debe abrir esos canales de diálogo e interacción con los ciudadanos, para aprovechar su potencial contribución en el proceso decisorio sobre opciones de políticas, en la coproducción de bienes y servicios públicos y en el monitoreo, control y evaluación de su gestión; y 3) la ciudadanía debe aprovechar la apertura de esos nuevos canales

---

1 La Open Government Partnership (o Alianza del Gobierno Abierto), constituida en 2010, alcanzó en sólo una década la adhesión de los gobiernos nacionales de casi 80 países.

participativos, involucrándose activamente en el desempeño de esos diferentes roles (como decisor político, productor y contralor).

Hasta aquí el argumento y el razonamiento parecían impecables. Sin embargo, más allá de algunas experiencias aisladas relativamente exitosas que abrigaban expectativas de una rápida difusión de esta nueva forma de gobernar, los supuestos de los que partían los propulsores del gobierno abierto no tenían un sólido sustento real. No pongo en duda que los avances tecnológicos han sido, históricamente, una fuente importante de cambio cultural. Pero la condición básica para que la tecnología incida sobre la cultura es que exista voluntad política para difundir e imponer sus aplicaciones, con todas las consecuencias que ello implica.

Esta afirmación merece una aclaración. La mayoría de las aplicaciones tecnológicas son rápidamente adoptadas por el mercado y los usuarios, sin necesidad de someterlos a compulsión alguna. Pero en el caso que nos ocupa, estamos hablando de **abrir** la «caja negra» del Estado y de instar a los funcionarios a que **escuchen** a los ciudadanos, **respondan** a sus propuestas, los **acepten** como coproductores y admitan que **deben rendirles cuenta**, además de **responder** a sus críticas y observaciones. Se trata de nuevas reglas de juego en la relación gobierno-ciudadanía. Y si bien podemos aceptar, provisoriamente, que la tecnología permitiría esa interacción, también debemos admitir que para que los funcionarios políticos y los administradores permanentes se muestren dispuestos a funcionar bajo estas nuevas reglas, hace falta una enorme dosis de voluntad política desde el más alto nivel gubernamental para imponerlas. Un grado de determinación que rompa con estructuras y mecanismos decisorios ancestrales, que, por muy distintas razones, pocos estarían dispuestos a modificar.

Pero además, del lado de la ciudadanía, la filosofía del gobierno abierto supone que una vez producida la apertura de los canales, los

ciudadanos estarán prontamente dispuestos a participar y ejercer los roles que potencialmente se les atribuyen y reconocen discursivamente. ¿Es posible imaginar esta recreación del ágora ateniense, en un espacio ahora virtual? ¿O, como ocurría en la antigua Grecia, sólo un pequeño grupo de sofisticados oradores y demagogos entablarían un diálogo para discutir y decidir el futuro político de la *polis*? Lo que pretendo destacar es: 1) que, como bien lo ha destacado Amartya Sen, no es concebible la participación de la sociedad civil en el diseño, puesta en marcha y evaluación de las políticas estatales, a menos que esta haya sido empoderada; 2) que el empoderamiento implica que el ciudadano conoce sus derechos individuales y los colectivos, la forma en que se puede obtener la garantía de su ejercicio y la capacidad de análisis de la información pertinente, así como su capacidad de agencia, o sea, de ser o hacer aquello que se tiene razones para valorar; y 3) que, aun empoderado, el ciudadano valora la participación política y tiene la voluntad de ejercerla.

Estos supuestos, del lado de la sociedad civil, negarían de hecho las profundas desigualdades económicas, sociales, educativas y culturales de la población, la brecha digital existente entre clases sociales, la distinta capacidad de agencia de la ciudadanía, el alto grado de desafección política que exhiben muchas sociedades y la natural tendencia al *free riding* de la mayoría de los ciudadanos, que, a diferencia de lo que ocurría en la antigua Atenas, no poseen esclavos que les dejen tiempo libre para acudir a la plaza virtual para deliberar.

De todos modos, es innegable que se han producido avances. Más de cien países cuentan hoy con legislación que consagra el derecho ciudadano a la información pública y, en algunos de ellos, esa norma tiene estatus constitucional. Se están difundiendo cada vez más diversos mecanismos que facilitan el involucramiento ciudadano, como las audiencias públicas, el presupuesto participativo o la votación en línea

de proyectos sometidos a consideración de los ciudadanos, especialmente a nivel de gobiernos subnacionales. La presentación de planes de acción a la Alianza del Gobierno Abierto, en los que se comprometen acciones consensuadas con organizaciones sociales que, a su vez, las monitorean y evalúan, va creando una alentadora rutina. Pero confrontadas todas estas loables iniciativas con las promesas iniciales y las proyecciones académicas del *open government*, me llevan a afirmar que esta filosofía de gestión –como se solía afirmar hace medio siglo con relación al proceso de sustitución de importaciones– se halla todavía en su **etapa fácil**.

Podría objetarse esta afirmación, aduciendo que los progresos en la digitalización de la gestión pública durante la última década darían pie para sostener una conclusión diferente. Por cierto, las TIC han revolucionado la gestión pública y es, tal vez, el área en que mayores avances se han producido en la modernización estatal, sea en la simplificación de trámites, la aceleración de los tiempos de procesamiento de la información, la prestación de más y mejores servicios. El acceso ciudadano a repositorios de información pública, las encuestas de satisfacción de usuarios, el uso de las redes sociales para la comunicación con el gobierno o la celeridad de la respuesta estatal a solicitudes de información por parte de la ciudadanía serían imposibles o resultarían mucho más complejas y lentas de no ser por los soportes electrónicos que facilitan estas gestiones.

Pero gobierno electrónico no equivale a gobierno abierto, aun cuando, en nombre del gobierno abierto, muchas de las iniciativas que los países incluyen en sus planes de acción son típicas de un gobierno electrónico. En cambio, la práctica efectiva de un gobierno abierto nos acercaría al ideal de una democracia deliberativa, o al menos participativa, donde el ciudadano es coprotagonista junto al Estado. Para cumplir ese rol, el ciudadano no sólo debe tener acceso a la información,

sino que debería ser capaz de procesarla y utilizarla para intervenir activamente en todo el ciclo de las políticas públicas.

Pero el terreno de la producción de información es un campo de lucha por la apropiación de un conocimiento que resulte verosímil y pueda ganar legitimidad ante la ciudadanía como expresión objetiva de la realidad. Si desde la perspectiva de la relación «principal-agente» aceptamos que el Estado es agente de la sociedad y esta su principal, debemos preguntarnos qué debe conocer el principal y qué el agente. Si la pregunta la planteamos desde el enfoque del rol que la sociedad encomienda al Estado, la respuesta debería apuntar a los resultados que derivan del desempeño de ese papel. Por lo tanto, el objeto de ese conocimiento debería ser la medida en que esos resultados, en última instancia, promueven o no el desarrollo integral de la sociedad, bajo condiciones de gobernabilidad y equidad.

Si bien esta respuesta es todavía vaga, nos señala la dirección de la búsqueda: el Estado debe conocer si los objetivos que se propuso alcanzar en la gestión del desarrollo fueron efectivamente alcanzados porque, cualquiera fuere el caso, debería rendir cuentas a la sociedad por su desempeño. Para la sociedad, la rendición de cuentas representa la base de datos esencial para juzgar si el contrato de gestión entre principal y agente se ha cumplido, si corresponde o no renovarlo o si conviene probar con otros programas o con otros agentes. Para el Estado, entonces, mejorar la información sobre sus resultados equivale a tornar más transparente su gestión y, en caso de haber producido los resultados propuestos, a legitimar su desempeño y a aspirar –si ello fuera posible o deseable– a renovar el mandato de sus ocupantes. Por eso, todo esfuerzo que se realice para aumentar o mejorar la calidad de la información debería servir a una mejor evaluación del cumplimiento del contrato de gestión entre ciudadanía y Estado.

En última instancia, la filosofía de Estado abierto, que trabajosamente intenta colarse en la gestión pública, se funda en la reducción de las asimetrías de información entre gobernantes y ciudadanos. La transparencia, la rendición de cuentas y la participación son imposibles sin acceso a información y, en definitiva, al conocimiento que este acceso permite a las partes. No sólo para que el ciudadano asuma los roles que le corresponden como «principal», sino también para que los «agentes» puedan gestionar con conocimiento.

Hemos visto que los sistemas de información suelen ser el talón de Aquiles de la gestión pública. Si no se dispone de los datos necesarios para establecer la distancia entre las metas que deben cumplirse y los efectos conseguidos, resulta imposible que funcione un proceso transparente y objetivo de rendición de cuentas. No puede saberse qué insumos fueron asignados a qué responsables, cuáles fueron las actividades que se completaron ni, menos todavía, qué efectos se lograron a través de los productos obtenidos. Idealmente, estos sistemas no sólo deberían informar cuál fue el desempeño en el proceso de conversión de insumos en productos (eficiencia), sino también de qué manera se convirtieron los productos en efectos o resultados inmediatos (efectividad), dimensión mucho más difícil de observar frente a la multidimensionalidad de la mayoría de las cuestiones de política pública.

No obstante, la dificultad no radica sólo en la complejidad de la tecnología requerida, sino en la disposición cultural de los funcionarios –políticos y de carrera– para someterse voluntariamente a la lógica implacable de un sistema que, primero, registra los compromisos de logro de resultados mediante metas e indicadores más o menos precisos; luego, exige el seguimiento o monitoreo del cumplimiento de esas metas en tiempos predeterminados; y, finalmente, expone desnudamente si se lograron o no los resultados finales previstos.

La filosofía de gobierno abierto multiplica hoy estas exigencias, en la medida en que los ciudadanos pasarían a cumplir un rol mucho más protagónico en todas estas instancias de la gestión pública. La tecnología informática dispone hoy de la capacidad necesaria para planificar, programar, monitorear y evaluar resultados en prácticamente cualquier área de la gestión. En cambio, la cultura burocrática es mucho más reacia a aceptar que el desempeño quede expuesto de un modo tan objetivo y personalizado a la mirada inquisidora de quienes pueden demandar una rendición de cuentas por los resultados.

Por eso, los cambios culturales han quedado a la zaga de las innovaciones tecnológicas en esta materia. Por eso, también, han tenido que multiplicarse los controles y exigencias de rendición de cuentas, en sucesivos intentos por compensar esa renuencia a lo que, propiamente, podríamos denominar «respondibilidad». Una condición esencial de una cultura responsable es la lenta decantación en la conciencia de valores que alienten esa disposición ética. Los valores compartidos en este sentido ético seguirán marcando la diferencia entre sociedades que basan la responsabilidad en mecanismos institucionales de responsabilización y sociedades que tienden a fundarla en la respondibilidad. Sólo la tecnología, unida a una firme y persistente voluntad política, podría contribuir a modificar esa cultura y cerrar la brecha.

Reflexiones finales

Desde la invención de la rueda o el descubrimiento del manejo del fuego, las revoluciones científicas y el desarrollo tecnológico han sido palancas fundamentales para la transformación de la civilización. La adopción de la contabilidad por partida doble, durante el Renacimiento, originó las modernas técnicas presupuestarias. La retención de impuestos en la fuente, durante la Segunda Guerra Mundial,

fue una innovación crucial para viabilizar la recaudación tributaria. La innovación acompañó tanto el desarrollo del capitalismo como la modernización de la administración pública. Pero desde fines del pasado siglo, el ritmo de la innovación se ha acelerado. Y en el sector público, ha creado un doble desafío: decidir qué políticas adoptar frente a la multiplicación y vertiginosa transformación de sus desarrollos, y aprovecharlos para su propia gestión.

Las TIC revolucionaron las aplicaciones de inteligencia artificial, el *machine learning* y la interoperabilidad en la gestión pública. Sus avances transformaron el manejo del talento humano, la administración financiera integrada, el gobierno electrónico o las iniciativas de Estado abierto. En cada uno de estos campos mejoraron las metodologías y procesos de generación de información, la calidad de los datos y las posibilidades de consolidación y procesamiento de la información. A su vez, el diseño de novedosos sistemas de información gerencial permitió aprovechar los datos generados para realimentar los procesos decisorios.

El acceso ciudadano a repositorios de información pública, las encuestas de satisfacción de usuarios de servicios públicos, el uso de las redes sociales para la comunicación con el gobierno o la celeridad de la respuesta estatal a solicitudes de información por parte de la ciudadanía serían imposibles o mucho más complejos y lentos, de no ser por los soportes electrónicos que facilitan estas gestiones. La digitalización hizo posible reducir o eliminar los trámites presenciales. Las posibilidades de error o fraude se han reducido visiblemente. Se están extendiendo las enormes ventajas de la Carpeta del Ciudadano, entre otras aplicaciones de las plataformas digitales en el sector público. Y pronto comprobaremos que todas estas innovaciones, cada vez más familiares en los negocios y la vida cotidiana, empalidecerán frente a las que vaticinan quienes saltean y atraviesan fronteras inimaginables de la ciencia y la técnica.

Nada parece interponerse a la tendencia de que el proceso de innovación en el Estado se acelere en el futuro y sea una fuente fundamental de transformación en la gestión pública. No sólo porque las nuevas TIC mejoran controles y reducen costos y tiempos de procesamiento, sino porque, como en otros campos, la tecnología será un factor sobredeterminante de cambio en la cultura administrativa.

Pero en un contexto complejo y cambiante, la incertidumbre será la nota dominante de la gestión de lo público. Si alguna competencia resultará crucial en el futuro, para evaluar el desempeño de los gobiernos, la gestión del riesgo frente a la incertidumbre que genera un cambio de época figurará, seguramente, al tope de la lista. Hace dos o tres décadas, los especialistas en gestión pública mirábamos con cierto recelo esa nueva herramienta del *management* que surgía e intentaba infiltrarse en el repertorio de las tecnologías de gestión. Hoy, a la luz del lugar que esta especialidad pasó a ocupar en la estructura organizativa de organismos públicos y empresas privadas, y del creciente número de funcionarios y ejecutivos que asumen este tipo de funciones, ya no quedan dudas de su importancia.

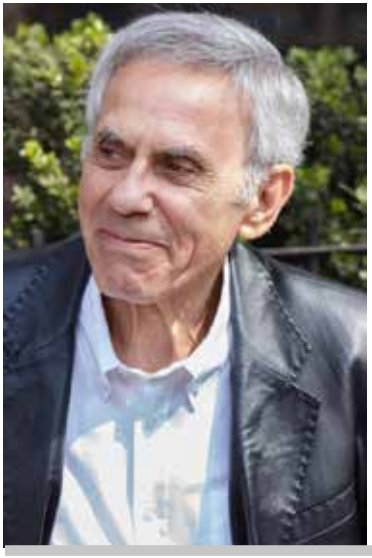
Riesgo no implica, meramente, la amenaza de que cierto objetivo pueda no lograrse. El desafío consiste en balancear riesgos que crean oportunidades con otros que generan amenazas, lo que requiere identificar la «incertidumbre relevante». En la medida en que los focos de incertidumbre que enfrentan los gobiernos se extienden y ahondan, una gran cantidad de riesgos internos y externos puede conspirar contra el logro de sus objetivos y metas. Su naturaleza puede ser estratégica, cibernética, jurídica o reputacional, e incluye aspectos operacionales tales como seguridad informativa, capital humano, control financiero y hasta continuidad institucional.

Si hay algo que caracteriza los riesgos propios de la actividad gubernamental, es su carácter dinámico. Casi nunca son estáticos,

y menos aún en la era actual. Al igual que los virus, que mutan, se forman y transforman de manera nunca vista, todo hace prever que esta característica dinámica de la gestión pública será más crítica en el futuro, en un mundo cada vez más incierto, complejo e interconectado. Hemos podido apreciar que muchas de las transformaciones actuales (v.g., *blockchain*, IA, robótica o tecnologías inteligentes en general) tienen el potencial de mejorar el desempeño gubernamental, pero también comprobamos que cada una de ellas crea riesgos potenciales, cuyo común denominador es que, en su mayoría, son desconocidos e irreconocibles. Y eso que, por lo limitado del alcance de este trabajo, no hubo oportunidad de hacer referencia a muchas otras innovaciones tecnológicas que también comprometen la actuación del Estado en tanto promotor, regulador o usuario, tales como el internet de las cosas, los vehículos autónomos o las impresiones 3D.

El riesgo tecnológico crea creciente incertidumbre y exige a los líderes gubernamentales anticipar el futuro con visión estratégica. El ecosistema institucional del sector público es crecientemente complejo a raíz de la creciente interconexión e interoperabilidad de los organismos públicos, que comparten datos, sistemas y dispositivos que elevan los niveles de riesgo; y la natural renuencia de esos organismos a cooperar o coordinar acciones, y su preferencia de funcionar bajo el formato de «silos» aumenta aún más los riesgos.

Por eso, en última instancia, el principal objetivo de este trabajo ha sido alertar acerca de la necesidad de mejorar la capacidad institucional de los gobiernos para alinear su desempeño con las exigencias de velocidad, complejidad y crecientes expectativas ciudadanas de recibir mejores, más rápidos y menos costosos bienes y servicios públicos, en un mundo en que la tecnología avanza y seguirá avanzando a un ritmo exponencial.



OSCAR OSZLAK. PhD Political Science y Master of Arts in Public Administration, UC Berkeley. Doctor en Economía y Contador Público Nacional (UBA, Argentina). Graduado del International Tax Program, Harvard Law School. Creador y exdirector de la Maestría en Administración Pública UBA. Investigador Superior CONICET. Expresidente de la Red INPAE (Inter American Network for Public Administration Education. Exsubsecretario de Reforma Administrativa y Asesor Presidencial (Presidencia Alfonsín). Fundador y expresidente de la Sociedad Argentina de Análisis Político, 1983-1994. Profesor Titular en Programas de Posgrado de las Universidades de San Andrés, FLACSO, Tres de Febrero, San Martín, Buenos Aires y otras. Profesor del Instituto del Servicio Exterior de la Nación. Obtuvo los siguientes premios y becas: United Nations Fellow, Peter Odegard Award, Tinker Foundation, Rockefeller Foundation, Guggenheim Fellow, Ford Foundation, CLAD, etc. Ganador del primer International Public Administration Award 2003 (American Society for Public Administration). Personalidad Destacada de las Ciencias Económicas, Políticas y Sociales por Ley de la Legislatura de

la Ciudad de Buenos Aires. Doctor Honoris Causa de la Universidad Nacional de Cuyo (2015). Profesor Consulto de la Facultad de Ciencias Sociales, UBA. Profesor Extraordinario de la Universidad Nacional de Villa María. Premio «Domingo F. Sarmiento» del H. Senado de la Nación Argentina (2017). Autor de *La formación del Estado argentino*, *Merecer la ciudad: los pobres y el derecho al espacio urbano*, *Proceso, crisis y transición democrática*, *Estado y sociedad: nuevas reglas de juego*, *Teoría de la burocracia estatal: ensayos críticos*, *La trama oculta del poder*, *El Estado en la era exponencial* y alrededor de 250 artículos, capítulos de libros, etc., publicados en Argentina, Estados Unidos, Europa y Asia.

CAPÍTULO 2

El Estado como garante de seguridad del ciudadano individual. Desafíos vinculados con el cibercrimen y el ciberdelito. Desafíos normativos y ejecutivos

Enrique del Carril

Introducción

Preguntarnos sobre la seguridad individual en el ciberespacio nos obliga a reflexionar sobre cuestiones previas que se relacionan con lo que ha implicado el ingreso, abrupto muchas veces, de las sociedades y las personas en la era de la información. Esa irrupción del mundo digital en absolutamente todos los aspectos de nuestra vida ha generado cambios profundos, que van más allá de meras cuestiones de costumbres de consumo o de manera de interrelacionarse.

Sin embargo, no es el objetivo de este trabajo tratar estos temas, sino reflexionar sobre cómo ha afectado nuestra seguridad (y la percepción que tenemos de ella) en nuestra condición de cibernautas. Porque esta nueva vida en línea, que ya es una dimensión vivencial,

una parte constitutiva de nuestro existir, parece haber sido descuidada por quienes tienen la misión de gobernarnos y asegurar nuestra seguridad, nuestro espacio y nuestras posibilidades en la vida en sociedad.

Tenemos la sensación de que el Estado no acierta a encontrar su papel en el ciberespacio, que todos sus intentos de intervenir en él son inútiles y, paradójicamente, a la vez totalitarios: el Estado de naturaleza salvaje del Leviatán de Hobbes convive con la sociedad distópica orwelliana de 1984.

En lo que sigue, se analizarán las obligaciones y los límites que tiene el Estado en su función específica de garantizar la seguridad personal de sus ciudadanos. Para ello, es preciso indagar en dos conceptos que parecen estar en pugna: seguridad individual y ciberespacio, y a partir de ellos se intentará delimitar cuál es el papel de los Estados nacionales en el ecosistema digital.

Para ello, nos haremos tres preguntas, cuyas respuestas son consecutivas y dependientes una de la otra. El primer interrogante es si efectivamente es el Estado quien debe proteger la seguridad personal en el ciberespacio, teniendo en cuenta las particularidades de este «lugar» en comparación con los espacios físicos en los que el Estado normalmente actúa.

Si llegamos a la conclusión de que existe un ámbito de incumbencia estatal en el ciberespacio, deberemos preguntarnos por su extensión, esto es, cuáles son los temas u obligaciones que tiene el Estado en la protección de sus ciudadanos en el mundo digital y cuáles sus límites y restricciones. Esta delimitación nos llevará al tercer interrogante, que involucra la demarcación de los medios que tiene el Estado para realizar este cometido.

En definitiva, el objetivo de este trabajo es llamar la atención sobre las características de la intervención estatal en línea en defensa y protección de sus ciudadanos. Para ello, es importante tener en cuenta

que el papel que le asignemos al Estado en la definición y concreción del desarrollo de las personas es determinante del grado de injerencia que este tendrá en el mundo digital y, en especial, de los medios que puede utilizar para lograr estos objetivos.

1. El Estado y la seguridad individual

Hasta hace apenas unas décadas atrás, la afirmación de que el Estado debía proveer y proteger la seguridad individual de sus ciudadanos era una obviedad. Más allá de las decisiones u opciones ideológicas sobre las dimensiones e incumbencias del Estado a las que se adhiriera, nadie dudaba de que una de sus funciones esenciales era la seguridad interior. El Estado debía proteger a sus ciudadanos, castigar los delitos y asegurar el bienestar, o al menos la paz, dentro de sus fronteras.

Para ello, el Estado de derecho, desde su misma concepción en el siglo XIX, cuenta con instrumentos jurídicos específicos. Además, las condiciones de uso de estos instrumentos están perfectamente delineadas en sus posibilidades y límites: el Estado cuenta con el dominio, mediante la ley y el poder de policía, de los espacios públicos o comunes en donde se desarrolla la vida social y tiene vedado el ingreso a los espacios privados y a las esferas de desenvolvimiento individual de sus ciudadanos; esta limitación es, también, un aspecto de la seguridad individual: existe una zona reservada al individuo que no puede ser penetrada por nadie.

Y más allá de algunas ambigüedades menores, la diferencia entre estos dos espacios de la vida social era más o menos clara. Y de allí que las reglas del accionar estatal también lo eran: el poder ordenador del Estado tenía plena vigencia y acción en los ambientes públicos o comunes y sólo podía por excepción ingresar en los privados. Para poder

acceder a la privacidad individual, la ley establece, en prácticamente todos los órdenes jurídicos del mundo, la necesidad de contar con razones suficientes y autorización expresa de un juez.

La Constitución argentina, por ejemplo, es especialmente enfática en este sentido: «las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados» (artículo 19) y «El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación» (artículo 18).

El énfasis de la Constitución en este tópico es sugestivo: en casi ningún otro lugar del texto constitucional se utilizan expresiones de la elocuencia de «... están solo reservadas a Dios y exentas de la autoridad de los magistrados».

Pero este énfasis y esta claridad en separar lo público de lo privado se están viendo enrarecidos por una transformación cultural que, como es obvio, no podía ser prevista por nuestros constituyentes.

La aparición de internet y lo que ha dado en llamarse Sociedad de la Información trastocó no solo el funcionamiento mismo de las sociedades, sino los propios conceptos de vida privada y pública, seguridad, intimidad o geografía.

Vivimos en un mundo que no solo está interconectado de un extremo al otro, sino que esa conectividad que trasciende fronteras ya no nos sorprende, ni siquiera nos detenemos a pensar en ella. Cuando enviamos un mensaje por una plataforma, o comentamos una imagen a alguien que está en la habitación contigua o sentado a la mesa con nosotros, no somos conscientes de que ese impulso eléctrico (ese mensaje, ese comentario) viaja a través de la red de redes y, seguramente, en su periplo cruce dos o tres fronteras

nacionales para volver, finalmente, a escasos metros del lugar donde estamos.

Esta circunstancia, en teoría, debería tener profundos impactos si la analizáramos desde las categorías jurídicas tradicionales. Por eso, cuando por alguna razón esta realidad nos interpela, como, por ejemplo, cuando somos víctimas de algún delito informático, advertimos que el derecho, tal como lo conocemos (esto es, el derecho de fuente estatal, nacional, escrito y formalizado por un determinado procedimiento), no puede dar una respuesta acabada a los conflictos de esta nueva sociedad.

De allí que sea preciso no solo establecer nuevas reglas para lidiar o enfrentar esta nueva realidad, sino también preguntarnos cuál debería ser la función del Estado ante ella.

Esta pregunta tiene múltiples aspectos y perspectivas, ya que, como se dijo, la nueva realidad del flujo de información ha constituido una nueva sociedad. Esto quiere decir que deberíamos volver a pensar la función del Estado en todos sus aspectos: educación, salud, bienestar, etc.

Aquí nos centraremos en los aspectos que hacen a la seguridad de los individuos que habitan una nación, y reflexionaremos sobre qué debe y puede hacer el Estado.

1.a. ¿Debe el Estado garantizar la seguridad en el ciberespacio?

El Estado debe asegurar la seguridad de sus ciudadanos. Esta afirmación, que, como se dijo, parece indudable, tiene sin embargo como presupuesto la noción de soberanía: los Estados nacionales resguardan la seguridad individual porque tienen el monopolio del uso de la fuerza en un espacio territorial determinado, y cumplen esa función mediante la aplicación de las leyes emitidas por los órganos específicamente designados para hacerlo.

En consecuencia, soberanía, aplicación de la ley y territorio son tres conceptos que coexisten y se presuponen (Barberis, 2003). Pero es evidente que esta interrelación no se verifica en el ciberespacio; ni el Estado tiene soberanía allí, ni la ley tiene aplicación irrestricta, ni es, obviamente, un territorio delimitado.

La pregunta sobre si el Estado debe garantizar la seguridad en el ciberespacio podría parecer un interrogante de simple respuesta, pero aun así vale la pena reflexionar sobre el tema, porque un análisis sobre la naturaleza misma del ciberespacio puede mostrar aspectos que muchas veces no han sido debidamente tratados desde la perspectiva del derecho.

La primera aproximación a este interrogante se relaciona con la propia idea de la ubicación espacial. Es evidente que el Estado puede y debe garantizar la seguridad en un espacio territorial determinado. El ciberespacio puede ser definido de muchas maneras, pero está lejos de considerarse un espacio físico. Porque si bien desde el punto de vista de su arquitectura es una red de nodos físicos conformados por servidores que se encuentran desperdigados por el mundo, lo esencial es la información que fluye libre entre ellos y no los propios servidores.

Esta información que circula es, en rigor, lo que constituye el ciberespacio (Gleick, 2013). En esta realidad, la potestad de un Estado (de cualquier Estado) para imponer su regulación es bastante endeble y, además, improbable.

Sin embargo, el criterio de la territorialidad se sigue utilizando para determinar el imperio y la jurisdicción del Estado en los asuntos del ciberespacio. Estándares como el lugar de alojamiento de los servidores principales, del asiento de la persona o sociedad que lo administra o dispone de ellos, o algún criterio similar, parecen ser los dominantes en el derecho en la actualidad. Por ejemplo, el Reglamento de Protección de Datos Personales de la Unión Europea (quizás la norma

jurídica más completa en la materia) establece que su ámbito de aplicación corresponde «al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no» (Hoofnagle, 2019).

En consecuencia, si la potestad del Estado para imponer su legislación está íntimamente vinculada con la potestad física sobre lugares físicos, ¿cuál será el criterio para imponerla en el ciberespacio?

La soberanía sobre un territorio tenía la ventaja de que era exclusiva. Esto implicaba, en la perspectiva de los individuos, que existían reglas objetivas, únicas y excluyentes que determinaban cómo debían comportarse en ese espacio. En cambio, en el ciberespacio pueden concurrir muchas legislaciones distintas originadas por todos aquellos países donde la actividad en línea repercute, por lo que el criterio de la soberanía ya no tiene la certeza suficiente para determinar cuál es la ley aplicable y a la que los individuos deben someterse.

El problema principal, tanto para el Estado como para los propios individuos, en este punto, es que la decisión de aplicar una u otra legislación queda supeditada a una multiplicidad de criterios en virtud de los cuales, en definitiva, la decisión final queda en manos de aquel a quien se le aplica la ley. En consecuencia, para someterse a la ley, no pesará sobre el individuo su ubicación territorial o la de su actividad, sino que se valorarán criterios de conveniencia (¿cuál es la legislación más permisiva?), de intereses económicos (¿dónde tengo más presencia *on line*?) o, simplemente, estratégicos (¿cuál es el Estado que puede castigarme si no cumplo su legislación?). En consecuencia, desde la perspectiva del Estado, la situación es crítica: cuando legisla el ciberespacio no tiene la plena potestad de hacer cumplir su ley, sino que el cumplimiento queda a exclusiva disposición de los particulares. Y no hay peor ley que aquella que no se aplica.

Como vemos, esta situación pone en jaque a los Estados, que se ven en la disyuntiva de crear leyes potencialmente inocuas o, simplemente, no legislar.

En segundo lugar, es preciso tener en cuenta que cuando hablamos del ciberespacio, nos estamos refiriendo a «lugares» virtuales que, en definitiva, pertenecen a personas o empresas privadas. Entonces, aquella clara delimitación entre ámbitos privados y ámbitos públicos se diluye en el ciberespacio, y por eso también las fronteras de intervención del Estado.

Consideremos un ejemplo simple: es cierto que una plaza pública y una red social son diferentes en sus realidades materiales, pero a la vez tienen muchas similitudes. Ambas se parecen en que son espacios en donde concurren e interactúan muchas personas, incluso multitudes. Pero cualquier red social (o cualquier otra actividad en línea) es, como se dijo, propiedad de una empresa o persona determinada que tiene una relación contractual con sus usuarios y, por ello, controla el flujo de información y fija políticas internas de admisión y conducta dentro de la plataforma.

Esto nos lleva a una situación paradojal, porque a la vez de ser un espacio público multitudinario, significa una limitación en lo que respecta a la aplicación de la ley por parte de un Estado, porque en un Estado de derecho los espacios privados se rigen por las relaciones bilaterales o contractuales, y no por el imperio de la ley (Suzor, 2013).

Es cierto que la cultura jurídica de origen continental europeo, de la que Argentina es parte, ha sido más permisiva en la aplicación de la ley a las relaciones entre particulares, pero no ocurre lo mismo en la tradición jurídica anglosajona, que en general es reacia a imponer el interés público por sobre la voluntad de las partes (Citron, 2008).

Por otro lado, tampoco es posible sostener un abandono total del ciudadano por parte del Estado, solo porque el desenvolvimiento de

su actividad es en el marco de un contexto entre privados. Más allá de estas legítimas observaciones, las personas asumen y tienen una razonable expectativa de que el Estado las proteja contra agresiones de terceros. Y esta percepción no distingue entre el mundo de lo material y lo virtual.

El florecimiento de la red 4.0 trajo muchos problemas en este sentido (Hauschildt, 2014). Es que, si bien es cierto que las redes sociales son, en definitiva, un producto que ofrece una empresa o grupo empresario (Instagram o WhatsApp por Facebook, por ejemplo), lo que ocurre dentro de la plataforma tiene que ver con dinámicas sociales y no solo con relaciones contractuales bilaterales. Fenómenos como la mal llamada «pornovenganza» o las *fake news* escapan a la lógica contractual y se identifican más bien con un problema de seguridad personal que adquiere ribetes criminales, que precisan, por ello, la intervención estatal. Y las personas asumen que, más allá de lo que se pueda hacer en el contexto de la plataforma (bloquear al usuario, denunciar la cuenta), el Estado debería castigar esas conductas.

Es que la cuestión de la ciberseguridad ha pasado, en los últimos años, de una cuestión más bien vinculada con Estados y grandes corporaciones, a ser una preocupación de todos. Un claro ejemplo es el ataque masivo del *ransomware* WannaCry en el año 2017. Este *software* malicioso, que recorrió las redes, infectó millones de computadoras. Una vez activo, el virus encriptaba la información del disco rígido o de la nube y exigía el pago de un rescate en bitcoins para recuperar la información. Las víctimas de estos cibercriminales que pagaron el rescate de los datos se cuentan por millones de personas, empresas e instituciones, y se especula que las ganancias ilegales fueron siderales. Grandes empresas, pequeños negocios o emprendimientos, profesionales e incluso personas privadas vieron capturada su información, bajo la amenaza de perderla definitivamente si no realizaban el pago.

A partir de estas observaciones, podemos concluir que es necesaria una reconfiguración de la valoración jurídica de los espacios público y privado para conseguir un marco de intervención estatal que asegure ciertos derechos en el ciberespacio. Esta reconfiguración debe tener por objeto la seguridad de los ciudadanos en estos nuevos lugares que plantea el ciberespacio, y que resuelva la tensión entre lo público y lo privado sin abandonar la inviolabilidad de estos derechos, ya que constituyen un aspecto esencial de lo humano.

1.b. ¿Qué seguridad debe garantizar el Estado?

Como se dijo, en los sistemas jurídicos de tradición anglosajona, la pregunta sobre si es aplicable lo que llaman el *rule of law* viene generando una discusión vehemente. Es que, en esa cultura jurídica, la protección de derechos constitucionales es una afirmación del individuo contra el Estado y no contra otros. En cambio, en Argentina, la protección de los derechos constitucionales contra los particulares tiene larga tradición. Ya en el fallo «Kot» (1958), la Corte Suprema de Justicia de la República Argentina afirmó esta posibilidad mediante la aplicación del amparo (un remedio constitucional para la protección de los derechos) contra la acción de otros individuos.

Sin embargo, en la nueva dinámica del ciberespacio, ninguna de las dos opciones parece aplicable en términos absolutos. Resulta impensable que el Estado se desentienda absolutamente de lo que ocurre en las plataformas (que son, al fin y al cabo, propiedad privada) como el extremo opuesto, es decir, que el Estado regule y controle todo lo que ocurre en ellas.

La tensión entre la aplicación del *rule of law* y el *laissez affaire* existe desde los comienzos mismos de internet. Desde la «Declaración de Independencia en el Ciberespacio» (Barlow, 1996) hasta la cambiante política sobre la neutralidad en la red de la Comisión Federal de

Comunicaciones de los Estados Unidos de América (Mardsen, 2012), por citar algunos ejemplos, se ha planteado esta dicotomía. La cuestión gira en torno al interrogante sobre si la legislación es útil para proteger a los individuos en el ciberespacio o si solo sirve para anular la innovación y el desarrollo tecnológico que, en teoría, sería connatural a internet. En un extremo, se afirma que el ciberespacio es por naturaleza anómico y capaz de generar su propia autorregulación, por lo que cualquier injerencia foránea lo pervertiría; y desde el otro, que es un lugar enteramente dominado por grupos económicos que lucran irresponsablemente con nuestros datos personales, por lo que es indispensable que el Estado intervenga para equilibrar esa relación.

Esta tensión abre una serie de interrogantes para legisladores, gobierno y, en general, todos los gestores de políticas públicas. La disyuntiva de qué y cómo regular el ciberespacio tiene directa relación con la postura que se asuma en esta tensión. Una mirada más libertaria buscará evitar toda intervención estatal, con el consecuente peligro de dejar inermes a las personas ante ataques inescrupulosos y, en el extremo opuesto, una visión que desconfíe de todo lo que ocurre en la red intentará someterla enteramente al poder estatal, con el correlativo riesgo de frenar la innovación y el desarrollo. Por supuesto que, entre estas dos posturas extremas sobre la cuestión, existen gradaciones, que van desde la regulación de temas o materias específicas a un Estado que sólo sirva de árbitro en situaciones extremas.

Sin embargo, en lo que hace a políticas de seguridad individual, parece existir algún consenso en que es necesaria alguna intervención estatal, aunque cuán intensa debe ser esa intervención es un tema debatido.

Un ejemplo de ello podemos verlo en la sentencia de «Belén Rodríguez» de la Corte Suprema de Justicia de la Nación (Del Carril, 2019). Si bien el caso no se trataba específicamente de una

cuestión relacionada con la seguridad o el ejercicio de la ley penal, la Corte Suprema dejó asentadas en su argumentación algunas ideas relacionadas.

Belén Rodríguez es una modelo que demandó a los buscadores en internet (Google, etc.) porque su nombre estaba indexado en relación con sitios de pornografía. Su intención era responsabilizar a los buscadores por esta relación que afectaba su honor y, además, obligarlos a retirar su nombre de los resultados de búsquedas vinculados con esos sitios. La Corte consideró que, si bien no podía atribuirse a los buscadores responsabilidad alguna por este hecho, debían retirar la indexación en cuestión cuando mediaba una notificación fehaciente. En la relación de los argumentos de la Corte Suprema, queda claro que, en el futuro, los buscadores debían actuar de esta manera una vez notificados por quien se consideraba afectado. Pero más allá de este hecho, la Corte Suprema también advirtió que, en ciertas ocasiones, esta notificación del damnificado era innecesaria porque el contenido mismo es de suyo ilegal. En estos supuestos, afirma, los buscadores debían actuar espontáneamente, bajo pena de incurrir en responsabilidad por los daños que pudieran ocasionar.

La Corte Suprema no sostuvo ni insinuó alguna responsabilidad penal de los buscadores en el caso de que omitieran retirar este material (o, en rigor, la indexación a este material), pero la cuestión queda abierta. Es que un posible análisis desde la mirada del derecho penal podría concluir que alguien que conoce la existencia de un contenido ilícito en su ámbito de disposición y no hace nada al respecto podría considerarse un partícipe, o al menos un encubridor, de la conducta ilícita.

Por otro lado, la Corte tampoco precisó con toda la exactitud que sería deseable, cuáles son estos contenidos evidentemente ilegítimos. En este punto, la postura de los jueces de la Corte se divide, mientras que el voto mayoritario considera que estos contenidos están

conformados por: 1) la pornografía infantil; 2) los datos que faciliten la comisión de delitos o que instruyan acerca de estos; 3) los que pongan en peligro la vida o la integridad física de las personas; 4) los que hagan apología del genocidio, del racismo o de otra discriminación con manifiesta perversidad o incitación a la violencia; 5) los que desbaraten o adviertan acerca de investigaciones judiciales en curso y que deban quedar secretas; 6) los que importen lesiones contumeliosas al honor; 7) los montajes de imágenes notoriamente falsos; y 8) los que importen violaciones graves a la privacidad exhibiendo imágenes de actos que por su naturaleza deben ser incuestionablemente privados, aunque no sean necesariamente de contenido sexual; por su parte, los ministros Lorenzetti y Maqueda opinan que son aquellos en los que «... el contenido de la publicación sea expresamente prohibido o resulte una palmaria ilicitud», como, por ejemplo, «la incitación directa y pública al genocidio y la pornografía infantil».

Como se ve, el tema de la atribución de responsabilidad en el ciberespacio tiene múltiples aristas y actores. Y la regulación de este espacio debe diferenciar los distintos niveles de responsabilidad. No es lo mismo el accionar de quienes lo utilizan para atentar contra la seguridad de las personas que las responsabilidades que les caben a los gestores o «dueños» del ciberespacio. Una regulación estatal debe repensar esta relación en términos distintos a los cauces tradicionales; parafraseando a la Corte en el fallo citado, responsabilizar a los intermediarios de internet por los hechos cometidos en sus plataformas es como imputar al Estado por un delito cometido en la vía pública.

En términos de eficiencia de las políticas de seguridad que un Estado puede planificar, esto es fundamental. Según cual fuere la decisión que cada gobierno tome, serán distintos sus métodos y posibilidades.

Si la decisión es tomar a los propietarios de las plataformas como simples privados que deben acatar la ley aplicable en un territorio, el

resultado es una legislación intervencionista; en cambio, si la decisión es que las plataformas no son en absoluto responsables, sino que sólo son las gestoras de un «espacio» donde ocurren situaciones (lícitas o ilícitas), se optará por una legislación más pasiva.

En conclusión, 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. Y que esta regulación debe considerar las plataformas, en algunos aspectos, como espacios abiertos o públicos y, en otros, como relaciones contractuales bilaterales.

Pero esto nos lleva al siguiente interrogante: si el Estado tiene cierta capacidad de injerencia en el ciberespacio, ¿qué puede hacer por sí un orden jurídico nacional para proteger a sus ciudadanos?

1.c. ¿Qué puede hacer el Estado para proteger la seguridad en el ciberespacio?

El problema de los medios y las posibilidades que tiene un Estado para garantizar la seguridad individual en el ciberespacio plantea también cuestiones absolutamente novedosas para el derecho.

Este nuevo espacio, que es –si vale la metáfora– transnacional e inmaterial, se resiste por su misma arquitectura y constitución a la ejecución de políticas de seguridad pública.

Una comparación con la ejecución tradicional de estas políticas en los espacios físicos puede servirnos para poner de relieve lo complejo de esta situación.

Como se dijo, desde el surgimiento del Estado de derecho y de la mano del constitucionalismo decimonónico, los espacios geográficos en que se dividía una nación respondían a una delimitación clara

y precisa fácilmente discernible. Por un lado, los espacios públicos en donde el tránsito y la concurrencia de las personas es permitida e indiscriminada; en ellos, el Estado podía ejercer la fuerza pública legítimamente porque era el garante de la seguridad de las personas que allí se encontraban. Por el otro, el espacio privado, identificado paradigmáticamente con el domicilio (y extendido a las comunicaciones privadas). En él, el Estado no tenía injerencia, salvo autorización expresa de los jueces fundada en ley; es decir, mediante la intervención y autorización de un funcionario estatal que tenía garantizada su imparcialidad e independencia y por un acto del Poder Legislativo que, en la lógica de aquel constitucionalismo, representaba la voluntad del pueblo.

En el medio de estos dos espacios aparecían, en ocasiones, zonas grises o áreas indeterminadas, en las cuales la acción estatal estaba permitida en mayor o menor medida según criterios variantes, generalmente delimitados por la jurisprudencia o, en menor medida, por la legislación.

Para ser más claro: si es indudable que un parque es un lugar público y el hogar uno privado, por ejemplo, un local comercial, un hotel o un cine comparten caracteres comunes con ambos, ya que pertenecen a un individuo que se reserva la potestad de admitir el ingreso o la permanencia en él, pero, en principio, no lo hace. En estos espacios intermedios, la acción del Estado no es ilimitada, sino que se funda y justifica en razones de interés público. En el derecho continental, la justificación de estas razones dio lugar al llamado «poder de policía», que en un primer momento estaba circunscripto a razones de moralidad, salud y seguridad pública y con el transcurso del tiempo fue ampliándose a otros supuestos (Legarre, 2004). Tanto en los supuestos de espacios públicos como en los espacios semiprivados sujetos al poder de policía, el Estado tenía asegurada su intervención directa, bajo determinadas condiciones.

Ahora bien, ese «lugar» que llamamos ciberespacio es de naturaleza híbrida. Si bien comparte bastantes características con los espacios semiprivados en su condición objetiva (los dueños tienen derecho de admisión y permanencia, pero en principio su acceso es indiscriminado), lo cierto es que la actuación de los individuos en él difiere mucho de aquellos y parece pertenecer al ámbito de lo privado, en su sentido más íntimo y exclusivo, por el contenido de lo que se publica y el uso que se le da.

Pensemos, por ejemplo, en una red social cualquiera. Es evidente que la plataforma pertenece a un particular (una persona, una empresa) y que el acceso a ella es indiscriminado, aunque el «dueño» se reserva la posibilidad de excluir a quien incumpla ciertas obligaciones. Estas obligaciones están, generalmente, objetivadas en los «términos y condiciones» que debemos aceptar al crear un perfil en la red social. Hasta aquí las similitudes.

Pero las diferencias también son considerables. En primer lugar, la interacción de los individuos en la red suele (aunque esto dependerá de la naturaleza de la plataforma) parecerse más a las conductas que se asumen en el resguardo de los espacios privados. Es común, en estas plataformas, tener conversaciones sobre temas íntimos o mostrarse como lo haríamos frente a personas de nuestro círculo estrecho de confianza. Desde el punto de vista subjetivo, las personas piensan en estos espacios como lugares protegidos, resguardados de miradas ajenas (aunque la definición de quién es «ajeno» también se ha vuelto bastante elástica).

En estas condiciones, la ambigüedad del espacio proyecta esta misma ambigüedad en la determinación de las posibilidades del Estado de ingresar en ellos. Es evidente que no es posible aplicar las categorías del «poder de policía» a las que se hizo referencia (razones de moralidad, salud y seguridad pública habilitan la intervención de

por sí), ni tampoco es posible sostener la exclusión absoluta de la autoridad, aun ante la evidencia de un peligro público (en un amplísimo sentido del término).

Si la Constitución argentina es tan clara y enfática al afirmar que «las acciones privadas de los hombres están solo reservadas a Dios y exentas de la autoridad de los magistrados», no parece hoy tan evidente cuáles serían estas acciones merecedoras de tamaña protección.

2. Nueva seguridad, nuevos actores

A esta cuestión, más jurídica si se quiere, se le suma otro problema de índole más práctica. Otra vez, si comparamos con los espacios físicos materiales, podemos dimensionar la cuestión. Veamos.

Si el Estado, en el ejercicio legítimo del poder de policía o con expresa autorización de un juez, decidía ingresar en los ambientes semiprivados o privados, lo hacía. En esas condiciones de legitimidad a las que nos acabamos de referir, el uso de la fuerza pública, es decir, el monopolio estatal de ejercer fuerza sobre cosas y personas, le permitía, sin más, ingresar en estos espacios. Una inspección a un local comercial con fines de seguridad e higiene o un allanamiento a una morada en una investigación criminal son claros ejemplos de ello. En estos casos, el Estado ingresa al lugar, aun contra la voluntad del titular, y obtiene, con la fuerza o sin ella, la información o los objetos que vino a buscar.

Pero esto no funciona de igual manera en el ciberespacio. Para «ingresar» a una red social y obtener de ella información no es suficiente con la sola voluntad y ejercicio legítimo de una acción por parte del Estado. Se precisa, al menos, de la anuencia del dueño de ese ciberespacio. El gestor y cuidador de la información y los «objetos» (si vale este vocablo en el mundo digital) es el que puede permitir el

acceso o denegarlo; y si, además, se quiere obtener información que no se encuentra a la vista de todos, su colaboración activa resulta esencial.

Supongamos una situación en la que se investiga un delito de tráfico de imágenes de abuso sexual infantil en alguna red social. Para llevar a cabo una investigación eficiente y con posibilidades de éxito, los funcionarios del gobierno deberían, en primer lugar, generar un perfil en la red social. Y este es el primer escollo: si los investigadores quieren tener éxito en su investigación necesitan generar, obviamente, un perfil falso. Les quedan, entonces, dos opciones: o mentir sus datos (y, en consecuencia, violar los términos y condiciones de la red) y tomar el riesgo de que el administrador de la plataforma los excluya en el caso de que sean detectados, o avisar a la plataforma que precisan un perfil específico para la investigación y, en ese caso, quedan a disposición de la voluntad del administrador. Pero en la gran mayoría de las investigaciones, este accionar es muy poco útil. La verdadera información que deberían obtener no está a la vista de los usuarios de la red social. Porque lo esencial es recopilar direcciones IP, logueos, correos electrónicos vinculados, información sobre tarjetas de crédito, vínculos estrechos de esa persona en la red social, conversaciones mantenidas en canales bilaterales o grupales privados; y esto es sólo una mención rápida de la información que puede obtenerse. Pero, en este supuesto también, para hacerse de ella necesita de la colaboración activa del dueño de la plataforma.

En el ámbito de la investigación criminal (en rigor, también en el ámbito de la práctica del derecho en general) ha surgido este nuevo actor no institucional, sin cuya colaboración no es posible ni siquiera pensar en la seguridad personal en el ciberespacio.

Los propietarios de las plataformas, redes sociales y páginas web resguardan y administran cantidades inconmensurables de

información personal que ni siquiera el Estado más intervencionista puede soñar con obtener.

Y si bien es cierto que, al menos en lo que hace a la investigación criminal y la prevención de delitos graves, estos nuevos actores colaboran de buen grado con aquellos países en lo que se vive en un Estado de derecho, es común que establezcan reglas o estándares para entregar la información que los jueces e investigadores les requieren.

Estos requisitos están conformados por condiciones jurídicas y reglamentarias heterogéneas. En primer lugar, por los términos y condiciones establecidos unilateralmente por las plataformas; en segundo lugar, por límites al acceso a la información originadas únicamente en estrategias de marketing enfocadas a la protección de la privacidad. Apple, por ejemplo, es una corporación que hace de la confidencialidad de la información de sus usuarios una política ostensible y publicitada, hasta el punto de haberse negado a permitir el acceso de las fuerzas de seguridad norteamericanas a la información de un terrorista que había cometido un atentado en el famoso caso del «IPhone de San Bernardino» (Rozenshtein, 2018).

Por último, las compañías fuerzan a los Estados a cumplir con condiciones y leyes extranjeras. Es común que una empresa de tecnología, para entregar información a un juez, le imponga los estándares del Reglamento Europeo de Protección de Datos de personas, la Privacy Act de los Estados Unidos de América o cualquier otra regulación. La decisión de aplicar una ley u otra no se funda en razones de soberanía o criterios jurídicos como los del derecho internacional privado, sino en que son las leyes que la empresa considera que debe cumplir, ya sea por la ubicación de la casa central de sus negocios, porque es la ley de su clientela más significativa o por cualquier otra razón utilitaria o estratégica. Es más, la imposición de esta ley extranjera viene mediada por la interpretación que hacen de ella los servicios legales de

la empresa, por lo que ocurre con frecuencia que las exigencias para entregar la información a los Estados difieren de empresa a empresa, aun cuando aleguen el cumplimiento de la misma ley.

En consecuencia, en el ciberespacio, al Estado no solo le resulta imposible aplicar coactivamente sus leyes, sino que en muchos casos debe someterse a una ley extranjera según cómo es interpretada por una empresa o por sus abogados.

El panorama, como se ve, es, al menos, pintoresco. La irrupción de los administradores del ciberespacio en la lógica de la seguridad individual viene generando una indeterminación absoluta en materia de validez y vigencia de las leyes (Kelsen, 1982).

Conclusión

Ante esta situación, los gobiernos, y en especial aquellos operadores del derecho que están encargados de la producción normativa de los Estados, pueden reaccionar de dos maneras. Una primera reacción, más instintiva si se quiere, es la de intentar reafirmar la soberanía de la ley nacional con los parámetros de una cuestión territorial.

En este intento, se podría intentar imponer legislativamente obligaciones de diversa índole y reforzarlas con amenazas de sanciones. Esta opción, posible por cierto, tiene el inconveniente de que solo será viable en tanto los sujetos obligados, los prestadores de servicios en internet, consideren que les resulta conveniente acatarlas (como se vio, por razones comerciales, estratégicas, de publicidad, etc.). Pero si no lo consideran así, no lo harán. En este caso, en el supuesto más extremo, el servicio que ofrezcan dejará de tener presencia en el país. Pero si es un producto realmente popular en el ciberespacio, será igualmente utilizado, porque los cibernautas encontrarán la manera de sortear las barreras legales o tecnológicas que se quieran imponer.

En conclusión, la seguridad en el ciberespacio es posible, y el Estado debe proveerla. Pero tanto la legislación como la actividad estatal deben tener en cuenta que, en el contexto actual, la creencia de que por la sola circunstancia de dictar una ley esta será inmediatamente aplicable no es más que una quimera.

Este nuevo horizonte en la aplicación del derecho obliga a los gestores de las políticas de seguridad pública a idear soluciones novedosas y, en especial, asentadas en la realidad de las cosas. La asistencia internacional y la cooperación entre los sectores público y privado son condiciones ineludibles para una legislación y una acción estatal efectiva y realista.

Porque legislar en materia de seguridad bajo los paradigmas de la aplicación territorial de la ley puede tener el mismo efecto que no legislar. Y la seguridad en el ciberespacio es un eje fundamental de la vigencia de los derechos en la sociedad contemporánea; para «no dejar a nadie atrás» (UN, 2019).

Referencias bibliográficas

Barberis, J. A. (2003). *El territorio del Estado y la soberanía territorial.* Buenos Aires: Ábaco.

Barlow, P. (1996, febrero 8). *Declaración de la Independencia en el ciberespacio.* Retrieved from Wikisource: https://es.wikisource.org/wiki/Declaracion_de_independencia_del_ciberespacio.

Bernal, A. É. (2017). «Ciberespacio, ciberderecho y ciberabogados». *La Ley España*.

Citron, D. K. (2008). «Technological due process». *85 Wash. U. L. Rev. 1249*, 1249-1313.

Del Carril, E. H. (2019). «Belén Rodríguez revisitado». *Revista de responsabilidad Civil y Seguros*.

Gleick, J. (2013). *La información. Historia y realidad.* Madrid: Crítica.

Hauschildt, V. M. (2014). «Las redes sociales y su incidencia». *Aequitas Vol. 8, nº 8*, 140-158.

Hoofnagle, B. v. (2019). «The European Union General Data Protection Regulation: What it is and what it means». *Journal of Information & Communications Technology Law*, 65-98.

Kelsen, H. (1982). *Teoría pura del derecho.* (R. J. Vernengo, Trans.) México: Universidad Autónoma de México.

Legarre, S. (2004). *Poder de policía y moralidad pública. Fundamentos y aplicaciones.* Buenos Aires: Ábaco.

Mafla, E. (2011). *Seguridad ciudadana en el ciberespacio*. Recuperado 6 18, 2020, de https://repositorio.flacsoandes.edu.ec/handle/10469/6502.

Mardsen, C. T. (2012). «Neutralidad en la red: historia, regulación y futuro». *Revista de Internet, Derecho y Política*, 24-43.

Menéndez, I. V. (2007). «Ciberconstitucionalismo. Las TIC y los espacios virtuales de los derechos fundamentales». *Revista Catalana de Dret Públic* (35), 19-42.

Roze Suzor, N. (2013). «The role of rule of law in virtual communities». *Berkeley Technology Law Journal vol. 25*, 1817.

Rozenshtein, A. Z. (2018). «Surveillance Intermediaries». *Stanford Law Review*, 99-189.

UN High-Level Panel on Digital Cooperation. (2019). *The Age of Digital Interdependence.*

ENRIQUE H. DEL CARRIL. Abogado (UCA) y Mag. en Derecho Judicial (Austral) con tesis sobresaliente y mejor promedio. Especialista en Ética y Derecho Constitucional y nuevas tecnologías. Profesor en universidades de la Argentina y del extranjero. Dictó capacitaciones en poderes judiciales de la Argentina, El Salvador, Colombia y Costa Rica, entre otros. Integra el Comité de los Cuadernos de Derecho Judicial de Ed. La Ley y ha publicado libros y artículos en revistas nacionales y extranjeras. Premio La Ley al Fortalecimiento del Poder Judicial (2005) y reconocimiento del National Center for Missing & Exploited Children por sus aportes contra la pornografía infantil en internet (2015). Miembro Titular de la Asociación Argentina de Derecho Constitucional y del Centro de Estudios Jurídicos Notariales, Miembro Honorario del Comité de la Escuela de Formación de la Corte Superior del Callao, Perú. Director del Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal de la Ciudad de Buenos Aires.

CAPÍTULO 3

La soberanía en un mundo convergente. Apuntes para entender los dilemas para la seguridad y defensa

Sol Gastaldi

Introducción

Desde su creación, el Estado ha tenido como tarea indelegable garantizar la seguridad y defensa de su territorio y sus habitantes. El ejercicio de la soberanía se manifiesta de forma más cabal a través de la capacidad de garantizar dicha seguridad. Sin embargo, la soberanía no es un atributo absoluto, sino que su ejercicio está sujeto a la incidencia de diferentes variables de la política doméstica y del sistema internacional, como la capacidad de controlar sus fronteras o la posición del país en ese orden internacional.

Con el devenir de la globalización, la capacidad soberana de los Estados fue puesta en debate. Crecientes interacciones a nivel global entre los Estados, entre los mercados y entre las personas hicieron pensar a muchos que estaba pereciendo el sistema de los Estados-nación, y el estudio de la categoría de la soberanía estatal y su ejercicio

se volvió recurrente para la ciencia política. Paralelamente, se perfilaron cambios en los riesgos y «nuevas amenazas» moldearon el escenario de la seguridad internacional.

Ante el constante avance de las tecnologías de la información y las comunicaciones, en este siglo XXI, vuelven a replantearse viejos debates. La soberanía, frente a la dinámica del denominado «ciberespacio», se expone a otros desafíos, a la par de una revolución en casi todos los campos de la actividad humana donde esa tecnología poco a poco ingresa. Los países se vuelven «ciberdependientes», y esa misma ciberdependencia los torna vulnerables a las nuevas amenazas del espectro cibernético, aquel ámbito creado por el hombre, de naturaleza dual –real y virtual–, mediante el cual pueden desarrollarse acciones que impactan de distinta manera sobre la seguridad y defensa de los Estados.

Algunos países, como Estados Unidos, empezaron a preocuparse por la ocurrencia de un «ciber Pearl Harbor» (Stiennon, 2017); otros fueron víctimas de ciberataques sin saberlo inicialmente, como en el caso de Irán, que vio afectadas sus centrifugadoras de enriquecimiento de uranio de la planta de Bushehr por la acción del gusano Stuxnet en 2010; y en otros casos, el ataque masivo de sitios web y sistemas gubernamentales dio lugar a que varios países europeos iniciaran de manera sostenida una política de ciberdefensa comunitaria, como en el caso de los miembros de la OTAN, luego de los atentados cibernéticos contra Estonia en el año 2007. Muchos se apresuraron a señalar que el mundo había entrado en una ciberguerra.

Casi simultáneamente, se produjo la mayor filtración de documentos secretos de la historia en los Estados Unidos a través de Wikileaks, y Edward Snowden reveló unos años después que el «Tío Sam» todo lo escuchaba, a través del desarrollo y empleo de programas informáticos de vigilancia masiva sobre los ciudadanos. Posteriormente, un *exploit,* justamente creado por la Agencia Nacional de Seguridad de los

Estados Unidos (NSA), fue robado y empleado en el secuestro de ordenadores más grande de la historia, a través del *ransomware* WannaCry. Y mientras todo esto sucedía, el ISIS creaba su Cibercalifato Unido.

Frente a esta compleja realidad, los Estados se encuentran ante la necesidad de responder a dinámicas novedosas como los delitos cibernéticos, el hacktivismo, el ciberterrorismo y la ciberguerra.

El presente capítulo aborda de manera teórica y empírica aspectos clave de la actual situación estratégica que impactan sobre la capacidad de los Estados de garantizar la seguridad y la defensa del territorio y su población, frente al vertiginoso avance de una agenda de seguridad marcada por los desafíos del ciberespacio. Esto no significa que hayan desaparecido problemáticas tradicionales, pero en un mundo hiperconectado y convergente, se visualizan asuntos que demandan no sólo políticas públicas urgentes, sino una alta cuota de imaginación, pues este escenario estratégico, marcado por el creciente predominio del mundo digital sobre el mundo físico, aún no ha terminado de perfilarse.

Teniendo en cuenta estos aspectos, se indagará cómo, a través de los cambios tecnológicos del ámbito cibernético, se introducen nuevas amenazas para la seguridad y defensa de los Estados y el ejercicio de la soberanía. Para ello, en primer lugar, se repasará la función del Estado nacional como garante de la soberanía y la integridad territorial, considerando la soberanía como un concepto dinámico, sujeto a cambios políticos y económicos del sistema internacional.

En segundo lugar, a partir de la evolución de las tecnologías de la información y de las comunicaciones y el denominado ciberespacio, se analizará si esta evolución conlleva un cambio en la manera de administrar la soberanía por parte de los Estados, para lo cual se planteará una idea novedosa, consistente en que estamos pasando del paradigma de la globalización al paradigma de la convergencia.

Como veremos, la territorialidad excluyente asociada al concepto de soberanía es el principal escollo que esta encuentra en la nueva fase digital.

Por último, y a efectos de observar los impactos de estos cambios sobre la seguridad y la defensa nacional de los Estados, se analizarán los desafíos que el debate actual pondera como los principales dilemas del ámbito cibernético, que son el hacktivismo, el ciberterrorismo y la ciberguerra.

1. La soberanía como un concepto dinámico

El politólogo argentino Guillermo O'Donnell (1978; 2010) es, para todo análisis sobre el Estado y sus funciones, un referente teórico indiscutido. Inmerso en la tradición weberiana de pensamiento, destacó al Estado como una entidad política de dominación conformada por cuatro dimensiones: una legal, una burocrática, otra dimensión representada por una identidad colectiva y, por último, un filtro que regula fronteras, de territorio, mercado y población, tal como apunta Martín D'Alessandro (2011). En este sentido, y a los fines de este capítulo, cobra especial interés analizar esta última dimensión, relacionada con el rol de control y administrador que posee el Estado sobre sus fronteras y de lo que estas contienen, con el propósito de resguardar el bienestar de la población. Esta dimensión relacionada con el control y administración se ha ejercido de diferentes maneras a lo largo de la historia, a través de la evolución del Estado, de las condiciones materiales de producción, de las sociedades y, también, del factor tecnológico.

Cuando nos referimos a control y administración nos referimos, indudablemente, a la noción de soberanía estatal, a la capacidad del Estado en términos jurídicos y políticos de ejercer su autoridad dentro de sus fronteras.

El concepto de soberanía nos remonta al año 1648, cuando se firma la Paz de Westfalia, se pone fin al sistema medieval y se establece un orden internacional donde cada Estado que lo compone es la fuente absoluta de poder en su territorio; es la autoridad suprema. Tal autoridad no vino exenta de responsabilidades, como garantizar la seguridad de los súbditos (hoy ciudadanos), no sólo en el plano interno, proveyendo seguridad interior, sino, a la vez, frente a las otras unidades políticas de ese sistema internacional, garantizando la defensa nacional ante la siempre presente probabilidad de guerra interestatal. La obligación de garantizar la seguridad hacia el interior del Estado y frente a otros Estados ha sido siempre una tarea indelegable de este, y atributo indispensable de su estatidad (Oszlak, 1990), expresada en el monopolio de la violencia física legítima.

A fin de ir aclarando el concepto de soberanía, en primer lugar debe hacerse referencia a la asociación que posee este término con la idea de autoridad. Tal como lo ha señalado David Held (1997:129), el término hace referencia a la «autoridad política de una comunidad que tiene el derecho reconocido de ejercer los poderes del Estado y determinar reglas, regulaciones y medidas dentro de un territorio determinado». Esta conceptualización recoge uno de los elementos definitorios, que es el principio del reconocimiento de la autoridad del Estado por parte de la comunidad internacional de Estados (Oszlak, 1982; Krasner, 2001; Zacher, 1992).

En segundo lugar, podemos mencionar como otro elemento de la soberanía la territorialidad excluyente (Sassen, 1996), lo que equivale a decir que el Estado y sólo él es el único actor que posee el monopolio de la violencia física legítima dentro de los límites territoriales del propio Estado (Oszlak, 1982; Weber, 2002). En este marco, los gobiernos fluyen de la absoluta soberanía del Estado sobre su territorio nacional (Sassen, 1996). Sin embargo, tal como apunta Sassen (1996), desde

hace mucho tiempo han aparecido diversos desafíos relacionados con la territorialidad excluyente de los Estados.

El auge de la globalización en el siglo XX vino, en cierta medida, a poner en debate la capacidad del Estado de ejercer su soberanía. Así, vimos cómo el vertiginoso crecimiento de organizaciones supranacionales, regímenes internacionales, el desarrollo de la economía mundial y los servicios financieros transnacionales cuestionaron justamente los dos componentes clave de la soberanía estatal: la autoridad y la territorialidad excluyente. Seguramente se recordará cómo estos procesos fueron vistos como la declinación del Estado-nación. Sin embargo, dieron lugar a nuevas fórmulas soberanas de ejercicio del control y de la autoridad de los Estados en el nivel supranacional. En otras palabras, los Estados no dejaron de ser los operadores de esta nueva globalización, pese al surgimiento de otros actores con capacidad de proyectar intereses en la arena internacional, como organizaciones no gubernamentales.

Como sostiene Sassen (1996:45), como consecuencia de la globalización, la soberanía y el territorio se han visto reconstituidos y en parte desplazados hacia otros ámbitos institucionales fuera del Estado y fuera de la estructura del territorio nacional; en otras palabras, la autora se refiere a la descentralización de la soberanía y la desnacionalización parcial del territorio, para concluir que la globalización ha representado una trasformación en la articulación de soberanía y territorio.

La cuestión territorial cobra gran relevancia para nuestro análisis, pues en el marco de la globalización, ejercer el control de los «flujos» –de personas, información, transacciones económicas– que atraviesan las fronteras del territorio es una tarea que se ha tornado más compleja que en el pasado, e impacta, indiscutidamente, sobre la soberanía de los Estados. Sobre este punto, resulta interesante recordar el aporte de otro conocido autor, Stephen Krasner (2001), quien especifica las

dimensiones del concepto de soberanía, teniendo en cuenta el contexto global. El autor identifica, entonces, cuatro tipos de soberanía:

- Soberanía internacional legal, consistente en el reconocimiento internacional del Estado como entidad territorial con independencia jurídica formal.
- Soberanía westfaliana, que excluye a los actores externos de las estructuras domésticas de autoridad de un Estado, remitiendo a la libertad de un Estado de elegir las instituciones y políticas que considere más óptimas.
- Soberanía doméstica, que representa la organización interna de la autoridad política y la capacidad de las autoridades de ejercer un control efectivo dentro de sus fronteras.
- Soberanía de interdependencia, consistente en la capacidad de un Estado de controlar y regular los flujos de información, ideas, personas y capitales a través de sus fronteras.

Es interesante –y útil– la diferenciación que hace el autor, ya que, tal como señala, un Estado puede gozar de soberanía westafaliana y, sin embargo, tener una débil soberanía de interdependencia (Krasner, 2001). O sea, es posible que las distintas dimensiones de la soberanía no se manifiesten simultáneamente. Mientras la mayoría de los Estados gozan de un reconocimiento internacional como tales –soberanía internacional legal–, no todos los Estados pueden considerar que poseen soberanía westfaliana. Tal sería el caso de los denominados Estados fallidos[1].

---

1 Si bien se trata de un concepto de uso polémico, tomaremos la definición de Estado fallido de la Fundación por la Paz (Fund for Peace, 2011), cuando hace referencia a gobiernos que enfrentan una pérdida de control sobre el territorio o del monopolio del uso legítimo de la fuerza. Este organismo señala, además, que los Estados fallidos son incapaces de proveer servicios públicos o de interactuar

Teniendo en cuenta las dimensiones observadas por el autor, podemos ver también que la soberanía es un concepto que engloba no sólo aspectos jurídicos, sino también políticos. David Held (1997:130) sostiene al respecto que dentro de la soberanía que posee un Estado debe reconocerse el poder real con que cuenta para articular y llevar a cabo sus metas políticas de forma independiente, es decir, sin condicionamientos externos o sin colaboración internacional, lo cual describe como «soberanía práctica». Los aspectos políticos del concepto tornan necesario considerar que en ese sentido, la soberanía se asocia a la noción de autonomía, requiriendo a fines analíticos tener en cuenta la diferenciación hecha en cuanto a los aspectos políticos y jurídicos del término «soberanía».

A fines de los años setenta del siglo pasado, cuando empezaban a debatirse los efectos de la globalización como proceso emergente, Bull (1977) advertía sobre la viabilidad y utilidad del concepto de soberanía. Las evidencias que observaba en la política mundial, que anunciaban un cambio de tendencias, eran: el proceso de integración que se estaba iniciando en la Unión Europea; la desintegración de algunos Estados en referencia a procesos secesionistas y de autonomía política que se desarrollaban en Gran Bretaña, Canadá, España, Francia y Yugoslavia; la utilización del monopolio de la fuerza por organismos que no son propiamente Estados, como la Organización de las Naciones Unidas a través de las misiones de paz, o por organizaciones terroristas o guerrillas; la existencia de organizaciones no gubernamentales, empresas multinacionales y organismos

---

con otros Estados como miembros plenos de la comunidad internacional, es decir, pierden la capacidad para desempeñar funciones básicas de desarrollo o seguridad. Para un buen resumen sobre los usos y debates en torno a este tema, se sugiere ver Santos Villareal (2009).

internacionales; y la unificación tecnológica del mundo en una «aldea global», como describió McLuhan, debido al crecimiento de las comunicaciones.

A nivel de la seguridad internacional, la globalización fue acompañada de una ampliación en dicha agenda, impulsada a la vez por la finalización de la Guerra Fría, que condujo al estudio de las denominadas «nuevas amenazas», como el terrorismo, el crimen organizado transnacional, el tráfico de personas y de armas, entre otras, que, si bien no eran nuevas, traían como novedad los cambios en el marco institucional en que estas se desarrollaban, a menudo amparadas por Estados débiles, fallidos o privados de soberanía práctica, y la modalidad en las que estas se movían, traspasando fronteras, actuando en red y con una escasa predictibilidad (Bartolomé, 2018).

Estos aportes de reconocidos autores muestran que la cuestión de la soberanía ha sido un tema de estudio y análisis muy presente en la literatura, y ha sido visto como un concepto dinámico, sujeto a variables externas y domésticas. Es innegable que diversos sucesos alteran la soberanía de los Estados, y dentro de todos ellos, la globalización ha sido, por lejos, uno de los fenómenos que más ha impactado.

La globalización, su expansión y profundización en la actual fase digital, o revolución industrial 4.0, sigue configurando y reconfigurando la vida económica, social y política de las sociedades, aunque sus impactos sean diferentes en cada Estado particular, ya que se trata de un fenómeno asimétrico, que crea nuevos problemas, desafíos y vulnerabilidades para los Estados. En otras palabras, aparecen nuevos actores y nuevas reglas de juego que ponen en jaque a los Estados y la capacidad de los gobiernos de ejercer la soberanía estatal.

2. Del paradigma de la globalización al paradigma de la convergencia

En los últimos treinta años, hemos asistido a importantes cambios tecnológicos, que han impactado sobremanera la vida social, el quehacer político, el comercio internacional, la comunicación e incluso la seguridad y defensa nacional. Internet ha sido, seguramente, el invento paradigmático dentro de la llamada revolución de la información y de las comunicaciones.

Como es sabido, el origen de internet se remonta a la Guerra Fría: nunca se ha podido escindir la evolución científico-tecnológica de las necesidades de seguridad y defensa del hombre. En medio de la carrera armamentista con la exURSS, Estados Unidos diseñó a partir de 1967 una red de computadoras que conectaba centros de investigación y bases militares de ese país con el fin de que si uno de los nodos quedaba deshabilitado por un ataque nuclear, toda la red pudiera seguir funcionando de manera descentralizada, intercambiando información estratégica. Este ensayo de lo que se conocería décadas más tarde como «internet» fue así un proyecto militar de la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA, por sus siglas en inglés), denominado ARPANET, por lo que el origen de internet estuvo indefectiblemente asociado a la guerra.

Desde 1991, con la creación del protocolo www y la autorización en los Estados Unidos de la inversión privada con fines comerciales de este desarrollo, internet fue creciendo exponencialmente, lo que dio lugar al pasaje de la Sociedad Industrial a la Sociedad de la Información. Como bien señala el sociólogo español Manuel Castells (2007), internet posibilitó una nueva forma descentralizada de gestionar la información: la sociedad en red.

La globalización, inicialmente confinada a los procesos económicos mundiales, principalmente aquellos vinculados con los mercados

financieros, ha encontrado, a través de internet y el denominado ciberespacio, un vehículo para expandirse a la esfera societaria y desarrollar verdaderas comunidades globales a través de redes sociales, que escapan a la acción de cualquier Estado-nación. Estas comunidades globales trascienden las nacionalidades, las fronteras, la autoridad y la soberanía territorial de los Estados y se encuentran alojadas en el denominado ciberespacio. El auge de las redes sociales a partir del año 2009, cuando estas superaron el número de usuarios de casillas de correo electrónico, ha profundizado notablemente esta tendencia.

No es tarea sencilla hallar una definición homogénea de globalización. Hace tantos años que estamos insertos dentro de este paradigma, que parece una tautología decir que la globalización refiere a un proceso de expansión e interconexión de vínculos económicos, sociales y políticos a nivel transnacional que genera una fuerte interdependencia entre las sociedades y países del mundo. García Delgado (2000) argumenta que este proceso se caracteriza no sólo por esta creciente interdependencia, sino, además, por el pasaje del sistema de producción fordista al postfordista y por el predominio del sector financiero. Keohane y Nye (2000) consideran que el concepto de globalización ha sido pobremente entendido. Para comprender esta categoría, los autores comienzan definiendo globalismo, que observan como un estado del mundo que incluye redes de interdependencia a distancia multicontinentales, cuyas conexiones ocurren a través de flujos de capital y bienes, información e ideas, y personas y fuerzas. A diferencia de otros autores, que consideran el globalismo sólo en términos económicos (Beck, 1998; Pousadela, 2001), para Keohane y Nye el globalismo constituye un fenómeno multidimensional: además de económico, es militar, ambiental, social y cultural. La globalización, para estos autores, es el proceso mediante el cual se da el aumento del globalismo, es decir, de las redes de interdependencia.

Al igual que con el concepto de globalización, tampoco es tarea sencilla encontrar una definición consensuada de ciberespacio. En primer lugar, porque el sentido común nos lleva a pensar ese ámbito como un lugar virtual, cuasi imaginario, tal como lo pensó William Gibson (1984) en una novela de ciencia ficción –*Neuromante*–, al describirlo como una «alucinación consensual» o una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Sin embargo, tal como señala Ocón (2019), el fenómeno del ciberespacio no es tan solo un fenómeno puramente cognitivo, ya que tanto su existencia como su artificialidad se apoyan en estructuras que son netamente físicas, tales como los ordenadores, los cables submarinos y la fibra óptica.

En segundo lugar, porque proliferan definiciones técnicas, que prescinden de los aspectos políticos, sociales e incluso culturales que posee el ciberespacio. Así, en un sentido técnico, podemos definir el ciberespacio como un dominio global compuesto por una red interdependiente de infraestructuras de información, que incluye internet, las redes de telecomunicaciones, procesadores y sistemas informáticos (Departamento de Defensa, 2010:140), o como un espacio virtual por donde circulan los datos electrónicos de todos los ordenadores del mundo (Comisión Europea, 2010, citado por Bejarano, 2011: 54). De estas definiciones se puede apreciar que la información –o los datos– es el elemento clave. El prefijo ciber refiere a los recursos electrónicamente interconectados de la informática (Nye, 2010) y sobre la base del mismo es factible abordar el resto de los conceptos asociados (como cibernauta, ciberseguridad, ciberdefensa, ciberestrategia y otros).

Nye (2010:3) define el ciberespacio como un régimen híbrido único de propiedades físicas y virtuales que posee la particularidad de ser creado por el hombre, es decir, no existe *per se*, sino que es artificial:

posee una infraestructura física, la cual le da sustento a la infraestructura informacional, o virtual, a la que otros llaman también infraestructura lógica. De ahí que podamos caracterizar el ciberespacio como un ámbito dual: es virtual y físico a la vez. Ambas esferas se relacionan y no es posible prescindir una de la otra. Un autor que incluye ambos elementos es Martin Libicki (2009), mediante su concepción del ciberespacio compuesto por tres capas: la física, la sintáctica y la semántica, a través de las cuales se integran el *hardware*, el *software* y los usuarios.

De este modo, la mayor parte de las definiciones de ciberespacio se centran en sus aspectos tecnológicos, y son muy pocas las que resaltan el factor humano, aspecto sumamente importante para el análisis de la ciberseguridad. Es por ello pertinente considerar el ciberespacio como el ámbito digital de interacción humana a través del cual se procesan distintos tipos de relaciones entre personas, grupos o Estados (Gastaldi et al., 2018).

En fin, el ciberespacio posee diferentes características: naturaleza tecnológica –artificial– que se erige sobre una infraestructura física, opera de manera virtual, posee alcance global y la información es el elemento central a través del cual ocurren interacciones humanas. El ciberespacio es el ámbito de la sociedad en red. Hoy, este medio alcanza prácticamente a todas las actividades del hombre, es decir, es también omnipresente, pues de él dependen, entre otras cosas, el comercio electrónico, servicios públicos como la luz eléctrica o el suministro de agua potable, millones de bases de datos, comunicaciones, entretenimiento, e incluso, en pleno auge, la internet de las cosas, que interconecta de manera digital y automatiza dispositivos como la heladera, el lavarropas, la cafetera, el auto. Una última característica es la transversalidad: ciertas dinámicas que ocurren en el ciberespacio pueden afectar directamente

a las infraestructuras físicas y a los dispositivos técnicos más allá de la gestión de las percepciones sociales, es decir, de sus usuarios. Paralelamente, las barreras entre la capa física y lógica se tornan permeables, lo que da lugar a una serie de posibles acciones que permiten la influencia directa del mundo virtual en el mundo real, no solamente en los dispositivos físicos, sino también en la vida personal de los individuos (Gastaldi y Ocón, 2019). Un delito cibernético es un ejemplo de dicha transversalidad.

La actual omnipresencia del ciberespacio en el quehacer humano ha quedado más que evidenciada en el marco de la pandemia de COVID-19. Paradójicamente, las fronteras físicas entre Estados se cerraron, el flujo de personas se detuvo, y la actividad de empresas transnacionales y el comercio internacional se redujo, lo que pone en evidencia los límites de la globalización. Sin embargo, las «fronteras» del ciberespacio no se cerraron. La información continuó fluyendo de un rincón al otro del mundo. Ejemplos abundan. Empresas tradicionales empezaron a trabajar «en línea», haciendo uso como nunca antes del teletrabajo; el comercio electrónico y los sitios de venta por internet crecieron notablemente; las videoconferencias en gran parte del mundo fueron los únicos medios para ver a familiares y amigos, así como también para gestionar reuniones de gobierno y empresariales. Tanto es así que la capitalización de Zoom llegó a superar a la de cualquier aerolínea estadounidense (Thornhill, 2020). A esta lista podemos agregar cómo la educación a distancia se convirtió en el único modelo de enseñanza y aprendizaje disponible, así como también el desarrollo y auge de aplicaciones de telemedicina, de pago electrónico, entre otras aplicaciones digitales.

Treinta años después de escribir su popular novela *Neuromante*, William Gibson expuso la idea de que el ciberespacio no ha evolucionado en paralelo con el mundo real, sino que este se estaba fusionando

con aquel (Thornhill, 2020). Más allá de la pandemia por COVID-19, de si sus efectos en materia de trasformación digital y conectividad serán duraderos o no, lo cierto es que cada vez es más difícil separar el mundo real del mundo virtual. La tendencia actual hacia un mundo en el que convergen en tiempo real una multiplicidad de ámbitos y actividades, personas y cosas con plataformas digitales, ha llegado para quedarse.

La convergencia digital hace referencia a la desaparición de barreras técnicas entre dispositivos electrónicos que transmiten información digital (Ibáñez, 2006). Hoy, gracias a los adelantos tecnológicos, es posible tener, en un único aparato, la radio, la televisión, el teléfono, un videojuego, internet, hasta la billetera. Todos los medios de transmisión de información se están integrando en un único dispositivo electrónico. Pero esta convergencia digital va más allá de lo meramente técnico: tiende a generar un novedoso ensamblaje entre la materia física, los hombres y los datos.

Al respecto, John Sheldon (2016: 282) señala que la sociedad actual se ha vuelto «ciberdependiente», pues esta digitalización del quehacer humano abarca desde la forma en que nos comunicamos hasta cómo se combate en una guerra. Así, frente a estas dinámicas, tanto la autoridad del Estado como su capacidad de control se han visto nuevamente afectadas. La soberanía digital, entendiendo esta como la capacidad del Estado de controlar el flujo de datos que atraviesa sus fronteras, ha aparecido como una nueva manifestación del ejercicio soberano.

La constante expansión de la esfera digital sobre las múltiples dimensiones de la vida humana y la dependencia cada vez mayor de las sociedades de tales plataformas tecnológicas ha dado lugar a una convergencia digital que no se encuentra librada de nuevos riesgos, amenazas y vulnerabilidades.

3. Las amenazas al Estado en el mundo convergente

Como decíamos, bajo el nuevo paradigma de la convergencia, en el que existe una incremental estructuración de las relaciones políticas, económicas y sociales en los espacios virtuales, se han abierto las puertas a una serie de dinámicas novedosas en cuanto a los riesgos y las amenazas para los países y sus habitantes (Gastaldi y Ocón, 2019).

Un aspecto que caracteriza al ciberespacio, tal como lo ha vislumbrado Joseph Nye (2010), es la dispersión del poder. El poder ciberespacial, o ciberpoder, tiene como elemento definitorio que, a diferencia de otros recursos de poder, como el económico, el político o el militar, no se requiere ser un Estado o un gran actor estratégico para emplear este recurso: solo se necesita el conocimiento técnico y un ordenador. Un solo individuo, como ha sido el caso de Edward Snowden, puede poner en jaque la credibilidad de un país; o una organización, como Wikileaks, puede revelar hasta los secretos más oscuros de un Estado. Julian Assange, su fundador, declaró que desde adolescente espiaba los correos electrónicos de los generales de los Estados Unidos (Metro Ecuador, 24 de junio de 2020). De este modo, la capacidad de ejercer el poder cibernético, se encuentra dispersa en una considerable cantidad de actores. A través del ciberpoder, se pueden emplear los recursos electrónicamente interconectados de la informática para influir eventos dentro del mismo ciberespacio o bien fuera de él. Toda operación cibernética malintencionada u hostil afecta de algún modo la disponibilidad, confiabilidad e integridad de la información; pero, además, puede tener consecuencias –o efectos cinéticos– sobre el mundo físico, gracias a la transversalidad del ciberespacio.

Así, lo que este nuevo paradigma torna evidente es el desplazamiento –y creciente dependencia– de los tradicionales factores de poder hacia el factor cibernético y una redistribución del poder a través

del empoderamiento de individuos y grupos dentro de la política internacional, que socava el monopolio del poder tradicionalmente ejercido por los Estados (Sheldon, 2016), aunque sin reemplazarlo. Pese a esta diseminación de actores en el sistema internacional, los Estados-nación aún detentan las mayores capacidades tecnológicas y recursos financieros para ejecutar sofisticadas operaciones cibernéticas (Rid, 2010), como ha sido el caso de la afectación del programa de enriquecimiento de uranio iraní con el virus Stuxnet en 2010, presuntamente por parte de Israel y Estados Unidos, y el reciente caso de Australia, que denunció ser objeto de un ciberataque masivo apoyado por un país extranjero contra todos los niveles de su gobierno, el sector industrial, educativo, de salud, y contra proveedores de servicios esenciales y operadores de infraestructura crítica (*El País*, 19 de junio de 2020).

En general, podemos agrupar el uso malintencionado del ciberespacio en cuatro tipos de actividades, de acuerdo con los actores que realizan el ciberataque y la motivación que poseen: cibercrimen, hacktivismo, ciberterrorismo y ciberguerra (Adkins, 2001). Esta tipología, si bien no es excluyente, alcanza a casi todo el universo de los ciberataques.

La primera modalidad de ciberataque, que es ejecutada por individuos u organizaciones delictivas, alcanza a todos los tipos penales contenidos en las legislaciones de los países sobre delitos informáticos –como actos ilegales contra la disponibilidad, la integridad y la confiabilidad de la información, interrupción de las comunicaciones, acceso ilegítimo a sistemas informáticos, violación de correo electrónico, *grooming* y pornografía infantil, entre otros–; y a nivel internacional, existe la denominada Convención de Budapest –Convenio sobre el delito cibernético del Consejo de Europa–, que busca establecer parámetros comunes en materia de derecho procesal y penal entre los países signatarios y políticas de cooperación

internacional en materia de lucha contra el delito cibernético. El hecho de que aquel o aquellos que cometen un ciberataque de cualquier otro tipo sean individuos sin rostro, gracias a las diversas técnicas que facilitan el anonimato en la red, y a que el delito no reconozca fronteras, puesto que el victimario puede estar en un país y su víctima en otro, hacen de esta modalidad de ciberataques una de las más frecuentes. Y la necesidad de cooperación internacional y de articular entre los países procedimientos homogéneos de lucha contra este modo de criminalidad se torna un requisito indispensable. El caso del ciberataque masivo con el *ransomware* WannaCry en mayo de 2017, que cifró archivos de cientos de ordenadores en todo el mundo, es un ejemplo de la dificultad para aplicar categorías tradicionales, como las de soberanía y territorio, al análisis de esta dinámica del ciberespacio. WannaCry mostró que un simple *malware* puede no solamente hacer disfuncional un dispositivo, sino que incluso puede afectar la economía y la seguridad de individuos, organizaciones y hasta naciones enteras, tornando inoperables sistemas informáticos indispensables para la gestión de servicios, como fue la afectación del Servicio Nacional de Salud del Reino Unido (Kaspersky, s/f).

Las otras modalidades de ciberataque –hacktivismo, ciberterrorismo y ciberguerra– tienen una clara intencionalidad política. El hacktivismo es una modalidad de ciberactismo en red en la que, para el logro de sus metas, sus actores recurren al hackeo de sistemas informáticos, principalmente a través del robo de información sensible con el fin de hacerla pública, por lo que muchos casos de hacktivismo se logran mediante operaciones de ciberespionaje, como el caso de Edward Snowden. Otros ejemplos de hacktivismo son las acciones de Anonymous y Wikileaks. Este tipo de operaciones tienen una clara intencionalidad política: sacar a la luz cuestiones que, a su entender, se basan en situaciones injustas, que afectan la libertad de expresión o

los derechos humanos. Así lo ha manifestado Julian Assange (2012:15) cuando caracterizó a internet como una amenaza para la civilización humana debido a los programas de interceptación y vigilancia masiva que operan diversos Estados a través de la red.

El hacktivismo ha generado serios desafíos a los países. El caso de WikiLeaks muestra una encrucijada para los Estados respecto del viejo dilema entre seguridad y libertad. En este sentido, lo que significó para muchos la defensa de la democracia y la libertad de la información, y una vulneración del derecho a la privacidad, para muchos gobiernos implicó una severa amenaza que alteró importantes vínculos tanto para la política interna como externa de las naciones, tras la revelación de información clasificada con motivos de seguridad nacional (Gastaldi y Ocón, 2019).

Tratando de dar una respuesta a este dilema, la Asamblea General de las Naciones Unidas dictó en 2013 la Resolución A/68/167 sobre el Derecho a la Privacidad en la Era Digital, en la cual se afirma que las garantías contenidas en el artículo 12 de la Declaración Universal de Derechos Humanos y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos sobre el derecho a la privacidad poseen plena vigencia en el ciberespacio. Luego de esta afirmación, cualquier captura de datos de los ciudadanos por medios electrónicos por parte de los Estados, incluso de metadatos, puede ser considerada una interferencia en el derecho a la privacidad de las personas. Por lo tanto, sólo el cumplimiento de los principios de legalidad, necesidad y proporcionalidad podría otorgar una justificación a una acción estatal contra este derecho (Gastaldi y Gioffreda, 2019).

En cuanto al ciberterrorismo, es preciso distinguir dos fenómenos, que pueden estar o no relacionados entre sí. El primero es el empleo de internet con fines terroristas, que en este caso remite principalmente al desarrollo de operaciones de propaganda y reclutamiento

y adiestramiento de combatientes para las organizaciones terroristas; y el segundo, el desarrollo de operaciones cibernéticas con fines terroristas, es decir, atentados a través de programas informáticos con efectos cinéticos sobre el mundo real. En la academia no existe un consenso respecto de si ambas manifestaciones pueden incluirse o no dentro del término «ciberterrorismo» (Sánchez Medero, 2015; Tellechea, 2018). En ambos casos, estas dinámicas traspasan las fronteras de los Estados y exigen acciones compartidas por parte de la comunidad internacional para combatir este flagelo. Paralelamente, debe señalarse la importancia que adquiere la red, no sólo con fines terroristas, sino también como un aspecto clave para las políticas de seguridad: su empleo con fines contraterroristas.

A fin de arrojar un poco de luz sobre el tema desde un enfoque de política pública, la Organización de las Naciones Unidas, a través de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), considera que el uso de internet con fines terroristas abarca seis modalidades, que en ocasiones suelen superponerse: la propaganda, que remite al reclutamiento; la radicalización y la incitación al terrorismo; la financiación; el adiestramiento; la planificación y ejecución de un atentado; y los ataques cibernéticos (UNODC, 2013).

Con relación a la última modalidad, la UNODC (2013:12) reseña el caso de un cibertaque que sufrió Israel en el año 2012, que consistió en múltiples operaciones cibernéticas contra sitios web, tales como la Bolsa de Valores de Tel Aviv y la compañía aérea nacional, además de la exposición pública de datos de tarjetas de crédito de ciudadanos israelíes. Sin embargo, la problemática del ciberterrorismo es más compleja aún, puesto que si bien a la fecha no se han registrado actos de terrorismo perpetrados a través de la red con efectos cinéticos, como podría ser derribar un avión en pleno vuelo o tomar el control de los semáforos de una ciudad y provocar accidentes de

tránsito masivos, la teoría indica que tales acciones podrían ser ejecutadas. El ciberterrorismo supone así una tangible amenaza políticamente construida, resultado de un mundo convergente. Por ello, el problema del ciberterrorismo se relaciona puntualmente con la necesidad de proteger las infraestructuras críticas, garantizando la ciberseguridad de sus redes y sistemas informáticos. Cometer un atentado de ese tipo requeriría de las organizaciones terroristas una gran inversión, mucha preparación y un alto conocimiento técnico, por lo que el mismo resultado –causar terror– se puede conseguir con mucho menos esfuerzo y a un costo inferior, tal como lo demuestran las organizaciones terroristas que suelen recurrir al empleo de artefactos explosivos improvisados como material para ejecutar atentados. Lo que queremos decir es que, seguramente, un lobo solitario con un cinturón explosivo causaría más pánico y terror que un apagón en el servicio eléctrico o una operación de *defacement* contra un sitio web gubernamental, como ha ocurrido en una oportunidad en el sitio web del Ejército Argentino, presuntamente a manos del ISIS.

Finalmente, dedicaremos unas líneas a la cuestión de la denominada ciberguerra. Nuevamente, estamos frente a un concepto polémico e interesante. Del mismo modo en que no ha habido a la fecha un caso empírico de un atentado terrorista cibernético, tampoco ha habido una guerra interestatal que se desarrolle exclusivamente por medios cibernéticos (Rid, 2010). Como corolario de la convergencia, es innegable que la guerra emplea medios cibernéticos, que las Fuerzas Armadas recurren a ellos como una especie de multiplicador de fuerzas, así como los servicios de inteligencia emplean también estos medios para la obtención, procesamiento y análisis de la información y desarrollo de operaciones. El componente cibernético ha derivado en la creación de ciberejércitos, de componentes específicos dentro de las mismas fuerzas armadas.

Algunos años atrás, muchos autores consideraban que la ciberguerra se transformaría en la nueva modalidad de conflicto armado interestatal (Arquilla y Rondfelt, 1993; Clake y Knake, 2010; Nye, 2010; Stone, 2010). Sin embargo, esa expectativa inicial empezó a declinar con el tiempo. Nye (2018), por ejemplo, ha señalado que el correr del tiempo ha demostrado que hasta ahora, las ciberarmas parecen más útiles para enviar señales o sembrar confusión que para generar destrucción física. O, como argumenta Rid (2013), al considerar que si se hace un examen más detenido, lo que está ocurriendo es justamente todo lo contrario a una ciberguerra, pues lo que el empleo de medios cibernéticos habilita a los Estados es confrontar de manera solapada, sin entrar en un conflicto bélico. En otras palabras, las operaciones cibernéticas hacen la guerra entre Estados menos probable (Gastaldi, 2019).

En este marco, es importante remarcar que la convergencia ha dado lugar a una nueva capacidad estatal en el escenario internacional, creando una zona gris, distinta a la de la paz y distinta a la de la guerra, que se relaciona con la aptitud de los Estados de emplear el ciberespacio con fines estratégicos (Gastaldi y Gioffreda, 2019).

El ciberespacio presenta, a diferencia de otros ámbitos desde donde los actores estatales pueden ejercer poder y hacer valer sus intereses estratégicos –como el espacio terrestre, aéreo o naval–, aspectos novedosos. En primer lugar, el ciberespacio brinda un velo de engaño. Gracias al empleo de determinadas técnicas de anonimato, un actor puede ejecutar una ciberoperación y permanecer invisible. Si bien se recurre a herramientas de informática forense e inteligencia para identificar a un potencial agresor, al momento no sería posible alcanzar un 100% de seguridad al respecto, por lo cual resulta difícil establecer la atribución frente a un ciberataque. A pesar de ser un factor decisivo, la identificación de los atacantes resulta ser un desafío

extremadamente complejo para los actores estatales y, por lo tanto, central para la formulación de una respuesta ante la agresión. La atribución trata de identificar el «quién», el «dónde» y el «cuándo», para decidir «cómo responder».

Como corolario de la dificultad para establecer la atribución, un país o un actor no estatal puede rechazar la imputación y quedar absuelto de cualquier responsabilidad. Por ejemplo, si bien Rusia fue sindicado como el actor estratégico que estuvo atrás de los ciberataques contra Estonia en 2007, este país nunca lo reconoció.

En segundo término, si bien el ciberespacio reproduce las asimetrías de poder de los ambientes tradicionales, pues para realizar una compleja operación cibernética se requieren muchos recursos, además de un acabado *know-how* técnico, abre posibilidades para que pequeños Estados puedan desarrollar algún tipo de operación que pueda afectar los intereses de un Estado más poderoso, cuando en confrontaciones convencionales o en el marco de las relaciones internacionales no tendrían ventaja alguna. A esto podemos agregar un tercer elemento, que es el dilema que se plantea en virtud de la asociación entre la esfera pública y privada que prevalece en el ciberespacio, que hace que las operaciones cibernéticas entre Estados sean poco frecuentes y limitadas (Valeriano y Maness, 2016), por el riesgo inherente de infringir daños colaterales a la población civil.

Por último, no debe menospreciarse el vacío legal existente en materia de una normativa internacional referida al comportamiento de los Estados en el ciberespacio, que contribuye a potenciar la anarquía del sistema internacional y facilitar conductas autónomas por parte de las unidades políticas.

Volviendo a un aspecto mencionado antes, el mundo no ha visto al momento una guerra completamente cibernética. Por lo tanto, el análisis caería dentro del ámbito de la ciberdiplomacia. Autores como Valeriano,

Jensen y Maness (2018) plantean que las formas mayoritarias de empleo de herramientas cibernéticas por parte de los Estados podrían ser parte de una estrategia de diplomacia coercitiva o guerra política, y suelen adoptar alguna de las siguientes formas: ya sea una acción de «disrupción cibernética», tendiente a ejecutar una acción de bajo costo y poco dañina destinada a acosar a un Estado para influir en su decisiones; de «ciberespionaje», tendiente a alcanzar una capacidad para alterar o manipular información por medios cibernéticos para obtener una ventaja en un proceso de negociación; o de «degradación cibernética», que refiere a operaciones de alto costo destinadas a dañar capacidades e infraestructura.

En resumen, el ciberespacio puede ser usado de múltiples formas. Desde ya, su empleo de manera hostil puede adoptar diversas modalidades. Mientras el mundo sólo cuenta con instrumentos legales para afrontar los delitos informáticos, otras formas de ejercicio del ciberpoder continúan aprovechándose de la falta de acuerdos a nivel internacional para sancionar el mal uso de este medio, a lo que podríamos agregar las operaciones de desinformación, también denominadas como *fake news*. Todas estas modalidades afectan actualmente la capacidad de los Estados de ejercer su soberanía. ¿Qué enmascara esta falta de acuerdos? Que, tal vez, muchos Estados busquen mantener la anomia en el ciberespacio con el propósito de esconder sus reales capacidades ciberofensivas y evitar reducir de ese modo la libertad de acción o no perder una ventaja estratégica.

Esto induce a los países, indefectiblemente, a que estén alertas acerca de los desarrollos en materia de virus, *malware* y otras «ciberarmas», y a instruir a sus agencias gubernamentales para que empleen estrictas medidas de ciberseguridad y protección de las infraestructuras críticas de la información y las comunicaciones. Por ahora, el ciberespacio se mantiene como un juego de suma cero, y la soberanía estatal es vulnerada de manera sistemática.

A modo de reflexión final

La soberanía de los Estados siempre ha estado sujeta a cambios en las relaciones de poder en el sistema internacional y a las diferentes modalidades de su ejercicio. Por ello, no puede pensarse como una categoría absoluta, sino como un concepto dinámico. Muchos autores han establecido clasificaciones para tratar de abstraer la complejidad del fenómeno y hacerlo comprensible. Sin embargo, tales conceptualizaciones se enfrentan a nuevos fenómenos. El ciberespacio ha presentado un desafío no sólo intelectual, sino también práctico, para la política pública. ¿Cómo defender la soberanía en un ámbito virtual y de alcance global, en el que muchos actores estatales y no estatales tienen capacidad para influir y afectar los intereses de la nación y de sus habitantes? Pregunta sencilla de formular, pero difícil de responder. Algunos dirían, de manera simplista, que «cualquier Estado puede desconectarse de la red», lo cual es técnicamente cierto; pero en sociedades crecientemente convergentes, el costo de dicha desconexión sería incalculable. El error tal vez sea tratar de explicar dinámicas nuevas con conceptos tradicionales. Sin embargo, pensar la soberanía en términos no territoriales dejaría a esta categoría vacía de contenido.

Tal como dice Alexander Wendt (2005), la anarquía es lo que los Estados hacen de ella. Y del mismo modo, podríamos extrapolar la idea a la soberanía. Wendt (2005:23) señalaba que el hecho de que las prácticas de soberanía que desarrollan los Estados se hayan orientado históricamente hacia la producción de espacios territoriales diferenciados afecta a la conceptualización de lo que estos deben proteger. Así, podríamos pensar que la intención de extrapolar la soberanía al ciberespacio sólo podría darle al Estado el control de los medios materiales del ciberespacio, es decir, de la infraestructura física del mismo. El control sobre la información que fluye a través de dicha infraestructura

encierra dificultades no sólo técnicas, sino también políticas. Internet fue y será sinónimo de democracia, de libertad, y cualquier Estado que quiera avanzar en el dominio y control de estos flujos corre el riesgo de incurrir en una actitud represiva, de censura o coacción, que en algún momento se volverá contra sí mismo.

Esto no significa tampoco dejar el ciberespacio como un «estado de naturaleza». Se requiere avanzar en el establecimiento de consensos, normas o regímenes internacionales que establezcan parámetros aceptables para la conducta estatal y mecanismos de gobernanza. No se trata de intentar «territorializar» el ciberespacio, como modo de ganar soberanía. Se trata de establecer reglas de juego internacionalmente aceptadas para reducir la incertidumbre y la anarquía ciberespacial. A medida que el paradigma de la convergencia vaya ganando terreno, más difícil será materializar la soberanía. Tal vez, en ese entonces, los Estados deban empezar a pensar nuevas fórmulas de estatalidad, de convivencia y de bienestar frente a ese futuro inminente. Parafraseando a Saskia Sassen (1996), la convergencia digital supone una transformación en la articulación entre soberanía y territorio.

Mientras tanto, necesitamos continuar ajustando nuestras políticas de seguridad y defensa al componente ciberespacial para poder enfrentar los riesgos y amenazas de dicho entorno.

Siempre es un placer leer a Alvin y Heidi Toffler. Su visión del mundo del mañana nos llama la atención en el presente. En su obra *Las guerras del futuro* (1994:189-194), planteaban la importancia del empleo de armas no letales asociadas a la doctrina militar de negación de servicio. Recién cinco años después se iba a producir en la historia el primer ataque informático de negación de servicio distribuido (DDOS). Los Toffler, correctamente, señalaron entonces que si muchas de estas armas se hallaran en manos de delincuentes o terroristas, en lugar de ser monopolio de los «buenos», podrían

multiplicar la fuerza de aquellos, pero agregaron que, incluso siendo empleadas por autoridades legítimas, las armas no letales suscitarían inquietudes políticas y morales. Finalmente, se preguntaban: «¿Cabe la posibilidad, en definitiva, de que lleven a menos matanzas –y también menos democracia– si los Estados consiguen cegar, deslumbrar, desorientar o derrotar de cualquier otro modo no letal a quienes critiquen su proceder?» (Toffler y Toffler, 1994). Así, pues, la situación estratégica actual ha logrado responder a este interrogante del pasado a partir del desarrollo y uso de armas cibernéticas, las que finalmente han dado origen a este nuevo ámbito entre la guerra y la paz, tal como ellos lo pensaron décadas atrás: «Es posible que mañana, tras el fracaso de unas negociaciones diplomáticas, los Gobiernos recurran a medidas no letales antes de lanzarse a una guerra tradicional y sangrienta (...) Esta área entre el fracaso de la diplomacia y el primer disparo es un terreno que hasta hoy nunca ha sido cuantificable. Ha sido un espacio inexistente. La no letalidad surge así no como una simple sustitución de la guerra o una prolongación de la paz, sino como algo diferente y radicalmente nuevo en la escena internacional» (Toffler y Toffler, 1994:194).

El ciberespacio y la convergencia han hecho esto hoy posible, y en las capacidades estatales y de los *policy makers* está la clave para transitar la nueva era.

Referencias bibliográficas

Adkins, B. (2001). *The Spectrum of Cyber Conflict from Hacking to Information Warfare: what is Law Enforcement's Role?* Air command and Staff College. Air University. Disponible en http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/01-003.pdf.

Arquilla, J.; Ronfeldt, D. (1993). «Cyberwar is Coming!». *Comparative Strategy*, Vol. 12, Nº2, Spring, pp. 141-165.

Assange, J. (2012). *Criptopunks. La libertad y el futuro de internet*. Buenos Aires: Editorial Marea.

Bartolomé, M. (2018). «La seguridad internacional contemporánea: contenidos temáticos, agenda y efectos de su ampliación». En *Relaciones Internacionales*, *55*, pp. 123-145.

Beck, U. (1998). *¿Qué es la globalización?* Barcelona: Paidós.

Bejarano, M. J. (2010). «Alcance y ámbito de la seguridad nacional en el ciberespacio». En IEEE. *Cuadernos de Estrategia Nº 149 – Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio*. IEEE – Instituto Universitario General Gutiérrez Mellado.

Bull, H. (1977). *The Anarchical Society. A Study of Order in World Politics.* Nueva York: Columbia University Press.

Castells, M. (2007). «Communication, power and counter-power in the network society». *International Journal of Communication, 1,* 238-266.

Clarke, R. y Knake, R. (2010). *Cyberwar. The Next Threat to National Security and what to do about It*. Washington DC: Harper Collins.

D'Alessandro, M. (2004). «Control estatal y administración: una reseña de su desarrollo». *POSTdata: Revista de Reflexión y Análisis Político,* 10, 95-129.

D'Alessandro, M. (2011). «Democracia, agencia y Estado. Teoría con intención comparativa de Guillermo O'Donnell (reseña)». En *POSTdata: Revista de Reflexión y Análisis Político, 16* (2), 319-321.

Departamento de Defensa de los Estados Unidos (2010). *Joint Publication 1-02. Dictionary of military and associated terms*. Disponible en http://www.dtic.mil/dtic/tr/fulltext/u2/a485800.pdf.

El País (2020, 19 de junio). «Australia denuncia ser objetivo de un ciberataque apoyado por un país extranjero». Disponible en https://elpais.com/internacional/2020-06-19/australia-denuncia-ser-objetivo-de-un-ciberataque-apoyado-por-un-pais-extranjero.html.

Fernández, A. (2002). «Las nuevas funciones del Estado». En *Estudios Sociales, 22-23, 211-228.*

Fund For Peace (2011). Índice de Estados fallidos. Disponible en https://www.casede.org/BibliotecaCasede/Indice_de_Estados_Fallidos_AnaliticaInternacional.pdf.

Gastaldi, S. (2019). «El ciberespacio en las relaciones internacionales. Enfoques teóricos rivales». Ponencia presentada en el XIV Congreso Nacional de Ciencia Política «La política en incertidumbre. Reordenamientos globales, realineamientos domésticos y la cuestión de la transparencia», organizado por la Sociedad Argentina de Análisis Político y la Universidad Nacional de San Martín.

Gastaldi, S. et al. (2018). «Ciberdefensa y soberanía nacional: indagando teorías y definiendo conceptos». Primeras Jornadas de Ciencia y Tecnología de la Universidad de la Defensa Nacional. Buenos Aires, 28 de julio.

Gastaldi, S y Gioffreda, C. (2019). «El ciberespacio como escenario estratégico. Dilemas para los Estados y la política pública». Ponencia presentada en el XIV Congreso Nacional de Ciencia Política «La política en incertidumbre. Reordenamientos globales, realineamientos domésticos y la cuestión de la transparencia», organizado por la Sociedad Argentina de Análisis Político y la Universidad Nacional de San Martín.

Gastaldi, S. y Ocón, L. (2019). «Ciberespacio y defensa nacional: una reflexión sobre el dilema libertad-seguridad en el ejercicio de la soberanía». En *Defensa Nacional. Revista científica, 02,* pp. 88-109.

Gibson, W. (1984). *Neuromante*. Barcelona: Minotauro.

Held, D. (1997). *La democracia y el orden global. Del Estado moderno al gobierno cosmopolita*. Barcelona: Paidós.

Kaspersky (s/f). *¿Qué es el ransomware WannaCry?.* [En linea]. Disponible en https://www.kaspersky.es/resource-center/threats/ransomware-wannacry.

Keohane, R. y Nye, J. (2000). *Power and interdependence.* Nueva York: Longman.

Krasner, S. (2001). *Sovereingty. Organised hypocrisy.* Nueva Jersey: Princeton University Press.

Ibáñez, J. (2006). «Globalización e Internet: poder y gobernanza en la sociedad de la información». *Revista Académica de Relaciones Internacionales*, *5*. Disponible en http://www.relacionesinternacionales.info.

Libicki, M. (2009). *Cyberdeterrence and cyberwar*. Rand Corporation. Recuperado de https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Metro Ecuador (2020, 24 de junio). *Julian Assange enfrenta nueva acusación: es relacionado con Anonymous.* Disponible en https://www.metroecuador.com.ec/ec/noticias/2020/06/24/julian-assange-enfrenta-nueva-acusacion-ee-uu.html.

Nye, J. (2010). *Cyber Power*. Cambridge: Bedfer Center for Science and International Affairs.

Nye, J. (2018, 5 de julio). «Ciberataques: ¿el arma perfecta?». Projetc Syndicate. Disponible en https://www.project-syndicate.org/commentary/deterring-cyber-attacks-and-information-warfare-by-joseph-s--nye-2018-07/spanish.

Rid, T. (2012). «Cyber war will not take place». *Journal of Strategic Studies*, 35 (1).

Rid, T. (2013). «More attacks, less violence». *Journal of Strategic Studies*, 36 (1), pp. 139-142, DOI: 10.1080/01402390.2012.742012.

Rid, T. y Buchanan, B. (2014). «Attributing cyber attacks». *Journal of Strategic Studies*, DOI: 10.1080/01402390.2014.977382.

Sassen, Saskia (1996). *¿Perdiendo el control. La soberanía en la era de la globalización?* Barcelona: Bellaterra.

Ocón, A. (2019). «Una aproximación a la geopolítica del ciberespacio». Ponencia presentada en el XIV Congreso Nacional de Ciencia Política «La política en incertidumbre. Reordenamientos globales, realineamientos domésticos y la cuestión de la transparencia», organizado por la Sociedad Argentina de Análisis Político y la Universidad Nacional de San Martín.

O'Donnell, G. (1978). «Apuntes para una teoría del Estado». *Revista Mexicana de Sociología*, 40(4). 1157-1199. México: UNAM.

O'Donnell, G. (2010). *Democracia, agencia y estado. Teoría con intención comparativa*. Buenos Aires: Prometeo.

Organización de las Naciones Unidas (2014). *Resolución A/RES68/167*. [En línea]. Disponible en https://undocs.org/es/A/RES/68/167.

Oszlak, O. (1982). «Reflexiones sobre la formación del estado y la construcción de la sociedad argentina». *Desarrollo Económico. Revista de Ciencias Sociales, Vol. XXI, enero-marzo.*

Oszlak, O. (1990). *La formación del Estado argentino*. Buenos Aires: Editorial de Belgrano.

Pinto, J. (1996). *Max Weber actual. Liberalismo ético y democracia.* Buenos Aires: Eudeba.

Pousadela, I. (2001). «La globalización y lãs transformaciones em El capitalismo contemporáneo». *Res Pública*, *1.*

Sánchez Medero, G (2013). «El ciberterrorismo: de la web 2.0 al Internet profundo». *Revista Ábaco, 85* (3), pp-100-108.

Santos Villareal, G. (2009). *Estados fallidos: definiciones conceptuales.* Centro de Documentación, Información y Análisis de la Subdirección de Política Exterior de la Camára de Diputados de México. Disponible en http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-07-09.pdf.

Sheldon, J. (2016). «The rise of cyberpower». En J. Baylis; J. Wirtz; C. Gray (Eds). *Strategy in the Contemporary World.* Oxford: Oxford University Press.

Skocpol, T. (1989). «El Estado regresa al primer plano. Estrategias de análisis en la investigación actual». *Zona Abierta, 50* (enero-marzo), pp. 71-122.

Stiennon, R. (2017, 7 de diciembre). «Cyber Pearl Harbor versus the real Pearl Harbor». *Forbes*. Disponible en https://www.forbes.com/sites/richardstiennon/2017/12/07/cyber-pearl-harbor-versus-the-real-pearl-harbor/#5e3f10365bf7.

Stone, J. (2013). «Cyber war will take place!». *Journal of Strategic Studies, 36* (1), 101-108, DOI: 10.1080/01402390.2012.730485.

Tellechea, M. (2018). «Ciberterrorismo, ¿realidad o mito?». En *Cuaderno de Trabajo del Centro de Investigaciones y Estudios Estratégicos*, *5*, disponible en Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE), https://www.anepe.cl/wp-content/uploads/Cuaderno-de-Trabajo-N%C2%B05-2018.pdf.

Thornhill, J. (2020, 06 de abril). «COVID-19 está acelerando el paso al 'teletransporte'». *Financial Times* [En línea]. Disponible en https://www.elfinanciero.com.mx/financial-times/covid-19-esta-acelerando-el-paso-al-teletransporte.

Toffler, A. y Toffler, H. (1994). *Las guerras del futuro. La supervivencia en el alba del siglo XXI.* Barcelona: Plaza y Janés.

UNODC (2013). *El uso de Internet con fines terroristas*. Viena: Oficina de las Naciones Unidas contra la Droga y el Delito.

Valeriano, B; Maness R. (2016). *Cyber War vs Cyber Realities. Cyber Conflict in the International System*. Oxford: Oxford University Press.

Valeriano, B; Maness R. y Jensen, B. (2018b, 13 de julio). «Cyberwarfare has taken a new turn. Yes, it's time to worry». *The Washington Post*. Disponible en https://www.washingtonpost.com/news/monkey-age/wp/2017/07/13/cyberwarfare-has-taken-a-new-turn-yes-its-time-toworry/?noredirect=on&utm_term=.3c29afc7 b1a4.

Weber, M. (2002). *Economía y sociedad.* México D.F.: Fondo de Cultura Económica.

Wendt, A. (2005). «La anarquía es lo que los Estados hacen de ella. La construcción social de la política de poder». *Revista Académica de Relaciones Internacionales*, *1*. Disponible en https://revistas.uam.es/relacionesinternacionales/article/view/4828.

Zacher, M. (1992). «The decaying pillars of the westphalian temple: implications for the international order and governance». En J. Rosenau y E. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics.* Cambridge: Cambridge Studies in International Relations.

SOL GASTALDI. Licenciada en Ciencia Política de la Universidad de Buenos Aires y magíster en Defensa Nacional de la Universidad de la Defensa Nacional. Investigadora docente de la Universidad de la Defensa Nacional, Facultad de la Defensa. Directora del proyecto de investigación «Paz y Guerra en el Ciberespacio. El fenómeno del ciberconflicto y sus impactos para la Defensa Nacional», financiado por la Universidad de la Defensa Nacional a través del programa UNDEFI. Profesora de grado en la carrera de Ciencia Política de la Universidad de Buenos Aires y de posgrado en la Maestría en Defensa Nacional de la Universidad de la Defensa Nacional. Posee diversas publicaciones en libros y revistas especializadas en ciencias sociales nacionales e internacionales sobre defensa nacional, estrategia, planeamiento militar, relaciones civiles-militares y ciberdefensa.

CAPÍTULO 4

La brecha digital de género en América Latina

Ana Inés Basco
Paula Garnero

Introducción[1]

El mundo entero está siendo atravesado por el paradigma de la digitalización, también llamado revolución 4.0, caracterizado por la posibilidad tecnológica de generar, transmitir, procesar y analizar una enorme cantidad de datos en tiempo real. Se trata de una gran variedad de tecnologías digitales que imponen una nueva forma de organización de la vida productiva y social; cambia la forma en que las personas se comunican, trabajan y generan valor.

Desde una visión más positiva del cambio tecnológico, se destaca que las tecnologías digitales son potencialmente igualadoras de oportunidades. Por ejemplo, las TIC pueden facilitar la vida de personas con discapacidad; potenciar a las empresas medianas y pequeñas para

1 Se agradece la colaboración de Ángeles Barral Verna, consultora del INTAL, BID.

acceder a mercados globales; conectar a la población de zonas rurales/ciudades chicas con el resto del mundo; brindar oportunidades de trabajo remoto, capacitación o diagnóstico médico a distancia, entre muchas otras.

Sin embargo, la naturaleza misma del progreso tecnológico lleva a una distribución asimétrica y a la concentración de sus beneficios en pocos actores; las oportunidades no se distribuyen de forma equitativa entre los países, ni entre las empresas de distintos tamaños, ni entre las personas[2].

En esta cuarta revolución industrial, se observa el desarrollo de economías cada vez más basadas en servicios, como así también una notable expansión de las plataformas digitales, que ofrecen nuevos y generalizados espacios de interacción (Basco, Beliz, Coatz y Garnero, 2018). Conviven los riesgos vinculados a la pérdida de empleo por la automatización, y el surgimiento de nuevas oportunidades y formas novedosas de trabajo.

¿Cómo ven estos cambios las latinoamericanas y los latinoamericanos? ¿Qué tan dispuestas y dispuestos están a incorporar tecnologías digitales en sus hábitos? ¿Existen percepciones distintas sobre el impacto del cambio tecnológico entre mujeres y hombres en América Latina? ¿Existen sesgos de comportamiento que condicionen la «vocación» de las mujeres generando una menor inclinación

---

2 Por ejemplo, a nivel mundial, se observa que la mayor adopción de tecnologías de la industria 4.0 se concentra en empresas de gran tamaño. Incluso, el desarrollo y producción de ciertas tecnologías se concentra en pocos países. En el mercado de robótica industrial, los principales cinco países productores de tecnología (China, Japón, Alemania, Estados Unidos y Corea) son al mismo tiempo los principales receptores/adoptantes, lo que genera importantes barreras de entrada para nuevos actores (Basco, Beliz, Coatz y Garnero, 2018).

hacia carreras duras? ¿Hay brecha de habilidades digitales entre mujeres y hombres?

Estas son algunas de las preguntas que nos hicimos desde el Instituto para la Integración de América Latina y el Caribe (INTAL) del Banco Interamericano de Desarrollo (BID). Buscamos encontrar las respuestas principalmente a partir de una alianza que tenemos junto a Latinobarómetro, y con la cual realizamos todos los años una encuesta anual en la que indagamos la opinión de 20.000 latinoamericanos/as en 18 países de la región, en relación con el impacto del mundo digital en sus vidas[3].

1. Hábitos digitales

En este documento se define brecha digital de género como la diferencia entre mujeres y varones en relación con el uso y acceso a las nuevas tecnologías e internet, así como también en relación con las habilidades tecnológicas.

En América Latina, algunas tecnologías puntuales avanzan a pesar de que un alto porcentaje de la población no logra satisfacer necesidades básicas. Según datos de Latinobarómetro 2018, el 89% de las personas tiene teléfono celular, mientras que el 75% no cuenta con calefacción/aire acondicionado. Incluso, la penetración de

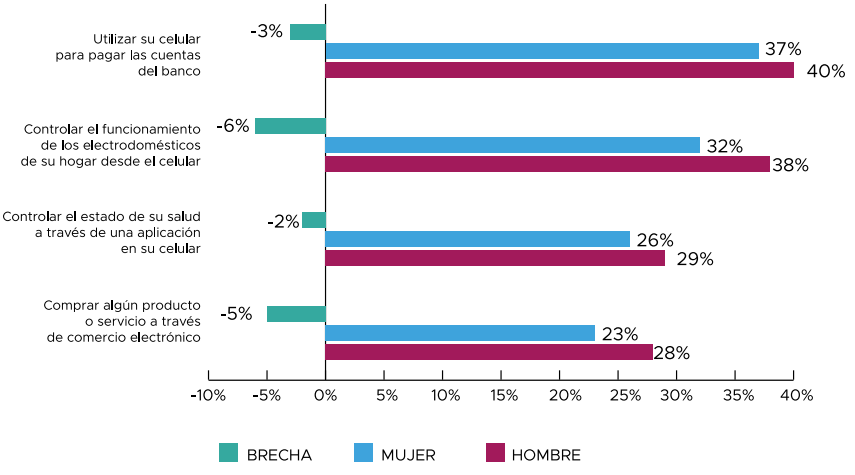
3 Latinobarómetro constituye el principal banco de datos de opinión pública en América Latina y es, por lo tanto, una encuesta de opinión pública anual, con muestras representativas de cada país, que aplica un cuestionario común con una unidad metodológica y técnica que permite la representación de las opiniones, actitudes, comportamientos y valores de 18 países de América Latina. El estudio representa a una población de 600 millones de habitantes y los temas principales de su abordaje y seguimiento son la democracia, el estado de la economía, el avance tecnológico y los esfuerzos de integración regional.

Smartphone (47% de la población) es mayor que la del agua caliente por cañería (36% de la población). Entre las personas que sólo acceden a una comida diaria, el 80% tiene celular y el 32% tiene *smartphone*.

La conectividad a internet resulta una prioridad para los habitantes de la región: el 65% de la población se mostró a favor de garantizar la universalidad en la provisión de este servicio, incluso cuando esto implique postergar la inversión en carreteras. Sin embargo, en América Latina, cerca de 300 millones de personas no tienen acceso a internet (OCDE, 2017). Esto representa un problema serio; más aún, considerando que la brecha digital tiende a profundizar las desigualdades socioeconómicas preexistentes y que el punto de partida es de inequidades de género muy marcadas en el acceso a internet y a los derechos digitales en todos los países en desarrollo (Pombo, Gupta y Stankovic, 2018).

Al analizar los hábitos digitales, se encontró que las mujeres se muestran menos familiarizadas que los hombres con el uso (y potencialidades) de apps y plataformas digitales en el apoyo de tareas cotidianas, lo que da lugar a brechas de género de entre 6% y 2% (ver Gráfico 1). El hábito digital más aceptado en la región es utilizar el celular para pagar las cuentas bancarias (37% entre las mujeres y 40% entre los hombres). La brecha más grande (-6 puntos porcentuales) se muestra en la opción de utilizar el celular para controlar electrodomésticos del hogar (38% de los hombres lo hacen o estarían dispuestos a hacerlo, vs. 32% de las mujeres). Las latinoamericanas muestran también rezago (-5 puntos porcentuales) en la realización (y predisposición a realizar) compras a través de plataformas digitales (23% vs. 28% entre los hombres).

Gráfico 1. Porcentaje de personas que utilizan o les gustaría utilizar tecnologías para la realización de determinadas tareas



Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

Colombia, a pesar de registrar valores promedio superiores a los regionales, exhibe las brechas de género más amplias en todos los hábitos: en el uso del celular para controlar electrodomésticos (14 puntos porcentuales); en las compras por plataformas digitales (12 puntos porcentuales); en la utilización de celulares para controlar la salud (10 puntos porcentuales); y de celulares para pagar cuentas bancarias (7 puntos) (ver Tabla 1). En el extremo opuesto, se destacan Brasil, Nicaragua, Costa Rica, con brechas de género muy bajas e incluso con algunos hábitos en los cuales las mujeres se muestran más favorables que los hombres.

Tabla 1. Brecha de género en hábitos digitales. Resultados por país

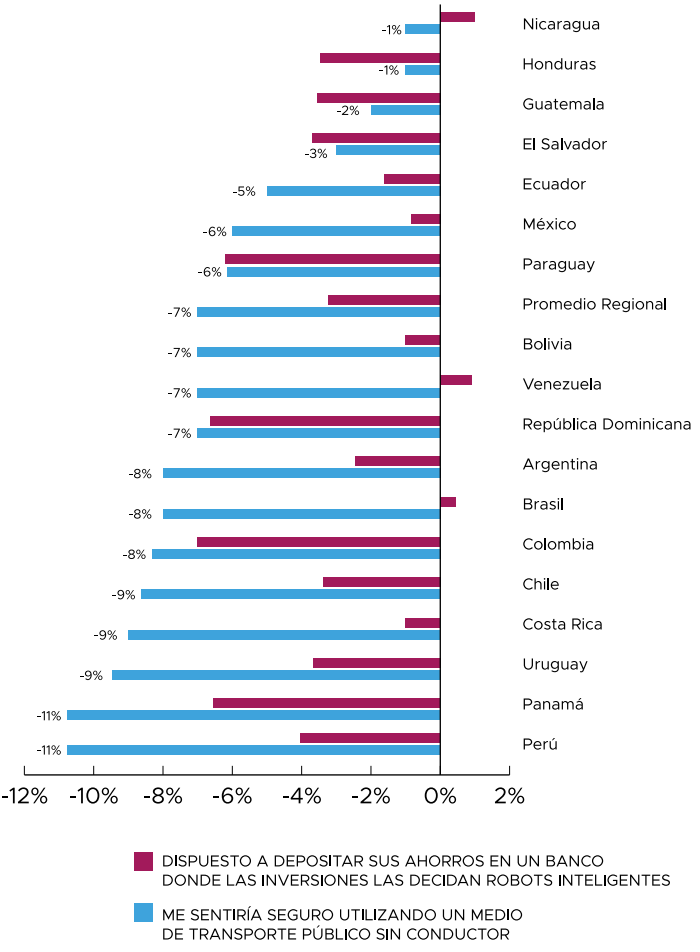
País	Controlar Salud	Comercio Electrónico	Pagar Cuentas Bancarias	Controlar Electrodomésticos
Colombia	-10%	-12%	-7%	-14%
Bolivia	-8%	-7%	-9%	-12%
Perú	-4%	-8%	-7%	-12%
Paraguay	-3%	-9%	-7%	-9%
Chile	-4%	-6%	-2%	-7%
Honduras	0%	-6%	2%	-7%
Rep. Dominicana	-2%	-4%	0%	-6%
Argentina	-8%	-3%	-1%	-6%
Panamá	-4%	-3%	-1%	-6%
Promedio Regional	-2%	-5%	-3%	-6%
Uruguay	1%	-5%	-4%	-5%
Guatemala	-5%	-11%	-8%	-4%
Ecuador	2%	0%	-3%	-4%
México	-3%	-4%	-5%	-4%
El Salvador	0%	-1%	-6%	-3%
Venezuela	0%	-4%	0%	-3%
Brasil	2%	-5%	2%	-2%
Nicaragua	2%	-1%	4%	-2%
Costa Rica	0%	-1%	-3%	2%

Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

El hábito de utilizar plataformas digitales para generar ingresos es incipiente en la región (9% de utilización promedio)[4]. Con excepción de Colombia, en todos los países de América Latina, menos mujeres que hombres utilizan esta tecnología como una forma alternativa de ingresos (8% vs. 10%), lo cual se traduce en una brecha de género de -2 puntos porcentuales.

4 Se consideraron las respuestas afirmativas a la pregunta: P64N: ¿Ha usado usted alguna plataforma digital para generar ingresos? Por ejemplo Uber o Cabify.

Gráfico 2. Inteligencia artificial aplicada al sistema de transporte público y al sistema bancario. Brecha de género por países



Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

La menor aceptación de las latinoamericanas frente al avance tecnológico en la vida cotidiana alcanza también al avance de la inteligencia artificial en el transporte público y en el sistema bancario (ver Gráfico 2). Consultados sobre la posibilidad de viajar en un vehículo

público conducido en forma autónoma, se encontró una brecha promedio de 7 puntos (19% de confianza en las mujeres vs. 26% en los hombres). Debe destacarse que en los 18 países de la región las mujeres se mostraron menos favorables que los hombres a utilizar vehículos autónomos, con picos en Panamá y Perú, donde la brecha de género alcanzó los 11 puntos.

Con respecto a la posibilidad de depositar ahorros en un banco donde las inversiones las decidan robots inteligentes, tanto la brecha de género como el promedio regional de aceptación fueron menores (11 y -3 puntos porcentuales, respectivamente). Los países con brechas de género más altas fueron Bolivia, Colombia, Panamá y República Dominicana (7 puntos). En cambio, las mujeres se muestran más favorables que los hombres a utilizar inteligencia artificial en el sistema financiero en Brasil, Venezuela y Nicaragua.

2. Robots, tecnología y empleo

Uno de los interrogantes que suenan más en el contexto de la revolución 4.0 está asociado al posible desplazamiento de la fuerza de trabajo. Desde la primera revolución industrial, las sociedades muestran una particular preocupación por el «desempleo tecnológico», tema ampliamente abordado por la literatura. A mediados de la década del 90, Jeremy Rifkin anunciaba «el fin del trabajo humano»: preveía una enorme pérdida de puestos de trabajo por el avance tecnológico y el comienzo de una *nueva era,* donde las personas gozarían de más tiempo para el ocio y de una renta universal para la subsistencia. Parte de la literatura señala que estamos frente a la obsolescencia de buena parte de la fuerza de trabajo (Mokyr, Vickers y Ziebarth, 2015). Frey y Osborne (2013), de la Universidad de Oxford, estimaban que en los Estados Unidos se perdería el 47% de ocupaciones en los siguientes 20 años.

Ese pronóstico sombrío no sólo no se materializó, sino que estudios posteriores demostraron que las tecnologías avanzan sobre determinadas tareas y no sobre ocupaciones enteras. Aplicando una metodología corregida al trabajo de Frey y Osborne, nuevas estimaciones para 21 países de la OCDE suponen que sólo el 9% de los empleos podrían estar en riesgo frente a la automatización y la digitalización (Arntz, Gregory y Zierahn, 2016). Estas posturas apelan a la evidencia de que la mayor parte del impacto de la automatización sobre el empleo en la última década se viene produciendo dentro del puesto de trabajo, dedicando menos horas a tareas automatizables y más horas a tareas complejas y de relación interpersonal (Albrieu et al., 2019). Es decir, que el impacto primario podría suceder en la combinación de tareas desempeñadas dentro de los puestos de trabajo, y no tanto en la combinación o la cantidad de puestos de trabajo de la economía (Pounder y Liu, 2018).

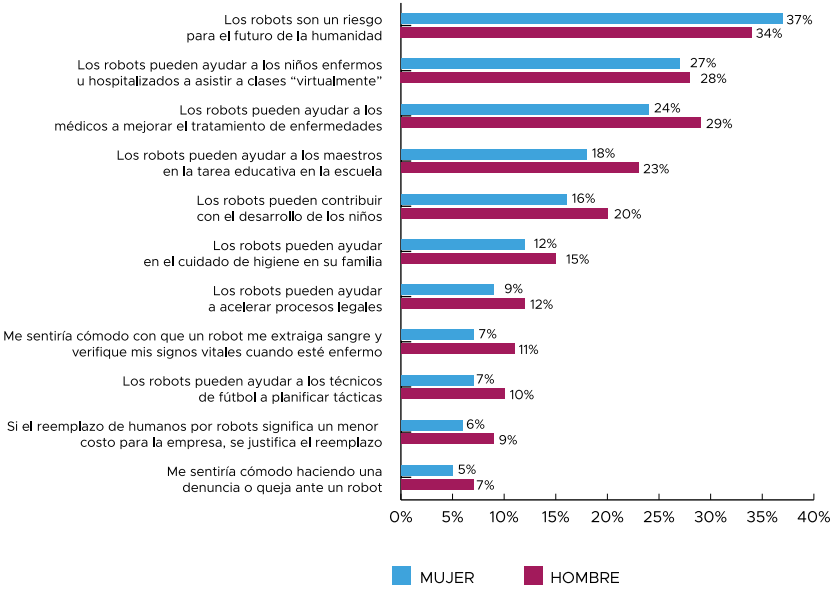
Más allá de cuál de estas dos visiones es la correcta, lo cierto es que algunos estudios indican que la automatización de tareas producto del cambio tecnológico podría afectar más a hombres que a mujeres, debido a que reemplaza principalmente habilidades físicas en donde ellos son mayoría (WTO, 2017).

A pesar de ello, y si bien los robots son aún temidos por la mayoría de las personas de la región, se observa un mayor rechazo a su avance entre las mujeres; el 37% de las latinoamericanas cree que son un riesgo para el futuro de la humanidad (vs. 34% entre los hombres).

Las mujeres muestran mayor resistencia al avance de los robots en todas las áreas de la vida cotidiana (ver Gráfico 3). Las brechas de género más grandes (5 puntos) se presentan en las opiniones sobre la posibilidad de los robots de ayudar a los maestros en las tareas educativas y a los médicos en el tratamiento contra enfermedades. En este sentido, no puede perderse de vista que en América Latina, las

actividades relacionadas con el cuidado y la reproducción, como servicio doméstico, salud o educación, se encuentran feminizadas. Así, surge el interrogante de si el mayor rechazo de las mujeres al avance de los robots se funda en el temor a perder el empleo o en la creencia de que este tipo de tareas difícilmente puedan automatizarse y seguirán dentro del dominio humano.

Gráfico 3. Percepciones de mujeres y hombres en relación con el avance de los robots [5]



Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

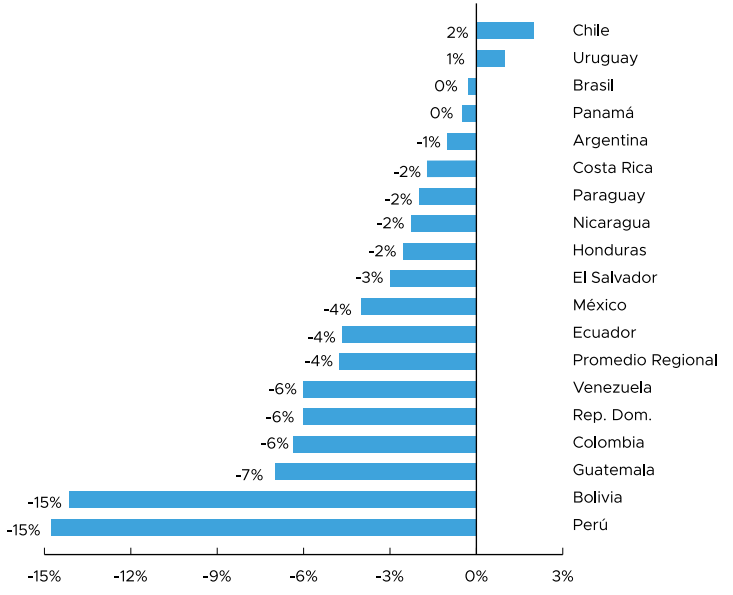
Asimismo, 8 de cada 10 personas en América Latina perciben positivamente la tecnología y la consideran beneficiosa para su empleo.

---

5 Se muestran los porcentajes de personas «de acuerdo» con cada una de las afirmaciones.

Esta percepción es más marcada en los hombres que en las mujeres (80% vs. 76%), lo que confirma una brecha de género promedio de 4 puntos. En la mayoría de los países no se encuentran diferencias sustantivas en la percepción de mujeres y hombres con respecto a los beneficios de la tecnología en el empleo (ver Gráfico 4), con excepción de Bolivia y Perú, donde alcanza 15 puntos. Contrariamente, en Chile y Uruguay, más mujeres que hombres la consideran beneficiosa.

Gráfico 4. Brecha de género en la percepción de la tecnología como beneficiosa para el empleo. Resultados por países

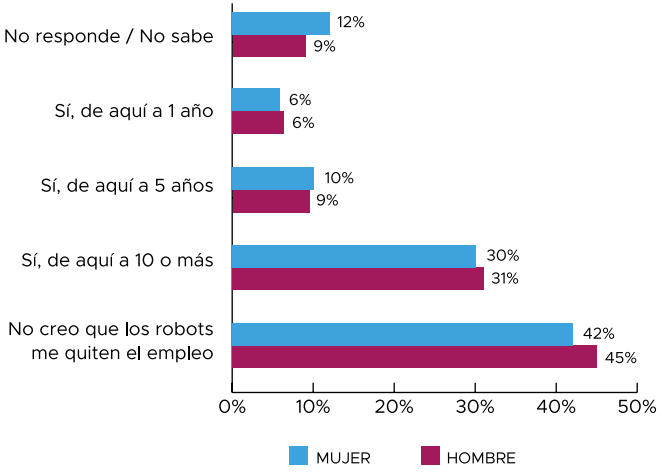


Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

Consultadas sobre la posibilidad de que los robots le quiten el empleo, en promedio, el 46% de las mujeres reconoce que –tarde o temprano– esto podría ocurrir, aunque no se observan diferencias significativas en las percepciones por género (ver Gráfico 5). En cambio, se evidencia

un optimismo levemente mayor entre los hombres que entre las mujeres frente a la posibilidad de conservar el empleo (45% vs. 42%), y un mayor porcentaje de mujeres que no pueden o no saben responder (12% vs. 9%).

Gráfico 5. Temor a perder el empleo por el avance de los robots. Promedio por género



Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

3. Habilidades para los trabajos del futuro

En la cuarta revolución industrial, surgen múltiples y novedosas formas de trabajo, como así también la universalización de nuevos requerimientos en términos de habilidades. Pero también, como fue mencionado, deja en evidencia el potencial de la automatización para destruir ocupaciones rutinarias de baja calificación y, al mismo tiempo, generar oportunidades en sectores intensivos en tecnologías, que demandan trabajadores calificados con habilidades cognitivas y socioemocionales acordes al paradigma 4.0 (Basco, Beliz, Coatz y Garnero, 2018). En países con altos niveles de adopción de tecnologías

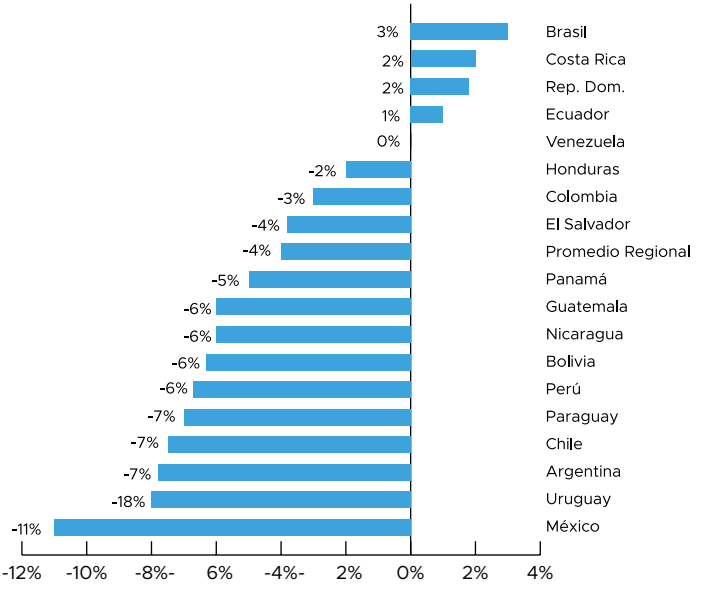
de la industria 4.0[6], se observa, además, que el desempleo tecnológico es también compensado por el derrame que los sectores dinámicos ejercen sobre otros sectores de baja complejidad tecnológica. Esto lleva a los muchos trabajadores con habilidades básicas a competir por empleos en sectores de baja productividad y, por lo tanto, a percibir bajas remuneraciones.

Según un informe del Banco Mundial (2016), en los países desarrollados existe una profundización en la tendencia de polarización de los mercados laborales, lo que genera grandes desigualdades de ingresos entre las personas. Un estudio sobre la tendencia del perfil del empleo en Argentina y Uruguay muestra un notable aumento de la importancia relativa de las tareas cognitivas y una reducción de las tareas manuales (Apella y Zunino, 2016). En este contexto, el acceso a las nuevas tecnologías y el desarrollo de habilidades duras (en ciencia, tecnología, ingeniería y matemática) y blandas (socio emocionales) se convierten en aspectos cruciales para la inserción laboral. Muchos países están reformulando sus políticas educativas para garantizar la formación continua que permita la readaptación (*re-skilling*) de sus trabajadores (Garnero, 2019). Un reciente estudio que caracteriza la demanda y oferta de habilidades laborales en los cinco países de la región (Argentina, Brasil, Chile y Colombia, México), confirma que, actualmente, 3 de cada 10 empresas enfrentan carencia de habilidades STEM y socioemocionales en su dotación de personal y 6 de cada 10 reconoce que en los próximos años su demanda de este tipo de habilidades crecerá (Basco, De Azevedo, Harracá y Kersner, 2019).

---

6 Sistemas ciberfísicos de integración; máquinas y sistemas autónomos (robots); internet de las cosas (IoT); manufactura aditiva (impresión 3D); *big data* y análisis de macrodatos; computación en la nube; simulación de entornos virtuales; inteligencia artificial; ciberseguridad; y realidad aumentada, entre otras.

Gráfico 6. Mi educación me permite estar preparada/o para los trabajos del futuro. Brecha de género por países



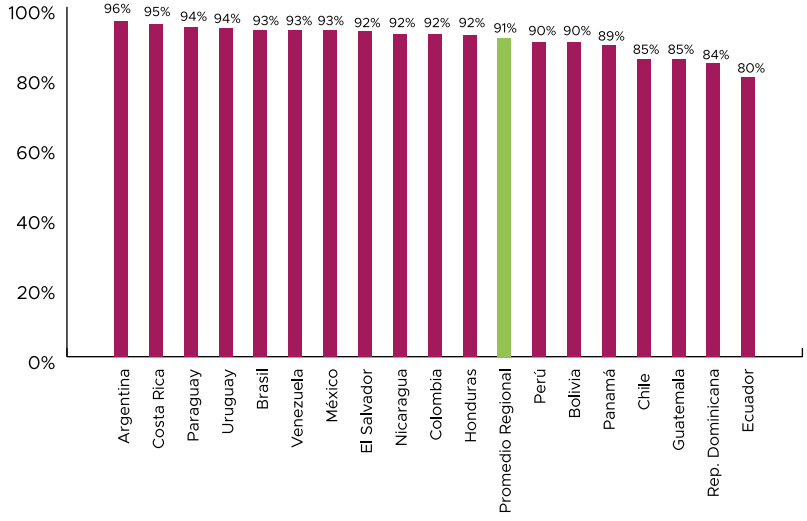
Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

En este contexto, llama la atención que el 66% de la población de América Latina confía en tener las habilidades necesarias para integrar la oferta laboral que exigen los trabajos del futuro. En los extremos se destacan República Dominicana, donde el 78% de la población se considera preparada, y Uruguay, donde sólo el 49% cree tener estas habilidades. En 13 de los 18 países de la región, las mujeres se perciben menos preparadas; el 64% de las latinoamericanas dijo que su educación le permite estar preparada para los trabajos del futuro (vs. 68% los hombres), lo que da lugar a una brecha de género de 4 puntos (ver Gráfico 6). México es el país que exhibe la mayor diferencia entre mujeres y hombres (11 puntos porcentuales), seguido por Uruguay (8 puntos porcentuales). En cambio, en Brasil, Costa Rica, República Dominicana y Ecuador, las mujeres se muestran más confiadas que los

hombres en relación con sus habilidades y con los desafíos laborales del futuro.

Asimismo, 4 de cada 10 personas reconocieron interés por aprender más habilidades asociadas a las nuevas tecnologías (computación, programación) y así lograr una mejor preparación para los trabajos del futuro. Sin embargo, en este caso las diferencias por género no son tan pronunciadas: se destaca apenas una brecha de 2 puntos porcentuales (42% de los hombres vs. 40% entre las mujeres).

Gráfico 7. Las mujeres tienen las mismas capacidades que los hombres para la ciencia y la tecnología (% de población de acuerdo por país)



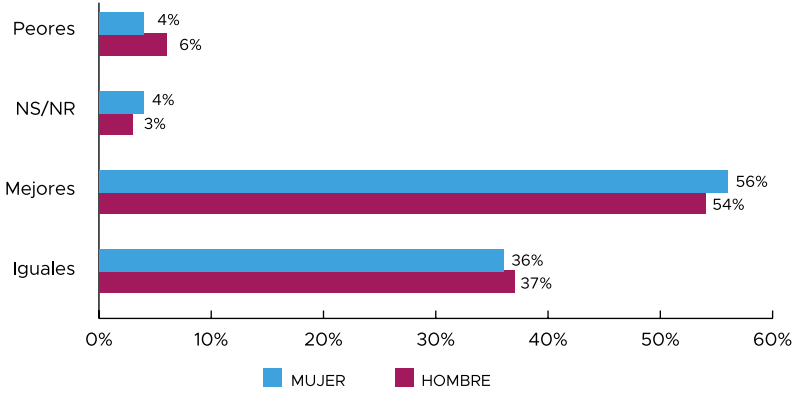
Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

Afortunadamente, 9 de cada 10 personas considera que las mujeres tienen las mismas capacidades en ciencia, tecnología e innovación que los hombres. En algunos países, como Argentina y Costa Rica, prácticamente la totalidad de la población está de acuerdo con la igualdad de capacidades (ver Gráfico 7). Se destaca que incluso en Ecuador –que

muestra el nivel mínimo–, 8 de cada 10 personas reconocen la igualdad de capacidades.

Se consultó, además, si consideran que los equipos de trabajo con diversidad de género pueden dar resultados distintos a los equipos de trabajo conformados únicamente por hombres[7]. La mayoría considera que los equipos integrados por mujeres y hombres pueden dar mejores resultados (55% en promedio), y otro gran porcentaje considera que no habrá diferencia entre los resultados (36% en promedio), pero no se encontraron diferencias significativas en las respuestas por género (ver Gráfico 8). Los países más convencidos de que los equipos de trabajo integrados por hombres y mujeres lograrán mejores resultados son Venezuela y República Dominicana (70%) y los menos convencidos son Nicaragua y El Salvador (43% y 42%, respectivamente).

Gráfico 8. Performance de un equipo de trabajo formado por hombres y mujeres. Promedio regional por género



Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

7 P43N ¿Cree que un equipo de trabajo formado por hombres y mujeres tendrá mejores (1) o peores (2) o (3) iguales resultados que un equipo formado solo por hombres?

4. Los niños y las tecnologías digitales

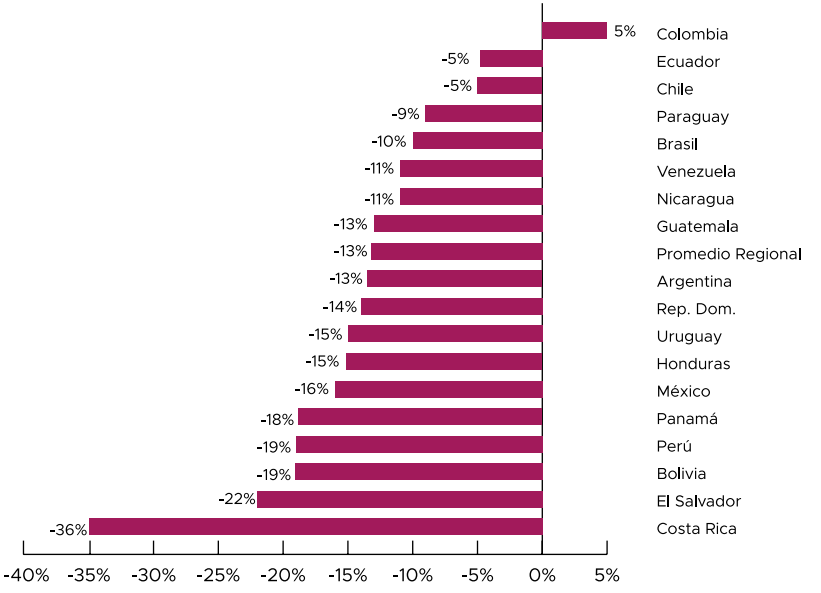
Según diversas estimaciones, más de la mitad de los niños que hoy se encuentran en el nivel primario se ocuparían en trabajos que aún no existen[8]. La flexibilidad de las personas para aprender continuamente y la capacidad de adaptación a condiciones tecnológicas siempre cambiantes representan activos decisivos en el actual paradigma productivo (Garnero, 2019). Por lo tanto, desde la primera infancia y a lo largo de vida, las personas deben lograr acumular capital humano para el desarrollo de habilidades acordes a las ocupaciones del futuro.

En plena era de la digitalización, no hay un consenso universal sobre las repercusiones del avance de las nuevas tecnologías sobre el bienestar de los niños (Unicef, 2017). Entre los aspectos positivos, se destacan el potencial de internet y las ofertas de ocio digital para estimular la creatividad de los niños mediante el acceso a contenidos de calidad; plataformas digitales para facilitar el aprendizaje en instancias de formación; redes sociales para potenciar la libre expresión de ideas, para la socialización y para la denuncia de abusos, etc. Entre los aspectos negativos, preocupan la «adicción a la pantalla» de los niños y la dependencia digital; la propagación de discursos de odio y de contenidos negativos que puedan manipular los valores sociales; el uso de la información para potenciar redes delictivas y explotación de los derechos de los niños, etc. (Unicef, 2017). Al mismo tiempo, entre la población joven y adulta, la ludificación, el uso de celulares y dispositivos móviles y nuevas modalidades de capacitación *online* se han convertido en aliados estratégicos en los nuevos diseños y modalidades formativas (Garnero, 2019).

---

8 Por ejemplo, la consultora argentina Scoop Consulting estimó que el 65% de los niños que empezaron la escuela primaria en 2017 dedicarán su carrera profesional a puestos de trabajo inexistentes en la actualidad.

Gráfico 9. Es importante introducir a los niños a las nuevas tecnologías desde una edad temprana. Brecha de género por países en el nivel de acuerdo con esta idea

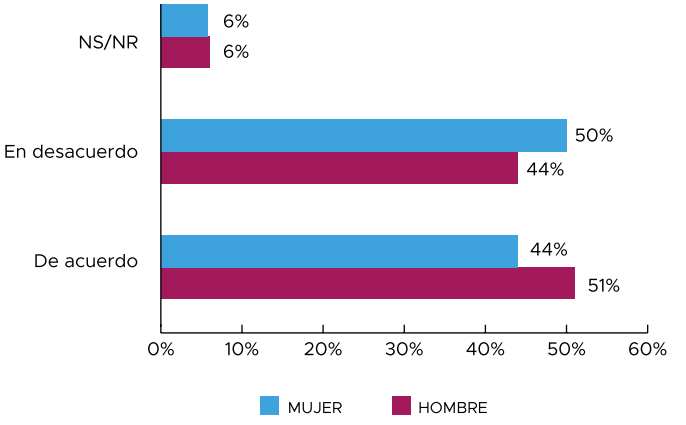


Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

En este contexto, se indagó acerca de la importancia de introducir a los niños a las nuevas tecnologías desde una edad temprana. En promedio, el 60% de la población regional dijo estar de acuerdo, el 35% se mostró en desacuerdo y el 5% no supo o no pudo responder. Al analizar las respuestas por género, sorprendió que más hombres que mujeres se mostraran de acuerdo con esta idea (67% vs. 53%). La brecha de género, que promedia 13 puntos, muestra picos máximos en Costa Rica (36 puntos porcentuales) y grandes magnitudes en El Salvador, Bolivia y Perú (cercanas a 20 puntos) (ver Gráfico 9). Colombia es el único país donde más mujeres que hombres apoyan la introducción de tecnologías desde la edad temprana.

Se consultó también si se sentirían cómodos con que sus hijos reciban clases a través de la web; otra vez se encontró una mayor resistencia entre las mujeres que entre los hombres, y una brecha de género de -7 puntos porcentuales (ver Gráfico 10).

Gráfico 10. Se sentiría cómodo si sus hijos recibieran clases a través de la web. Promedio regional por género



Fuente: elaboración propia sobre la base de los datos de INTAL-Latinobarómetro 2018.

5. El comercio electrónico

Existe literatura que evidencia que el comercio electrónico podría ayudar al empoderamiento económico de las mujeres, al permitir que las personas puedan elegir de manera más flexible dónde, cómo y cuándo trabajar. Estas condiciones pueden aumentar el empleo femenino, al permitirles combinar las responsabilidades laborales con las familiares, que de forma generalizada recaen más sobre las mujeres que sobre los hombres.

En algunos casos, este medio puede eliminar las interacciones cara a cara o enmascarar el género de las partes relevantes y así limitar las posibilidades de discriminación por género. Según un informe de la ICT[9] de 2016, las micro y pequeñas empresas administradas por mujeres informaron que cuando se trata de cumplir con las normas y regulaciones, un proceso que a menudo involucra múltiples interacciones cara a cara, el «comportamiento discriminatorio de los funcionarios» es un problema importante (en comparación a lo reportado por empresas administradas por hombres). Estas interacciones son cada vez menos necesarias en el comercio electrónico (Barral y Barafani, 2020).

Debido a estas ventajas, las pequeñas y medianas empresas (pymes) lideradas por mujeres ya están aprovechando este canal de comercialización. Mientras en el medio tradicional solo el 25% de las pymes están lideradas por mujeres, en el comercio electrónico esta proporción se duplica (Gaitan, 2018). En la reciente encuesta «The Future of Business Survey», elaborada por Facebook, la OCDE y el Banco Mundial[10], se observa que en Argentina, Brasil y Chile, más del 30% de estos negocios son propiedad o administrados mayoritariamente por mujeres, y valores cercanos al 26% se observan en Colombia, México y Perú[11].

A pesar de los beneficios del comercio electrónico para la mujer, existe también evidencia que indica que la discriminación por género está presente en las interacciones comerciales *online,* que parecían ser neutrales. Un estudio de caso que analiza las interacciones en eBay encuentra que las mujeres tienden a recibir una menor cantidad de

---

9 e-trade for Women: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-eTrade-for-Women.aspx.

10 La encuesta pregunta sobre las percepciones, desafíos y perspectivas de las pequeñas y medianas empresas que están presentes en internet en 33 países.

11 La definición está basada en «al menos el 65% de los miembros son mujeres».

ofertas y un pago menor en los procesos de subasta de bienes idénticos (Kricheli-Katz y Regev, 2016). Los autores muestran que las mujeres vendedoras reciben 80 centavos por cada dólar que recibe un hombre cuando vende productos nuevos idénticos en eBay y 97 centavos cuando vende el mismo producto usado. Por su parte, Adams-Prassl (2019) documenta, usando información de más de 2 millones de tareas completadas en un popular mercado laboral *on-line*, que allí la mujer gana un 20% menos por hora que los hombres; un resultado que no puede explicarse porque las mujeres seleccionan sistemáticamente tareas de menor valor. La autora proporciona evidencia de que la brecha salarial es atribuible a las diferencias en los patrones de trabajo de las mujeres con hijos y las responsabilidades de cuidado: tales mujeres tienen horarios de trabajo más fragmentados, que socavan su productividad. Así, incluso en un mercado que se supone bastante flexible y en ausencia de discriminación del empleador, las responsabilidades domésticas, que abrumadoramente recaen sobre las mujeres, afectan cómo ellas realizan su trabajo y, por lo tanto, cuánto ganan (Montserrat et al., 2019).

Lo cierto es que, según Latinobarómetro 2018, existe una brecha de género de 5 puntos porcentuales en la utilización del comercio electrónico: solamente el 23% de las mujeres realiza o le gustaría realizar este tipo de transacciones para comprar o vender, contra el 28% de los varones.

Pese a estos resultados, Kleinberg et al. (2018) son optimistas en cuanto al potencial de las interacciones digitales para reducir la discriminación. Según estos autores, los algoritmos tienen el potencial para fomentar nuevas formas de transparencia y, por lo tanto, oportunidades para detectar la discriminación que de otro modo no estaría disponible *off-line*. Esto implica que los algoritmos no solo son una amenaza, sino que, con las garantías/regulación adecuadas, pueden

ser una herramienta positiva para generar mayor equidad (Kleinberg et al., 2018). La clave está en definir e implementar esas garantías y regulaciones óptimas.

6. Entendiendo la brecha tecnológica

Ahora bien, ¿por qué razón las mujeres estamos menos predispuestas a incorporar nuevas tecnologías en nuestras vidas y nos sentimos menos preparadas para ello que los hombres?

Existe cada vez más literatura que trata de explicar estas brechas. La desconexión existente entre la educación y las competencias necesarias afecta más a las mujeres que a los hombres. Los sistemas educativos definen las normas de género, y las escuelas y las universidades no siempre brindan a las niñas un entorno propicio para el aprendizaje. Además, las mujeres tienden a estudiar en mayor medida carreras asociadas a educación, salud, bienestar, humanidades y artes (ITC, 2015). Un estudio realizado por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) muestra que los sectores de altas tecnologías, como el químico, eléctrico, de maquinaria y aplicaciones electrónicas, de maquinaria industrial y equipos de transporte, tienen un elevado impacto indirecto de exportaciones de servicios. Según dicho estudio, es necesario abordar la baja participación de las mujeres en las industrias de altas tecnologías, para mejorar la igualdad de género (UNCTAD, 2015). En una investigación realizada por el INTAL-BID al equipo del CET (Chicas en Tecnología), se concluyó que solo uno de cada tres estudiantes de carreras asociadas a CTIM en Argentina son mujeres.

Diferentes investigaciones muestran que las personas no están dispuestas a estudiar algo que no conocen, que no saben cómo funciona, que les resulta lejano. Muchas veces, eligen estudiar una carrera

universitaria sobre la base de estereotipos familiares y sociales, los cuales persisten a lo largo del período de formación, y se reproducen también en el ámbito profesional. Estereotipos que empujan a las mujeres a pensar que no son buenas para las matemáticas. Que las ingenierías y las carreras numéricas son para los hombres. Ajzenman y López Bóo (2019), por ejemplo, abordan la cuestión de las normas sociales y estereotipos en educación desde una perspectiva de género. Señalan que una mujer talentosa podría verse limitada a seguir una carrera en las áreas de CTIM si piensa que esto está mal visto, o si tiene arraigada la creencia de que las mujeres «no-son-buenas-en-eso».

Los «estereotipos de género» emergen como una expresión de la desigualdad; mientras que el rol de los varones se asocia al trabajo fuera del hogar («al proveedor de familia»), el de las mujeres aparece relegado al ámbito privado y a las tareas del hogar (D'Alessandro, 2017).

Durante la vida laboral, también se observan prácticas de segregación horizontal y laboral. Las mujeres padecen estructuras organizativas en donde prevalece el desequilibrio entre la vida personal y profesional. Espacios conquistados por una mayoría masculina, y donde no tienen posibilidad de entrar, es otra situación frecuente en el ámbito de las nuevas tecnologías. En particular, en este campo se utilizan metáforas como «tubería con fugas» (*leaky pipeline*, en inglés) para describir cuando las mujeres inician un recorrido educativo o profesional, pero poco a poco lo van dejando por razones personales, o debido a barreras institucionales, estereotipos y otras formas de discriminación. Las mujeres experimentan el deslizamiento de los llamados «pisos pegajosos» –no pueden ascender en nuestra carrera profesional– y la dificultad para superar los «techos de cristal» –no pueden acceder a puestos jerárquicos–. Un relevamiento realizado por la CEPAL[12] en 72 grandes

12 Fuente: https://www.cepal.org/es/infografias/mujeres-en-puestos-de-alta-direccion-en-grandes-empresas-de-america-latina.

empresas de la región muestra que sólo 3 empresas (4%) contaban en el año 2015 con una mujer en cargo de directora general o presidenta; la representación de las mujeres en el directorio promediaba el 8% y la participación de las mujeres en los comités directivos, el 9%.

Un tema que no se puede dejar de mencionar está vinculado con las limitaciones de tiempo para la incorporación de nuevos conocimientos y habilidades. Si bien la economía del cuidado ha comenzado a valorarse e institucionalizarse, las mujeres siguen siendo las que proveen la mayor parte del trabajo no remunerado a nivel global (Barral Verna y Barafani, 2020). La distribución en el interior de los hogares continúa siendo una fuente importante de desigualdad pese a los avances en términos de corresponsabilidad masculina en el hogar y de participación laboral de las mujeres (OIT, 2019b). Un informe de la OIT (2018) indica que, globalmente, las mujeres llevan a cabo la mayor carga horaria de trabajo no remunerado, lo que representa el 76,2% del total horario. Según la CEPAL (2018), América Latina no escapa de estas tendencias mundiales, dado que el 77% del trabajo no remunerado es realizado por las mujeres.

Frente a este escenario, la desigualdad digital, que ya era evidente en la era pre-pandemia, crecerá en la era post-pandemia, y ensanchará la brecha laboral. Es evidente que hoy las mujeres se ocupan aún más de las tareas del hogar y de los hijos, por lo que enfrentan mayores dificultades para dedicarse al trabajo remunerado o para incorporar nuevas habilidades. Al 30 de marzo de 2020, según datos de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco), 37 países y territorios de América Latina y el Caribe han cerrado sus escuelas a nivel nacional (Unesco, 2020). Ello implica que al menos 113 millones de niñas, niños y adolescentes se encuentran en sus casas para prevenir la expansión del virus. Los cierres de estos centros de enseñanza suponen que debe brindarse más atención

a esta población, lo que sin duda sobrecarga el tiempo de las familias; en particular, el de las mujeres, que en la región dedican diariamente al trabajo doméstico y de cuidados no remunerados el triple del tiempo que dedican los hombres a las mismas tareas (CEPAL, 2019).

Con la crisis, se hace más notoria la brecha de capacidades en el uso de las tecnologías de la información y las comunicaciones necesarias para implementar la educación a distancia, así como en las habilidades que poseen tanto los profesionales de la educación como los padres, las madres y los estudiantes. Este es un desafío pendiente en la región, especialmente en el caso de las mujeres de los estratos de menores ingresos (CEPAL, 2020).

En el actual contexto de avance de la digitalización y en un mundo que será atravesado e impactado por las desigualdades que traerá aparejada la pandemia, es fundamental promover diferentes tipos de políticas para que disminuya la brecha digital de género.

En prácticamente todas las economías del mundo, las mujeres obtienen menor paga por su trabajo que los hombres; en América Latina y el Caribe, las mujeres perciben –en promedio– el 83% de lo que perciben los hombres, e incluso el 75% de lo que perciben los hombres cuando se comparan personas con igual cantidad de años de estudio (CEPAL, 2016). ¿Acaso las latinoamericanas participan menos que los hombres en los sectores más productivos de la economía regional? ¿Hay brecha de habilidades que justifique la diferencia en las remuneraciones que perciben mujeres y hombres? ¿Hay sesgos de comportamiento que condicionen la «vocación» de las mujeres que generan una menor inclinación hacia carreras duras?

Necesitamos políticas públicas que contribuyan a disminuir la brecha salarial y ocupacional de género, como por ejemplo aquellas que: redistribuyan el trabajo doméstico y el cuidado no remunerado que realizan mayormente las mujeres; contribuyan a conciliar la vida

familiar y laboral; fortalezcan la seguridad de los ingresos de las mujeres a lo largo de toda su vida; y promuevan mecanismos para alentar la contratación de mujeres y fortalezcan la perspectiva de género en políticas de empleo y educación.

También, por supuesto, medidas que ayuden a acortar en forma directa la brecha digital de género: becas para mujeres en ciencia y tecnología; educación digital para las niñas; acciones para promover un efecto aspiracional hacia las carreras asociadas a CTIM con mujeres como modelos referenciales; y cupos en las empresas y en la administración pública para trabajadoras con habilidades asociadas a CTIM.

Y frente a la pandemia, debemos evitar que las mujeres sean un factor de ajuste por parte del Estado para hacer frente a las crisis económicas, es decir, que posibles medidas de reducción del déficit público afecten políticas públicas y programas sociales vinculados a la disminución de la brecha de género.

Conclusiones

El progreso tecnológico está configurando nuevos mercados laborales, donde los atributos tradicionalmente asociados a la fuerza de trabajo masculina, como la fuerza, pierden importancia frente a otras habilidades, como la comunicación, la inteligencia emocional, la flexibilidad, la creatividad, etc. Todos estos atributos, que por el momento no pueden ser encontrados en máquinas, ni en los robots, ni en los algoritmos, son habilidades propias del ser humano, sin distinción de género. ¿Por qué las mujeres se muestran más reticentes a incorporar los avances tecnológicos en sus actividades cotidianas? ¿Tiene esto vinculación con el hecho de que las mujeres estudian menos carreras asociadas a las nuevas tecnologías? ¿Cuánto influyen aspectos vinculados a los mayores niveles de informalidad que tienen las mujeres

y al menor acceso a determinados activos como las mismas nuevas tecnologías?

Los datos disponibles parecen encontrar alguna relación entre la menor apertura por parte de las mujeres latinoamericanas a las tecnologías de la información y la comunicación con el hecho de que estudian menos carreras asociadas a las nuevas tecnologías. También influye el hecho de que las mujeres tienen menos dispositivos tecnológicos y utilizan menos internet y otras plataformas digitales, como el comercio electrónico.

Ahora bien, ¿es posible elegir lo que no se conoce? ¿Pueden las mujeres aceptar el avance tecnológico cuando no tienen acceso a muchas de las tecnologías que se ofrecen para educar a sus hijos, curar a los enfermos, incluso para gestionar cuentas bancarias (cuando muchas de ellas trabajan en la informalidad)?

Además de, por supuesto, factores estructurales que evidencian gran cantidad de restricciones que afectan más a las mujeres que a los hombres, existen sesgos y estereotipos de género que se van trasladando de generación en generación y llevan a una menor predisposición de las mujeres a seguir carreras vinculadas a CTIM y a acceder menos a las nuevas tecnologías.

Es por ello clave formular políticas públicas que contribuyan a disminuir la brecha de género, con especial énfasis en los aspectos digitales. Y es fundamental, también, continuar investigando, para entender las verdaderas bases, factores determinantes, de la menor apertura de las mujeres a esta revolución 4.0. Factores clave para evitar que la brecha de género se incremente y, por qué no, también, verlo como oportunidad, para que esta nueva era abra nuevos caminos para las mujeres latinoamericanas.

Referencias bibliográficas

Adams-Prassl, Abigail (2019). «The Gender Pay Gap in an Online Labour Market: The Cost of Multi-Tasking». Mimeo.

Ajzenman, N. y López Bóo, F. (2019). «Nudges para mejorar vidas. Intervenciones para el bienestar de los países en desarrollo». *Revista de Integración y Comercio* (I&C N°45, Año 23, Abril 2019). INTAL-BID.

Albrieu, Ramiro; Basco, Ana Inés; Brest-López, Caterina; De Azevedo, Belisario; Peirano, Fernando; Rapetti, Martín (2019). *Travesía 4.0. Hacia la transformación industrial argentina*. INTAL-BID, CIPPEC, UIA.

Apella, I. y Zunino, G., (2017). «Cambio tecnológico y mercado de trabajo en Argentina y Uruguay. Un análisis desde el enfoque de tareas». *Informes Técnicos* No 11. Banco Mundial.

Arntz, M., Gregory, T. y Zierahn, U. (2016), *The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis*. París: OECD Social, Employment and Migration Working Papers, No. 189, OECD Publishing.

Azar, P., Espino, A. y Salvador, S. (2009). *Los vínculos entre comercio, género y equidad. Un análisis para seis países de América Latina*. Capítulo Latinoamericano de la Red Internacional de Género y Comercio (LA-IGTN).

Banco Mundial (2016). *Informe sobre el Desarrollo Mundial 2016: dividendos digitales. Cuadernillo del Panorama General*». Washington, DC: Banco Mundial.

Barral Verna y Barafani (2020). *Comercio y género: una relación a distintas velocidades*, INTAL-BID.

Basco, A. (2017). *La tecno-integración de América Latina: instituciones, comercio exponencial y equidad en la era de los algoritmos)*. INTAL-BID.

Basco, A., Beliz, G., Coatz, D. y Garnero, P. (2018). *Industria 4.0: fabricando el futuro*. INTAL-BID, UIA.

Basco, A., De Azevedo, B., Harracá, M., Kersner, S. (2019), *América Latina en movimiento. Competencias y habilidades en la Cuarta Revolución Industrial*. ALAI, INTAL-BID.

Basco, A. y Garnero, P (2019). «Una visión a futuro. La opinión de los latinoamericanos sobre las nuevas tecnologías». *Revista de Integración y Comercio* (I&C N°45, Año 23, Abril 2019). INTAL-BID.

Basco, A. y Lavena, C. (2019). *Un potencial con barreras: la participación de las mujeres en el área de ciencia y tecnología en Argentina*. INTAL-BID.

CEPAL (2016). «Pese a avances en el nivel educacional de las mujeres, persiste brecha salarial de género en la región». Disponible en: https://www.cepal.org/es/comunicados/pese-avances-nivel-educacional-mujeres-persiste-brecha-salarial-genero-la-region.

CEPAL (2020). «La pandemia del COVID-19 profundiza la crisis de los cuidados en América Latina y el Caribe».

D'Alessandro, M. (2017). *Economía feminista. Cómo construir una sociedad igualitaria sin perder el glamour*. Buenos Aires: Editorial Sudamericana.

Frey, C. y Osborne, M. (2013). *The Future of Employment: How Susceptible are Jobs to Computerization?* Oxford: Oxford University Paper.

Garnero P (2019). «Oferta de capacitación para el desarrollo de habilidades laborales 4.0 en Argentina». *América Latina en Movimiento*, ALAI, INTAL-BID.

Mokyr, J., Vickers, C., & Ziebarth, N. L. (2015). «The history of technological anxiety and the future of economic growth: Is this time different?». *Journal of Economic Perspectives*, 29(3), 31-50.

ONU Mujeres (2015). «Hechos y cifras: empoderamiento económico». Disponible en: http://www.unwomen.org/es/what-we-do/economic-empowerment/facts-and-figures#notes.

O'Rourke, K. H. and Sinnott, R (2001). «The Determinants of Individual Trade Policy Preferences: International Survey Evidence». *Trinity Economics Papers* 200110, Trinity College Dublin, Department of Economics.

Pombo, C., Gupta, R. and Stankovic, M. (2018). *Servicios sociales para ciudadanos digitales: oportunidades para América Latina y el Caribe*. Banco Interamericano de Desarrollo.

Rifkin, J. (1996). *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: el nacimiento de una nueva era*. Editorial Booket.

Shauman, K. A. and Xie, Y. (1996). «Geographic Mobility of Scientists: Sex Differences and Family Constraints». Demography, 33(4): 455-468.

UNESCO (2017). «Women in Science». Fact Sheet No. 43. FS/2017/SCI/43. Disponible en http://uis.unesco.org/sites/default/files/documents/fs43-women-in-science-2017-en.pdf.

UNESCO (2020). «COVID-19 Educational Disruption and Response» [en línea] https://en.unesco.org/themes/education-emergencies/coronavirus-school-closures.

UNICEF (2017). «Estado Mundial de la infancia 2017. Niños en un mundo digital». Disponible en https://www.unicef.org/media/48611/file.

World Trade Organization (2017). Gender Aware Trade Policy: A Springboard for Women's Economic Empowerment.

ANA BASCO. Cuenta con más de 20 años de experiencia profesional en materia de integración e innovación tecnológica en América Latina y el Caribe. Especialista en Integración Regional en el Instituto para la Integración de América Latina y el Caribe (INTAL) del Banco Interamericano de Desarrollo (BID), donde se desempeña desde hace 14 años liderando proyectos en materia de comercio, industria 4.0, futuro del empleo y género.

Previa a su incorporación en el BID, se desempeñó como consultora en el Ministerio de Agricultura de Argentina, en la Secretaría de Transporte del mismo país y en organizaciones de la sociedad civil.

Licenciada en Economía de la Facultad de Ciencias Económicas y Licenciada en Ciencia Política de la Facultad de Ciencias Sociales, ambas de la Universidad de Buenos Aires, de Argentina. Posee una Maestría en Integración Económica Regional de la Universidad Internacional de Andalucía, en España, y un postgrado en Gestión de Negocios Internacionales de la Universidad de Georgetown, en Estados Unidos.

PAULA GARNERO. Especialista en Transformación Digital e Innovación. Se desempeña como consultora internacional, asesorando a gobiernos, organizaciones y empresas de Argentina y América Latina en el diseño e implementación de políticas, programas y hojas de ruta para la construcción de una economía más productiva, más inclusiva y con igualdad de género. Actualmente es asesora de la Secretaría de Asuntos Estratégicos de la Nación. Licenciada en Economía egresada de la Universidad Nacional de Buenos Aires y magíster en Economía de la Ciencia y la Innovación, de la Barcelona Graduate School of Economics. Se especializó en transformación tecnológica y su impacto en la producción y el trabajo, con títulos en Gestión de Tecnología e Innovación de la Universidad Nacional de Tres de Febrero, y en Mejora de la Productividad de las PyMEs, de Chu San Ren, Japón. Ha investigado y publicado sobre el impacto del cambio tecnológico y la configuración de nuevos paradigmas económicos, productivos y sociales. Acompaña a organizaciones en sus procesos de innovación y transformación digital, con particular énfasis en tecnologías de la industria 4.0.

CAPÍTULO 5

La gobernanza de internet en Argentina: espacios multisectoriales, desafíos y recomendaciones

Agustina Callegari

Introducción

La arquitectura técnica de internet, sumada a su caracterización como un bien público global, pone sobre la mesa la discusión sobre los mecanismos, procesos y políticas que configuran el desarrollo de la red. En este contexto, aparece en escena el concepto de gobernanza de internet.

La gobernanza de internet se ha convertido en el espacio de juego que permite esbozar una respuesta sobre cómo se gobierna la red o, mejor dicho, cómo se gestiona y administra. Sin un punto central ni una autoridad que lo gobierne como consecuencia de su arquitectura descentralizada, internet ha desarrollado un modelo de gobernanza basado en la coordinación de procesos de múltiples partes interesadas. Si bien la gobernanza de internet en términos estrictos comenzó como una forma de gestionar sus recursos críticos, como los protocolos y nombres y números de internet, el sentido amplio que se le ha

dado al concepto en la última década ha dado un marco para las discusiones sobre temas político-sociales. Entre ellos se encuentran temáticas como la protección de datos personales y privacidad en internet, la libertad de expresión *online*, la regulación de aplicaciones y la inclusión digital, por nombrar algunas.

A nivel internacional, y desde una concepción institucionalista, la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés), por un lado, y el Foro de Gobernanza de Internet (IGF, por sus siglas en inglés) impulsado por las Naciones Unidas (UN, por sus siglas en inglés), por el otro, se han convertido en los espacios formales de gobernanza de internet. La ICANN es el organismo que ha recibido y recibe mayor atención en el campo de la gobernanza de internet como una institución de gobernanza global y como gestora del manejo y asignación de los nombres de dominio y números, función que lleva a cabo desde 1998. Por su parte, el IGF, desde su primera edición en 2006, se ha convertido en el espacio multisectorial por excelencia para la discusión y debate sobre temas que van más allá de la coordinación técnica de recursos, pero donde no se toman decisiones vinculantes.

A partir de las revelaciones de Edward Snowden acerca de las prácticas de vigilancia masiva en internet llevadas a cabo por la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) del gobierno de los Estados Unidos, la gobernanza de internet comenzó a ocupar un lugar más amplio en las agendas políticas regionales. A excepción de Brasil, que ya contaba con un espacio multisectorial para la definición de principios y políticas de internet[1], este era un tema que se encontraba

1 El Comité Gestor de Internet en Brasil (CGI.br) fue creado en 1995 por una orden conjunta del entonces Ministerio del Estado de Ciencia y Tecnología y el Ministerio de Comunicaciones como un órgano de gobernanza de internet en Brasil.

relegado a discusiones entre académicos y miembros de las comunidades técnicas. En este contexto, y teniendo en cuenta la importancia creciente que internet adquiere para el desarrollo económico y social de los países, los procesos nacionales de su gobernanza, que resultan esquivos para muchos actores por la arquitectura transnacional de internet y la presencia de capas que resisten al control local, adquirieron relevancia. Las iniciativas nacionales de gobernanza tomaron en su mayoría la forma de foros de gobernanza de internet, siguiendo los lineamientos del IGF Global y de la Cumbre Mundial de la Sociedad de la Información (CMSI). En otros casos, la gobernanza de internet a nivel nacional se vio permeada por otro tipo de iniciativas, como grupos de trabajo, que tomaron algunas características de los procesos institucionales de su gobernanza.

En Argentina, la gobernanza de internet tomó impulso en 2014, con la participación del país en el evento internacional conocido como NetMundial[2] y con la creación ese mismo año de la Comisión Argentina de Políticas de Internet (CAPI) por la Secretaría de Comunicaciones, que, pese a su corta experiencia, representó el primer abordaje institucional de la gobernanza de internet en el país. Aunque Argentina ya participaba en foros relevantes en el tema desde 2005, fue a partir de ese momento que la cuestión ganó espacio en agenda pública y, sobre todo, interés de las partes interesadas. En los siguientes años, se formaron distintos espacios de gobernanza de internet de carácter institucional y multiactorales. El impulso por parte del gobierno de algunos de estos espacios y su participación en otros demostraron que

2 NetMundial (San Pablo, Brasil, abril de 2014) fue la conferencia mundial impulsada por Brasil para proponer una agenda para el futuro de la gobernanza de internet como consecuencia de las revelaciones de vigilancia masiva llevadas a cabo por la NSA del gobierno de los Estados Unidos.

la gobernanza de internet ganaba lugar en la agenda. Al mismo tiempo, actores no gubernamentales, como la comunidad técnica, el sector privado a través de cámaras y la sociedad civil, buscaron, y aún buscan, consolidar espacios de estas características para darles un marco a las discusiones sobre el desarrollo de internet en el país.

Desde las distintas ediciones del IGF de Argentina hasta el rol del dominio de nivel superior geográfico (ccTLD, por sus siglas en inglés) nacional, la participación argentina en foros internacionales y regionales, e incluso el impulso que algunos eventos latinoamericanos y globales llevados a cabo en territorio argentino dieron al tema, la experiencia nacional presenta características propias pero con desafíos similares a los que enfrentan estos procesos a nivel global. Hoy en día, la gobernanza de internet ha perdido fuerza a nivel nacional, tanto por cuestiones del contexto político económico nacional como también por efecto de los desafíos que la gobernanza de internet presenta mundialmente.

En este sentido, este trabajo busca abordar la gobernanza de internet desde la perspectiva de los procesos nacionales de Argentina. Para ello, el artículo se estructura en tres partes. En el primer capítulo se caracteriza la gobernanza de internet desde un punto de vista conceptual, a la vez que se le da un marco a la aparición de espacios nacionales. Este último punto es de importancia para el segundo capítulo, que realiza un recorrido por los principales hitos de la gobernanza de internet en Argentina, desde los espacios académicos y técnicos de los años sesenta hasta el surgimiento de espacios de gobernanza institucionales en el nivel local entre 2014 y 2019. En la tercera sección se busca mirar la escena internacional para entender los desafíos de la gobernanza de internet, pero también sus aspectos positivos. Por último, teniendo en cuenta lo anterior, se presentan recomendaciones para mejorar este tipo de procesos en el país, con el

fin de maximizar las ventajas que el modelo ofrece para el desarrollo de internet en el país.

1. A qué se llama gobernanza de internet

Definir la gobernanza de internet no es tarea sencilla, debido a que el concepto adquiere diferentes alcances y presenta ambigüedades. Diferentes autores se han enfocado en abordar su definición tanto en términos semánticos como con la intención de definir su campo de acción. En esta sección se presentan algunas de las definiciones de gobernanza de internet realizadas por académicos en la materia y la definición adoptada en la Agenda de Túnez en el marco de la CMSI en 2005, que ha dado pie a la creación de espacios regionales y nacionales de gobernanza de la red.

Mientras que para Jeanette Hofmann (2005) la gobernanza de internet puede ser entendida como un proceso abierto y colectivo de búsqueda que tiene como fin llenar un «vacío regulatorio» –tanto conceptual como institucional– de una manera legítima en el ámbito de internet, para Milton Mueller (2010), la gobernanza de internet es la etiqueta más simple, directa e inclusiva para referirnos al conjunto de disputas y deliberaciones sobre cómo se coordina, se gestiona y se configura la red para reflejar políticas. En la misma línea, para Carlos Cortés (2014), puede visualizarse como un campo de disputa en el que se ponen en juego el qué, el cómo y el quién del control de internet.

Los niveles analíticos de estas conceptualizaciones tienen su contrapartida en una definición más descriptiva y normativa que analítica (Aguerre, 2015): la adoptada en el contexto de la CMSI. Allí, en el marco de Agenda de Túnez para la Sociedad de la Información (2005), se define la gobernanza de internet como «... el desarrollo y aplicación de los gobiernos, el sector privado, la sociedad civil, en sus respectivos

roles, de principios, normas, reglas y procedimientos que moldean la evolución y el uso de Internet». El proceso de esta definición y su texto en sí mismo han llevado al estudio dentro de la gobernanza de internet de la CMSI y del IGF como entidades o espacios formales (DeNardis, 2010). Asimismo, es la definición más citada como punto de partida en la literatura en el tema y en espacios internacionales y locales.

La definición de la CMSI destaca uno de los temas más debatidos desde el surgimiento de internet: la presencia y el rol de diferentes actores en el ecosistema de la red o, en otras palabras, lo que se conoce como gobernanza de múltiples partes interesadas[3]. Este abordaje adquiere relevancia en un contexto en el que la mayoría de las funciones de la gobernanza de internet no han sido de dominio de los gobiernos, sino que han sido ejecutadas a través de órdenes privadas, diseño técnico y nuevas formas institucionales (DeNardis, 2010). De esta forma, la gobernanza de internet no involucra solamente gobiernos, sino que coloca en una especie de «pie de igualdad» a actores clave para el desarrollo de la red, ratificando la posición de actores no estatales en dicho proceso y colocando prácticamente todos los problemas de comunicación e información en este marco (Van Eeten y Mueller, 2013).

El concepto de gobernanza y su no tan clara relación con el término «gobierno» (Hofmann, 2016), muchas veces utilizados como sinónimos, agregan una mayor complejidad al análisis y requieren de contextualización. Tal como señala Petros Iosifidis (2011), la diferencia entre gobernanza y gobierno radica en la fuente que ejerce el poder: el Estado es el principal actor en la acción de gobernar, mientras que la gobernanza involucra a varios agentes e implica un poder compartido.

---

3 Si bien la traducción no es exacta, este trabajo utiliza las palabras «múltiples partes interesadas», «multiactoral», como traducción del término en inglés, *multistakeholder*.

Esta idea de poder compartido que el concepto de gobernanza de internet trae consigo se encuentra, de esta forma, en pugna con la idea tradicional de que las políticas se definen unilateralmente por parte del Estado (Aguerre, 2017).

Por el cambio de enfoque que la gobernanza de internet propone en su gestión y coordinación, su carácter multiactoral es uno de los aspectos más mencionados, tanto en bibliografía sobre la temática como en foros y espacios. Como señala Cortés (2014), cuando se discute la gobernanza de internet en espacios internacionales, y como veremos también en los foros nacionales, es común que se enuncie el modelo de múltiples partes interesadas como el camino a seguir, sin tener en cuenta el fin al que se busca llegar. En esta línea, el autor sostiene que la gobernanza de internet puede convertirse en una «trampa de las formas», por los problemas que genera ver el multisectorialismo de la gobernanza de internet desde una perspectiva idealista. Esto se debe a que la dimensión multiactoral de la gobernanza de internet a menudo se eleva como un valor en sí mismo, antes que como un posible acercamiento a las problemáticas más relevantes en torno a internet (DeNardis y Raymond, 2013).

Desde una perspectiva más positiva, adoptada por diversos autores, Hofmann (2016) argumenta que el concepto de múltiples actores es un imaginario que proporciona significado y regularidad a un mundo fragmentado y desordenado: muestra el panorama de la gobernanza de internet de una manera coherente y que promueve la legitimación (Hofmann, 2016). Para la autora, la narrativa de múltiples actores no solo representa la realidad, sino que también genera expectativas, objetivos, nuevas categorías y puntos de referencia. En esta línea, el concepto de múltiples actores se vuelve para Hofmann performativo y, para dar sustento a su teoría, da cuenta de cómo organizaciones como la ICANN llevan estos procesos participativos a la realidad (Hofmann,

2016). Para De la Chapelle (2012), también desde una visión positiva de los procesos multisectoriales, la ICANN, así como también el ya mencionado IGF, son dos laboratorios que trabajan para llevar el principio de la multisectorialidad a un proceso concreto para el debate y formación de políticas de internet.

En este punto, cabe detenernos en el IGF, uno de los espacios más reconocidos de gobernanza de internet a nivel global y que también ha dado impulso a muchas de las iniciativas regionales y nacionales en relación con el tema. Esto se debe a que la Agenda de Túnez no solo definió el concepto de gobernanza de internet y creó el IGF global, sino que alentó el desarrollo de procesos a nivel regional y local. Si bien existe mucha bibliografía que da cuenta de procesos de gobernanza de internet a nivel global, los procesos nacionales no han sido tan estudiados (Aguerre et al., 2018). Recién adquirieron relevancia en los últimos años, con el fin de abordar el rol que las iniciativas nacionales juegan para legitimar los procesos multiactorales de gobernanza de internet a nivel local, en un contexto en el que, como se verá más adelante, el IGF global presenta signos de fatiga.

Teniendo en cuenta las definiciones sobre gobernanza de internet antes expuestas en este trabajo, aunque existen diferentes puntos de vista, se puede caracterizar la misma como procesos, actores e instituciones que buscan moldear las discusiones y las políticas vinculadas al desarrollo de internet. Aunque para algunos autores no se puede perder de vista la lucha de poder que existe entre actores, el foco que ha puesto en el carácter institucionalista de la gobernanza de internet nos da un punto de partida para abordar el caso argentino.

2. Gobernanza de internet en la Argentina

El desarrollo de internet es el elemento estructurador más relevante para entender la gobernanza de internet a nivel nacional, ya que,

pese a la naturaleza transfronteriza y descentralizada de la red, cada país la adoptó de forma diferente. En Argentina, el debate en torno a la gobernanza de internet adquirió relevancia en los últimos años. Sin embargo, el desarrollo de internet en Argentina no es nuevo y se remonta al desarrollo de la informática a nivel nacional, que comienza en la década del 60 en la Facultad de Ciencias Exactas y Naturales (FCEyN) de la Universidad de Buenos Aires (UBA). Desde allí, un grupo de investigadores impulsó diversas actividades vinculadas a la computación y al desarrollo de redes informáticas: la formalización de la carrera de Ciencias de la Computación, la adquisición de la primera computadora científica de la Argentina –Clementina– y la red de servicio de correo electrónico son algunos de los hitos que llevaron a que el país se conectara a internet por primera vez.

El 8 de abril de 1994, casi cuatro años después que en otros países de la región, se realizó la primera conexión a internet. Ese día, las universidades argentinas se conectaron por primera vez a internet a través de un enlace digital de Telintar, el brazo internacional de Telecom y Telefónica, colocado en la Universidad de Buenos Aires (Dunayevich et al., 2019). Desde ese momento, se fueron agregando nuevos enlaces, no solo en universidades sino también en organismos estatales, como la Cancillería y la entonces Secretaría de Ciencia y Técnica. Así, internet, que se impulsó desde el ámbito académico, comenzó a abrirse a nuevos actores, aspecto que se consolidó en 1995 con su despliegue desde un punto de vista comercial y con la privatización de Entel en 1997.

Otro aspecto central para el desarrollo de internet en Argentina, y también para entender el ecosistema de actores en torno al mismo, fue la asignación del dominio superior de código país (ccTLDs, por sus siglas en inglés) «.ar» y el rol de la Cancillería. El registro de dominio alto nivel para el país («.ar») se orquestó desde el ámbito académico en

1987 con el fin de poder comunicarse con el exterior vía correo electrónico. El primer dominio que se creó fue «mrec.ar», para el Ministerio de Relaciones Exteriores y Culto (Cancillería), organismo que tomó el papel de registrar todos los dominios «.ar» que se asignaban en el país. Este hecho puso sobre la mesa diferentes opiniones sobre quién debía gestionar el registro, es decir, sobre su modelo de gobernanza. En ese momento había dos posiciones distintas. Por un lado, el sector académico argumentaba que dicha gestión debía permanecer a su cargo. Por el otro, la Cancillería hacía hincapié en que era el Estado quien debía hacerse cargo de dicha gestión, entre otras cosas, porque el «.ar» es parte de la identidad regional. Finalmente, fue esta última posición la que se adoptó (Dunayevich et al., 2019). Unos meses antes de la primera conexión a internet, se creó el Centro de Información de la Red para Argentina (Nic.ar, por sus siglas en inglés) bajo el mandato de este organismo estatal, que consolidó un modelo de gobernanza de uno de los recursos críticos de internet bajo la órbita del Estado. El caso argentino sentó un precedente a nivel internacional y se diferenció de lo que ocurría en otros países de la región en cuanto a la gestión de los ccTLD, que eran administrados en la mayoría de los casos por el sector académico y por privados.

Aunque la Cancillería tenía un rol central en la gestión del «.ar», no fue hasta la segunda parte de la CMSI, en 2005[4], que el país adoptó una posición más activa en espacios internacionales en materia de internet. Durante la reunión llevada a cabo en Túnez, donde –como fue señalado antes– se adoptó la primera definición de gobernanza de internet, la delegación argentina participó activamente. Como explica Carolina Aguerre (2017), aunque la participación argentina en

4 La Cumbre Mundial de la Sociedad de la Información tuvo dos encuentros: Ginebra en 2003 y Túnez en 2005.

la reunión tuvo poco impacto en las políticas internas relacionadas con internet, logró posicionar a la Cancillería como el sector estatal responsable de dar seguimiento a estos temas. De esta forma, representantes de este organismo comenzaron a participar activamente en reuniones vinculadas a la gobernanza de internet, como las reuniones de la ICANN y en el IGF.

Además del rol del Estado en la gestión del «.ar» y de su participación en espacios internacionales, a partir de 2006, el Estado asumió un rol en el área de las políticas nacionales de internet. Desde la creación de Arsat (2006) como empresa estatal para desarrollar servicios de comunicación satelital, hasta el Plan Nacional Argentina Conectada de inversión en fibra óptica y la sanción de la Ley Argentina Digital (2012) de servicios de telecomunicaciones, el Estado comenzó a actuar no solamente como el regulador, sino también como proveedor de servicios en el sector de las comunicaciones (Aguerre, 2017). Sin embargo, la temática de la gobernanza, que desde los inicios de internet se llevó a cabo de forma informal a través de mecanismos de coordinación entre actores involucrados, apareció en la agenda pública recién en 2014.

La creación, en abril de 2014, de la Comisión Argentina de Políticas de Internet (CAPI) en el ámbito de la Secretaría de Comunicaciones, al mismo tiempo que el país participaba de la reunión NetMundial, que surgió como respuesta del gobierno de Brasil y otros sectores a las revelaciones de espionaje de Snowden, puso en escena el creciente interés del Estado en esta temática. La CAPI tenía como objetivo particular diseñar una estrategia nacional sobre internet y su gobernanza, así como también buscaba contribuir a una mayor representación del país en foros y organismos internacionales. Aunque solo se reunió en algunas ocasiones, se convirtió en el primer intento institucional de formalizar un proceso de gobernanza de internet, desde una perspectiva multiactoral, impulsado por el Estado.

La participación de Argentina en los foros internacionales adquirió más fuerza entre 2013 y 2015, cuando el país fue sede de algunas de las reuniones regionales y globales más relevantes del ecosistema. En agosto de ese año, Córdoba recibió a la Reunión Regional Preparatoria para el Foro para la Gobernanza de Internet (LACIGF) y en noviembre, el Nic.ar apoyó la organización de la Reunión Nº 48 de la ICANN, realizada en la ciudad de Buenos Aires. La ICANN (Nº 53) volvió a la ciudad de Buenos Aires en 2015, cuando el tema de la gobernanza de internet ya comenzaba a adquirir mayor peso en la agenda local. La reunión contó con una participación activa de actores locales de distintos sectores, que hasta entonces venían coordinando de manera informal, pero que empezaron a analizar la necesidad de que Argentina contara con un espacio de coordinación constante para estos temas –como ya estaba sucediendo en otros países de la región. La idea terminó de consolidarse ese año durante la reunión del LACIGF en México, donde comenzaron los preparativos para organizar el primer evento nacional de gobernanza de internet en octubre de 2015.

El Diálogo Argentino para la Gobernanza de Internet (renombrado Foro de Gobernanza de Internet de Argentina a partir de su formalización en 2016), organizado por un grupo de personas involucradas[5] en foros regionales y globales sobre el tema, se constituyó como el primer espacio institucional impulsado por participantes de distintos sectores. Para su organización, se creó un Comité multisectorial y se convocó a una reunión abierta, con el fin de definir los temas centrales del evento. Incluso, a través de los apoyos obtenidos para la organización, otorgó becas para que participantes de otras provincias argentinas pudiesen asistir al foro, llevado a cabo en la ciudad de Buenos

5 La autora de este artículo formó parte del Comité organizador del IGF en 2015, 2016 y 2017.

Aires. El evento consiguió poner el tema en la agenda pública, en un período de transición y cambio de gobierno.

En este contexto, varios de los actores participantes del evento pasaron a cubrir cargos públicos nacionales y comenzaron a impulsar el tema desde el Ministerio de Modernización (Aguerre, 2017). El proceso del diálogo, que tuvo apoyo del gobierno en los años siguientes y logró consolidarse como un espacio multisectorial con todos los actores involucrados, fue renombrado como Foro de Gobernanza de Internet de Argentina y tuvo ediciones en 2016, 2017, 2018 y 2019, y al momento de redacción de este artículo se encuentra pensando una alternativa *online* para 2020. Aunque cada año el IGF Argentina tuvo características diferentes, todas las ediciones mantuvieron el carácter multisectorial y participativo, al contar con representantes de todos los sectores involucrados en el comité multisectorial y durante las discusiones del evento. Sin embargo, desde sus inicios se ha enfrentado a desafíos para lograr una participación significativa de todos los sectores en todas las instancias, para incluir nuevas voces y así federalizar el debate y, sobre todo, para mostrar conexiones con políticas concretas posteriores al evento. Aunque puede ser que al foro le falte maduración, este punto es siempre contemplado por el comité multisectorial como algo que se busca alcanzar.

Como se mencionó anteriormente, la gobernanza de internet adquirió relevancia en la agenda pública a partir de diciembre de 2015. Si bien en materia de políticas y regulación de internet hay muchos aspectos que se podrían analizar en este período –desde los intentos por la Ley de Convergencia del ENACOM, los planes de País Digital, la Agenda Digital, hasta diferentes iniciativas de la Secretaría de Comunicaciones–, desde una perspectiva multisectorial e institucionalista de la gobernanza de internet, hay dos iniciativas en las que es importante detenerse. En primer lugar, los intentos de formalizar

grupos de trabajo multisectoriales impulsados desde el Ministerio de Modernización y de Comunicaciones y, en segundo lugar, el papel del Nic.ar durante estos años.

Dentro del Ministerio de Modernización, y como parte de la entonces Secretaría de Innovación y Gestión Pública, se creó la Dirección Nacional de Políticas y Desarrollo de Internet, con el objetivo de implementar e impulsar iniciativas de gobernanza de internet en la Argentina. El año en que la Dirección Nacional se enfocó en este tema[6], apoyó la organización del IGF Argentina y creó el Grupo de Trabajo Multisectorial de Gobernanza de Internet[7]. Al igual que la CAPI, aunque por distintos motivos, el Grupo de Trabajo no logró sostenerse en el tiempo. Esta vez, la estructura del Estado que se había creado al comienzo de la gestión fue modificada y la Secretaría de Comunicaciones, que ya impulsaba el tema de gobernanza de internet a través de otro espacio, los Grupos de Trabajo de Servicios de Internet[8], consolidó el tema bajo su órbita. En este contexto, la Secretaría de Comunicaciones, entre 2016 y 2019, no solo llevó a cabo consultas públicas en temas de internet de las cosas y espectro, sino que también participó activamente en diferentes espacios nacionales (en el comité del IGF nacional) e internacionales de gobernanza de internet (con un rol en el Grupo Asesor Multisectorial –MAG, por sus siglas en inglés–, del IGF Global).

El Nic.ar, al administrar el ccTLD nacional y teniendo en cuenta el lugar que los llamados recursos críticos de internet han tenido

---

6 A partir de 2017, la Dirección se enfocó en otra de sus funciones: las iniciativas de inclusión digital.

7 argentina.gob.ar/noticias/se_presento_el_grupo_de_trabajo_multisectorial_sobre_internet.

8 Los Grupos de Trabajo de Servicios de Internet fueron creados por Resolución 8/2016 del Ministerio de Comunicaciones http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=265591.

históricamente en la gobernanza de internet, se ha convertido en los últimos años en uno de los actores que mayor impulso da a la gobernanza de la red en el país. Como se mencionó anteriormente, el modelo de gestión del dominio de nivel superior nacional, aunque impulsado por la academia, quedó en manos de la Cancillería. No obstante, en 2011 su gestión salió del ámbito de este organismo, al crearse la Dirección Nacional del Registro de Dominios de Internet, dentro del ámbito de la Secretaría Legal y Técnica de la Presidencia de la Nación. Desde ese año, el NIC.ar se ha insertado en los espacios regionales e internacionales de gobernanza de internet, a los que incluso ha apoyado en su organización (como las reuniones de ICANN antes mencionadas) y, desde un primer momento, ha formado parte de forma activa del IGF Argentina.

Además de integrar el Comité del IGF Argentina, el NIC.ar ha impulsado espacios de gobernanza de internet con el fin de mantener el diálogo y el debate en torno a temáticas de interés para la comunidad local. Así, entre 2017 y 2019, organizó cuatro encuentros del ciclo de «Charlas Debate sobre Gobernanza de Internet», con el fin de fomentar la discusión de temas vinculados a internet de impacto en nuestro país. También, siguiendo el modelo de múltiples partes interesadas, el NIC.ar impulsó la iniciativa Blockchain Federal Argentina (2017-2019).

A las iniciativas del Nic.ar y del IGF Argentina para fomentar el debate y el conocimiento sobre gobernanza de internet en el país, también se les sumaron los espacios de formación en la materia, que junto con el IGF Argentina son los únicos espacios activos al momento de escribir este artículo. Por un lado, es posible mencionar la Diplomatura de Gobernanza de Internet (DiGI), organizada por el Centro de Tecnología y Sociedad de la Universidad de San Andrés desde 2017, con el apoyo de la CABASE y el Centro de Política Digital para América Latina, que se ha posicionado como el espacio de formación a nivel posgrado en

la temática. La Diplomatura se presenta como un programa multidisciplinar (con aspectos técnicos, legales y socioeconómicos) y también multisectorial, ya que en todas sus ediciones ha contado con profesionales de distintos sectores y también con participación regional. Por otro lado, siguiendo la experiencia de la Escuela del Sur de Gobernanza de Internet[9] (SSIG, por sus siglas en inglés), también en 2017, se lanzó la Escuela de Gobernanza de Internet de Argentina, organizada por el Centro de Capacitación en Alta Tecnología (CCAT LAT) con la colaboración de ENACOM y el apoyo del Capítulo de Internet Society Argentina, con el objetivo de desarrollar un espacio de capacitación y diálogo sobre el tema.

Si bien existen otros aspectos relacionados con la gobernanza de internet que podrían mencionarse en estas páginas, el recorrido realizado en esta sección permite identificar los principales hitos que dieron forma a los procesos de gobernanza de internet en Argentina. Desde el papel central que jugó la academia en tener la primera conexión a internet, su posterior apertura comercial y el rol de Cancillería en la región del «.ar» y en la participación internacional, se puede ver cómo el desarrollo de internet en el país se llevó a cabo de forma colaborativa entre distintos actores desde sus comienzos, pero con un rol central del Estado, ya sea creando espacios o participando activamente en ellos. Sin embargo, estos espacios –como es el caso del IGF nacional– enfrentan desafíos para mantenerse en el tiempo, muchos de los cuales están relacionados con el escenario en el que se encuentra la gobernanza de internet a nivel global.

---

9 Desde 2009, la SSIG se organiza cada año en distintos países de América Latina y el Caribe.

3. Desafíos y oportunidades de la gobernanza de internet

Aunque la gobernanza de internet ganó espacio en las agendas nacionales en los últimos años gracias a la importancia de la red para el desarrollo local, en el nivel global su relevancia enfrenta desafíos. Hitos globales como la reunión NetMundial (2014), la transición de las funciones de la Autoridad de Números Asignados en Internet (IANA, por sus siglas en inglés) del gobierno de los Estados Unidos a la comunidad de internet nucleadas en la ICANN (2016), y la renovación del mandato del IGF Global por diez años más (2016), parecían marcar el éxito del modelo y de los espacios de gobernanza. No obstante, a la vez que crecían las iniciativas locales de gobernanza de internet, la dificultad de la gobernanza de internet de mantener niveles de participación significativos de todos los sectores y de mostrar resultados concretos más allá de las reuniones o espacios institucionales de gobernanza de internet, se presentaba y aún se presenta como obstáculo para la consolidación del modelo como el camino a seguir en temas de internet.

Esta dificultad se debe a dos aspectos interrelacionados: los desafíos de participación que trae consigo el mismo modelo de múltiples partes interesadas y, en estrecha relación con el punto anterior, el rol de los Estados y el avance del modelo multilateral para la definición de políticas de internet.

En relación con la participación de todas las partes involucradas, erigida como bandera en muchos de los espacios globales, regionales e incluso nacionales de gobernanza de internet, no necesariamente significa que la participación de los distintos actores sea equilibrada. Por ejemplo: dentro de la ICANN, la baja participación de la sociedad civil en las políticas del Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) es uno de los debates actuales. Dentro del IGF, en términos

generales, podría decirse que sucede lo contrario: el foro cuenta con una amplia participación de la sociedad civil, pero la baja participación en las últimas ediciones de funcionarios de gobierno y empresas del sector también pone en tela de juicio la naturaleza multisectorial del foro. Esto se debe a un aspecto central de la gobernanza de internet que muchas veces se pierde de vista en los abordajes institucionales del tema: el juego de equilibrios de poder. El carácter participativo de muchos de estos espacios donde no se toman decisiones genera que los actores convocados que tienen más poder que otros sobre aspectos centrales de internet no acudan con la idea de rever sus posiciones en los espacios de trabajo y foros (Cortés, 2014); de esta forma, las discusiones no se traducen en acciones concretas. Para muchos participantes, este hecho demuestra que el modelo, en vez de dispersar el poder entre los actores, refuerza la dinámica de poder existente.

Es en este sentido que el IGF Global[10], cuya razón de ser está en el debate entre sectores y no en la toma de decisiones ni en la publicación de resultados, se encuentra actualmente siendo revisado por el Grupo Asesor Multisectorial (MAG, por sus siglas en inglés), no solo para acordar formas de incrementar la participación, sino también para hacer más relevantes las discusiones y el trabajo entre reuniones. Sin embargo, el MAG no es el único grupo que sigue de cerca esta revisión. En 2019, el Secretario de las Naciones Unidas creó el Panel de Alto Nivel para la Cooperación Digital (HLPDC, por sus siglas en inglés), que, entre sus recomendaciones, propone la creación de un IGF+ (plus), con elementos que pretenden generar nuevos mecanismos de

10 A nivel regional, el LACIGF también se enfrenta a desafíos y ha abierto un proceso de revisión para mejorar el impacto del Foro en la región. Al momento de redacción de este artículo, el Comité de Programa del LACIGF se encuentra revisando las propuestas de mejoras enviadas por la comunidad.

discusión y adopción de soluciones que tengan efectos directos en las políticas públicas. Para muchos actores involucrados en el IGF desde sus comienzos, estas nuevas propuestas traen consigo dudas sobre su implementación y sobre el rol del IGF como espacio multisectorial a la luz del rol de organismos multilaterales, como la ONU, en temáticas de internet.

En este contexto, y en relación con el segundo punto, además del rol de Naciones Unidas en el proceso de revisión del IGF, los espacios multilaterales por excelencia, como los de la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), han empezado a abordar temáticas de internet. La ITU, como organismo internacional para la coordinación del telégrafo, que luego incorporó la telefonía fija y móvil, ha buscado durante décadas tener mayor control sobre temáticas de internet, con el fin de tratarlas con una dinámica tradicional relacionada con la negociación, los acuerdos y la votación. Entre dichos intentos, se pueden ver algunas propuestas realizadas por el bloque de países árabes y países como China y Rusia, para rever la forma en que son gestionados los recursos críticos –como los nombres de dominio y las direcciones IP–, con el fin de que sean los Estados los que tengan autoridad sobre los mismos (Aguerre, 2015).

No obstante, si bien existe una presión de los Estados para incluir más mecanismos multilaterales, en muchos países de América Latina, como Argentina, esto no significa necesariamente un rechazo a la perspectiva multisectorial de la gobernanza de internet, sino que, aunque se tienen en cuenta sus debilidades, se la ve como un camino para la discusión. En nuestro país, como se pudo ver en uno de los apartados anteriores, la mayoría de los espacios de gobernanza de internet han sido impulsados desde el gobierno, aunque no se han mantenido en el largo plazo, principalmente por los cambios de prioridades en la agenda pública y por los cambios de mandato. Iniciativas como la CAPI y

como los grupos multisectoriales buscaron generar espacios impulsados por el Estado, aunque su corta duración no permite analizar el impacto que los mismos puedan haber tenido en el desarrollo de políticas internet en Argentina, aunque sí permiten ver un rol activo del Estado en impulsar e incluso participar –como en el caso del IGF Argentina– en este tipo de procesos.

Pese a que la lista de desafíos de los actuales procesos de gobernanza de internet es larga, también existen aspectos positivos que este tipo de procesos e iniciativas generan para el desarrollo de internet a nivel global, regional e internacional. En primer lugar, no hay que perder de vista que la gobernanza de internet se sustenta en su comunidad –global, regional y local–, compuesta por personas y organizaciones que representan a todos los sectores de internet y que tienen más de cincuenta años de experiencia creando, desplegando y coordinando la red. Este aprendizaje, que se encuentra muy bien documentado gracias al formato que muchos espacios de discusión y coordinación adquirieron, genera un campo propicio para pensar cómo mejorar los procesos y fortalecer los espacios ya existentes, con el fin de superar los signos actuales de fatiga que la comunidad enfrenta. Para ello, como plantea Evgeny Mozorov (en Cortés, 2014), es necesario prestar atención a cómo los valores inherentes a internet, como la transparencia y la apertura, se han manifestado en estos debates, e identificar formas de que los mismos sean tenidos en cuenta.

En segundo lugar, otro aspecto que ha sido mencionado por diferentes autores (DeNardis, 2017) y que puede verse como una oportunidad para resaltar la relevancia de los procesos de gobernanza de internet, es considerar este tipo de modelo como un instrumento para resolver problemas concretos y, de esta forma, tener impacto en políticas públicas. Es decir, una vez más, es necesario salirse de la

conceptualización de la gobernanza de internet y su carácter multisectorial como un fin en sí mismo –aspecto que es señalado como una crítica tanto por académicos en el tema como por participantes de los mismos foros–, para utilizarla como un proceso que permite encontrar soluciones e impulsar políticas concretas con respecto a la privacidad, la neutralidad en la red y el desarrollo de infraestructura para permitir mayor conectividad, entre otros temas.

Estos dos puntos u oportunidades, siempre sin perder de vista los desafíos y las tendencias actuales, pueden aplicarse también al caso argentino y traducirse en recomendaciones para fortalecer los espacios nacionales existentes o impulsar nuevos.

Reflexiones finales y recomendaciones

El presente artículo buscó abordar la gobernanza de internet en Argentina, con el fin de comprender su desarrollo, principales espacios, desafíos y oportunidades. Desde que el desarrollo de internet ha impulsado la creación de mecanismos y procesos a nivel global, tanto para gestionar y coordinar sus recursos críticos como para debatir y pensar sus aspectos políticos y socioeconómicos, actores locales, desde académicos, expertos técnicos y representantes de cámaras, hasta funcionarios del gobierno, han buscado contar con un enfoque similar en el ámbito nacional.

Tal como sucede en el nivel global y en la región, en nuestro país la gobernanza de internet presenta un abordaje institucional enfocado en el modelo de múltiples partes interesadas, característico de estos espacios. Sin embargo, como se señaló desde un comienzo, las iniciativas locales creadas hasta el momento no han logrado o enfrentan desafíos para sostenerse en el largo plazo. También, al centrarse en el debate y la discusión, sus esfuerzos no se han traducido directamente

en programas o políticas concretas que impulsen el desarrollo de internet en Argentina, situación a la que también se enfrenta su régimen global de gobernanza.

En este sentido, y sobre la base del recorrido realizado en este artículo sobre la experiencia argentina en lo que refiere a la gobernanza de internet y sus desafíos y aspectos positivos del modelo a nivel global, es posible pensar algunos caminos a seguir para fortalecer el ecosistema de internet en el país.

En primer lugar, se puede señalar que las iniciativas impulsadas en los últimos años han demostrado que existe una necesidad de que los actores locales tengan un espacio donde abordar los desafíos que la red trae consigo, teniendo en cuenta sus realidades locales de manera continua. La creación de espacios multisectoriales para la discusión de temas relativos a internet es esencial para que las discusiones y políticas que puedan adoptarse como resultado tengan en cuenta las opiniones de diferentes sectores. En esta línea, el recorrido llevado a cabo por los hitos de internet y su gobernanza en Argentina permiten ver que, como sucede a nivel global, los actores locales que conforman la comunidad de internet en el país –el ccTLD nacionales tanto en su rol técnico como de gobierno, las cámaras, la academia, entre otros– tienen años de experiencia, que puede utilizarse y traducirse en acciones concretas.

De esta forma, y, en segundo lugar, es importante fortalecer los espacios nacionales de diálogo y debate sobre gobernanza de internet, como el Foro de Gobernanza de Internet en Argentina. Por un lado, como sucede a nivel global, es necesario enfatizar su relevancia convirtiendo la reunión o evento anual en un proceso que cuente con una agenda de temas concretos y mecanismos de trabajo que se desarrollen durante todo el año. Tal como señala Aguerre (2017), el trabajo más distribuido hace más visible el trabajo y los logros que la

realización de un evento anual. Si bien esta idea ha estado en los objetivos del Comité Multisectorial del IGF local desde sus inicios, no se ha logrado mantener los niveles de participación de algunos sectores claves, como el gobierno, para que el Foro tenga mayor impacto. Dado el rol central que el gobierno tiene en políticas públicas de internet y ha tenido en el desarrollo de la gobernanza en el país, es importante que este participe en forma activa, para que el espacio mantenga su legitimidad y adquiera mayor relevancia.

En este sentido –y en un contexto en el que algunos gobiernos impulsan la adopción de mecanismos tradicionalmente multilaterales para la discusión e implementación de políticas de internet–, nuestro país no muestra oposición a los procesos multisectoriales, sino, más bien, una posición mixta: muchos espacios de gobernanza de internet multisectoriales han sido impulsados por el Estado, ya sea desde el cctTLD nacional o desde distintos ministerios, y otros han surgido de otros sectores, pero han buscando la participación activa del gobierno desde un comienzo. Este es un punto que es necesario seguir explorando. Futuros artículos e investigaciones en la materia podrían detenerse con mayor detalle en el rol del Estado en estos procesos y en relación con otros actores claves para el desarrollo local de internet, sobre todo teniendo en cuenta el juego de poder entre ellos.

Por otro lado, dado que no se puede perder de vista su carácter transfronterizo y su arquitectura descentralizada, es importante que los actores de internet del país sigan de forma activa y coordinada las discusiones que suceden en espacios regionales e internacionales. Aunque muchas veces sostener la participación en reuniones se hace costoso por temas económicos y de tiempos, los espacios nacionales de debate y también los académicos pueden colaborar para cerrar esa brecha. En la misma línea, aunque este trabajo no se enfocó en otros casos, es importante mirar otras experiencias regionales que han

tenido resultados positivos en torno a mecanismos de coordinación, sostenibilidad en el tiempo y resultados tangibles, como las de Brasil, México y Costa Rica, con el fin de comprender cómo el caso argentino podría beneficiarse de ellas.

Por último, cabe resaltar que nos encontramos en un momento clave para la gobernanza de internet. Se ha expuesto que la misma no ha logrado posicionarse como el único modelo a seguir para discutir todos los temas relacionados con la red y dar respuestas, y que, al mismo tiempo, el modelo multilateral adquiere importancia en otros espacios internacionales. No obstante, la gobernanza de internet, por su conexión con los valores inherentes a la red, sigue siendo un mecanismo relevante para dar un marco institucional a los debates y avanzar hacia la generación de políticas que tengan en cuenta la naturaleza de internet como recurso sin fronteras y a la vez que influyan positivamente en el ecosistema nacional. Pese a los desafíos, el surgimiento y el impulso de espacios nacionales en el tema demuestran que se puede avanzar en este camino.

A nivel nacional, queda mucho por hacer para impulsar internet. Aunque la gobernanza de internet y su modelo de múltiples partes interesadas no son la respuesta a todo, se constituyen como un camino plural, abierto y transparente, que puede ayudar al desarrollo de mejores políticas que beneficien a la comunidad.

Referencias bibliográficas

Agenda de Túnez (2005). Agenda de Túnez para la Sociedad de la Información. Recuperado de http://www.itu.int/wsis/docs2/tunis/off/6rev1-es.html.

Aguerre, C.; Canabarro, D.; Callegari, A.; Hurel, L.; Sautchuk, Patricio N. (2018). Mapping National Internet Governance Initiatives in Latin America. Internet Policy Review Series, Annenberg School of Communication. Disponible en SSRN: https://ssrn.com/abstract=3208218.

Aguerre, C., Galperin y Becerra, M. (2015). *La gobernanza de Internet: Argentina y Brasil en el contexto global*. Buenos Aires: Catálogos UBA, Universidad de Buenos Aires.

Cortés, C. (2014). La gobernanza de Internet: la trampa de las formas. Recuperado de http://www.palermo.edu/cele/pdf/CELE_GobernanzaDeInternet.pdf.

De la Chapelle, B. (2012). Multistakeholder Governance - Principles and Challenges of an Innovative Political Paradigm. Recuperado de http://www.collaboratory.de/w/Multistakeholder_Governance_-_Principles_and_Challenges_of_an_Innovative_Political_Paradigm.

Del Campo. Agustina (comp.) (2017). *Hacia una Internet libre de censura II: perspectivas en América Latina.* Buenos Aires: Universidad de Palermo.

DeNardis, D. L. (2010). The Emerging Field of Internet Governance. SSRN Electronic Journal. Recuperado de https://doi.org/10.2139/ssrn.1678343.

DeNardis, D. L., & Raymond, M. (2013). Thinking Clearly About Multistakeholder Internet Governance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2354377.

Dunayevich, J.; Ramírez, G.; Trentadue, C. (2019). Historia de NIC Argentina en el marco de la evolución de Internet en el país. Recuperado de https://nic.ar/sites/default/files/paper_-_historia_de_nic_argentina_en_el_marco_de_la_evolucion_de_internet.pdf.

Hofmann, J. (2005). Internet Governance: A Regulative Idea in Flux. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327121.

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: putting fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49. https://doi.org/10.1080/23738871.2016.1158303.

Iosifidis, P. (2011). *Global media and communication policy*. Palgrave Macmillan. Recuperado de https://books.google.com.ar/books?hl=es&lr=&id=kaCHDAAAQBAJ&oi=fnd&pg=PP1&dq=Iosifidis+internet+governance&ots=bYtJNXwz4F&sig=RU5H_a9oC41SIkYX_dYwHHh-7XE#v=onepage&q=Iosifidis internet governance&f=false.

Mueller, M. (2010). *Networks and states : the global politics of Internet governance*. MIT Press.

Lista de siglas

CABASE - Cámara Argentina de Internet
CAPI - Comisión Argentina de Políticas de Internet
CCLAT - Centro de Capacitación de Alta Tecnología
ccTLD - Country code top-level domain
CMSI - Cumbre Mundial de la Sociedad de Información (WSIS en inglés)
DNS - Domain Name System
GAC - Governmental Advisory Committee
HLPDC - High-level Panel on Digital Cooperation
IANA - Internet Assigned Numbers Authority
ICANN - Internet Corporation for Assigned Names and Numbers
IGF - Internet Governance Forum
ITU - International Telecommunication Union
LACIGF - Latin American and Caribbean Internet Governance Forum
MAG - Multistakeholder Advisory Group
NIC.AR - Network Information Center Argentina
NSA - National Security Agency
SSGI - South School of Internet Governance
UN - United Nations

AGUSTINA CALLEGARI. Especialista en políticas digitales y gobernanza de internet. Actualmente es Gerente Senior de Relaciones Externas en internet Society, una organización no gubernamental que trabaja para expandir el acceso a Internet. Previamente, Agustina se desempeñó como asesora en el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires (2011-2016) y como Directora de Políticas y Gobernanza de Internet en el Ministerio de Modernización de la Nación (2016-2017). Además, es investigadora invitada del Centro de Tecnología y Sociedad (CETyS) de la Universidad de San Andrés y participa como docente en el Curso de Postgrado en Derecho Informático de la Universidad de Buenos Aires. Licenciada en Ciencias de la Comunicación por la Universidad de Buenos Aires (graduada con honores) y una maestría en Servicios Tecnológicos por la Universidad de San Andrés.

El *back office* de la transformación digital de la administración pública

CAPÍTULO 6

La transformación digital de los gobiernos: lecciones de distintas partes del mundo

Bárbara Ubaldi

Introducción

Durante las últimas décadas, la irrupción de las tecnologías digitales ha cambiado la manera en que los gobiernos y las personas interactúan y se organizan en la sociedad y la economía. Desde la adopción inicial de computadoras y sistemas de comunicación básicos hasta la generación exponencial de datos y la incorporación generalizada de dispositivos móviles e inteligencia artificial (IA), el surgimiento de las tecnologías digitales ha demostrado su potencial efecto disruptivo en las operaciones internas de los organismos del sector público y su estrategia de diseño y ejecución de políticas y servicios. La adopción de tecnologías digitales basada en un enfoque gubernamental integral tiene el potencial para transformar la manera en que los gobiernos organizan y administran sus funciones centrales, e incentivar la colaboración entre los distintos niveles y dentro de cada uno de ellos.

Estos cambios pueden mejorar el desempeño de los gobiernos, al igual que la eficiencia en la prestación de los servicios públicos, y modificar la forma en que los ciudadanos consumen los servicios e interactúan con los organismos del sector público. Estas formas de interacción renovadas pueden contribuir al desarrollo y/o el fortalecimiento de la confianza y la credibilidad pública en los gobiernos, lo cual es crucial para reforzar la relación ciudadano-Estado. Desde esta perspectiva, la adopción de tecnologías digitales colabora con el establecimiento de cimientos sólidos para rediseñar la experiencia de los ciudadanos con la provisión de los servicios públicos y, en última instancia, tiene un impacto en la legitimidad de nuestros sistemas democráticos.

Anteriormente, los esfuerzos del «gobierno electrónico» por utilizar la tecnología para aumentar la eficiencia y la transparencia de los organismos públicos fueron fundamentales para apoyar la digitalización de los procesos gubernamentales y mejorar las operaciones del sector público. Algunos ejemplos de enfoques orientados al gobierno electrónico son la *digitalización* de los procedimientos administrativos a través de la implementación de sistemas informáticos en las distintas agencias gubernamentales o la transición hacia administraciones sin empleo de papeles y con canales informativos y de provisión de servicios en línea. A pesar de las ventajas considerables que ofrece el gobierno electrónico, este enfoque significó muchas veces aplicar la tecnología a procesos engorrosos, diseñados sobre la base de prácticas de gestión existentes y una lógica analógica dentro del sector público.

Con el tiempo, el énfasis se desplazó hacia la necesidad de fomentar formas de gobierno más participativas, innovadoras y ágiles, orientadas a objetivos más allá de la eficiencia y la productividad. Una mayor integración, coherencia y horizontalidad se encuentran en el centro de la transformación introducida por el paradigma del gobierno

digital que propone la idea de una *digitalización* plena de los sectores públicos.

El imperativo del gobierno digital aprovecha las tecnologías y los datos digitales para una transformación de los servicios más cohesiva, una colaboración transversal y un uso compartido de los datos para generar organismos públicos abiertos, orientados al usuario y proactivos. Desde esta perspectiva, el uso estratégico de herramientas y datos digitales para crear ecosistemas digitales dentro de los gobiernos puede equipar a los funcionarios públicos con las habilidades y los recursos necesarios para impulsar la transformación digital. Este cambio de paradigma propone un mayor nivel de madurez de los gobiernos digitales, lo que sirve como medio para satisfacer más eficientemente las necesidades de los ciudadanos, aumentar su bienestar y fortalecer la satisfacción pública en relación con los gobiernos. A fin de facilitar este imperativo, el sector público debe definir estándares comunes (por ejemplo, para el diseño y la provisión de los servicios públicos, el acceso a los datos y el uso de los mismos), desarrollar infraestructuras compartidas, administrar y utilizar los datos como un activo estratégico para la creación de valor público y establecer mecanismos para permitir a terceros (como el tercer sector y la comunidad de las denominadas *GovTech*[1]) colaborar con los gobiernos para incorporar innovación a la prestación de sus servicios. Contar con el marco de gobierno adecuado, facilitadores fundacionales y componentes de políticas brinda una base para una transformación digital coherente y sustentable del sector público que genere valor para los ciudadanos.

La robustez de estos cimientos puede incrementar significativamente el nivel de flexibilidad, resiliencia y capacidad de respuesta de un gobierno en tiempos de crisis. La pandemia del COVID-19 ha

1 Empresas que diseñan servicios tecnológicos para los gobiernos.

demostrado, más que nunca, que una base digital sólida es necesaria para la continuidad y la integración de las operaciones internas y los servicios de los gobiernos. Las pruebas reunidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2020) muestran que algunos países se encontraban preparados para recurrir rápidamente a herramientas y datos digitales para satisfacer las necesidades de los usuarios, garantizando a la vez la provisión continua de servicios remotos durante los períodos de confinamiento, así como el desarrollo inmediato de servicios gubernamentales intersectoriales para un fácil acceso a los beneficios sociales y económicos, o una comunicación eficaz sobre la propagación de la pandemia. Por el contrario, países con transiciones menos maduras hacia un enfoque de gobierno plenamente digital experimentaron dificultades para brindar servicios coherentes e integrados, con los consiguientes problemas de confiabilidad u operatividad que pueden afectar la confianza y la cohesión social en tiempos de crisis.

A medida que las oportunidades para las economías y las sociedades aumentan como resultado de las nuevas tendencias, traen consigo implicancias significativas para los gobiernos, que enfrentan una creciente presión para modificar su enfoque actual en relación con la elaboración de políticas, la prestación de servicios y la participación pública. Para mantenerse al día frente a la necesidad de estos cambios, los gobiernos deben evolucionar constantemente, demostrando ser abiertos, productivos, innovadores e inclusivos. El presente artículo presenta el marco desarrollado por la OCDE para abordar temas clave vinculados a la transición hacia una transformación digital real de los gobiernos, y analiza las tendencias predominantes en las respuestas diseñadas por los gobiernos observadas en el mundo entero.

1. La transformación digital: del gobierno electrónico al gobierno digital

La transformación digital del sector público requiere una transición desde un gobierno electrónico hacia un gobierno digital. La OCDE ha promovido activamente el cambio hacia un gobierno digital maduro recurriendo a las disposiciones de la Recomendación del Consejo de la OCDE sobre las Estrategias de Gobierno Digital (OCDE, 2014). La Recomendación, adoptada el 15 de julio de 2014, es el primer instrumento legal internacional referido al gobierno digital. Su propósito es ayudar a los gobiernos a adoptar enfoques más estratégicos en el uso de tecnologías y datos digitales, para fomentar gobiernos más abiertos, participativos, responsables e innovadores. De acuerdo con esta Recomendación, se entiende por gobierno digital «el empleo de tecnologías digitales, como parte integral de las estrategias de modernización de los gobiernos, para crear valor público» (OCDE, 2014).

El desafío en el contexto de la transformación digital, acelerada por el ritmo veloz de la digitalización, ya no es introducir tecnologías digitales a las actividades del sector público (gobierno electrónico). Por el contrario, consiste en incorporarlas a las agendas de transformación del sector público como un componente central de las iniciativas de los gobiernos destinadas a promover la evolución y la modernización continuas de las administraciones públicas, en todas las áreas de políticas y en todos los niveles de gobierno de una manera cohesiva, coherente y participativa.

La aplicación de esta Recomendación en numerosas evaluaciones sobre gobierno digital en todo el mundo con el objetivo de respaldar el análisis y la formulación de recomendaciones de políticas para la transición de los gobiernos a enfoques de gobierno digital ha conducido al desarrollo del Marco de Políticas de Gobierno Digital de la OCDE

(MPGD). Este marco abarca seis dimensiones que caracterizan a un gobierno digital:

- Digital por diseño
- Gobierno como plataforma
- Sector público basado en datos
- Abierto por defecto
- Orientado al usuario
- Proactividad

El MPGD (ver Gráfico 1) es un instrumento de políticas pensado para ayudar a los gobiernos a identificar determinantes clave para un diseño e implementación eficaces de enfoques estratégicos para una transición hacia una transformación digital real.

Basándose en las disposiciones de la Recomendación del Consejo de la OCDE sobre las Estrategias de Gobierno Digital, el MPGD se funda en el supuesto de que mejorar la madurez de estas seis dimensiones implica pasar de una gobernanza distribuida a modelos de gobernanza que ayudan a superar legados de burocracia, verticalidad y silos para fomentar la horizontalidad y la integración, la coordinación y las sinergias a lo largo de los distintos niveles de gobierno y entre dichos niveles. Este significativo cambio de paradigma en la definición de la gobernanza del gobierno digital se vuelve esencial para superar la idea de los servicios digitales vistos como resultados aislados y los efectos secundarios de políticas más amplias, destacando su importancia como objetivos centrales e integrales de la transformación del sector público (OECD, 2020ª, próximo a publicarse). Después de todo, los servicios públicos representan la forma más inmediata que tienen las personas de experimentar sus gobiernos.

Comprender que cuando los gobiernos diseñan un servicio público no lo hacen para servir a un estudio, una organización o una parte interesada, sino para responder a las necesidades de los

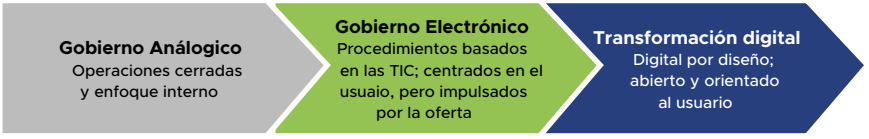
individuos (Downe, 2020), es esencial para reconocer la importancia de repensar las operaciones y los procesos internos. Esto permite articular las diferentes partes de la administración, a fin de mejorar la experiencia de los usuarios y fortalecer su confianza en los gobiernos. Un gobierno digital que presenta niveles de madurez mayores en las seis dimensiones mencionadas se encuentra mejor posicionado no solamente para alcanzar eficiencia interna y transparencia, sino también para brindar servicios que satisfagan las expectativas de los individuos.

Gráfico 1. Marco de Políticas de Gobierno Digital de la OCDE

Fuente: basado en la Recomendación del Consejo de la OCDE sobre las Estrategias de Gobierno Digital (OCDE, 2014).

De hecho, los gobiernos digitales logran que los servicios basados en la demanda y producidos en conjunto sean más factibles y presionan por enfoques más orientados al ciudadano y a la comunidad (colaborativos), un tema que se tratará más adelante en este artículo. El Gráfico 2 ilustra la progresión desde un gobierno analógico a un gobierno digital a través del gobierno electrónico, y su impacto significativo en la provisión de los servicios:

Gráfico 2. Avanzando hacia la transformación digital



Fuente: OCDE, 2020.

2. Sentando las bases correctamente: de una producción vertical y una gobernanza distribuida, a organismos que funcionan como sistemas

Si bien la digitalización no es una opción, la manera en que los gobiernos «se digitalizan» es un tema de debate e incertidumbre. Los gobiernos tienen un rol crucial que desempeñar en el establecimiento de las condiciones necesarias para la transformación digital del sector público, la economía y la sociedad en general. Este rol va mucho más allá de generar condiciones y marcos propicios para inversiones públicas y privadas en infraestructura digital e investigación y desarrollo. Les corresponde a los gobiernos decidir de qué manera las políticas son diseñadas, implementadas y monitoreadas, y cómo los servicios públicos son concebidos y provistos en este nuevo contexto.

A fin de satisfacer las necesidades cambiantes de sus votantes y servirlos en el lugar donde se encuentren y como lo deseen, de una manera segura, los gobiernos deberían entender que lo que impulsa la transformación digital no es la tecnología, sino una estrategia de gobierno digital capaz de contribuir a lo siguiente:

- Administrar una experiencia de usuario dinámica (digital) en un entorno abierto y participativo, utilizando datos.

- Superar desafíos organizativos que generan entornos de políticas inadecuados para la era actual, lo cual significa que los resultados ya no pueden ser considerados como una responsabilidad de un único organismo gubernamental.
- Desarrollar modelos y enfoques que vayan evolucionando para invertir estratégicamente en las tecnologías digitales, implementarlas y utilizarlas.

En segundo lugar, la transformación digital afecta significativamente el funcionamiento de la maquinaria de los gobiernos, la dinámica organizativa y las interacciones dentro del sector público y entre gobiernos y sociedades. Esto nos conduce a un tema clave. ¿Qué acuerdos de gobernanza son necesarios para colocar sistemáticamente las necesidades de los ciudadanos en el centro de los procesos de toma de decisión y permitir a la administración abordar de una mejor manera las demandas de las comunidades comprometidas digitalmente, sin relegar el servicio a una creciente población de edad avanzada? ¿Cuál es la gobernanza requerida para apoyar el desarrollo de una administración orientada al usuario, capaz de compartir, coordinar, reutilizar e integrar (recursos, procesos y tareas) para ser más ágil, conforme lo exige un entorno cambiante? ¿Cuál es el costo de no ajustar la gobernanza a esta realidad en constante evolución?

Marcos de gobernanza sólidos y acuerdos institucionales adecuados para promover un cambio de sistema y convertir al gobierno en un gobierno digital por diseño y orientado al usuario son elementos necesarios para transformar digitalmente el sector público. La integración de las tecnologías digitales en todas las áreas de políticas requiere la colaboración de una variedad de actores, un liderazgo sólido y una alineación entre la planificación, la formulación y la implementación de políticas, al igual que niveles deseables de continuidad y coherencia en una agenda de gobierno digital.

Para alcanzar esto, la configuración institucional debería permitir el nivel de coordinación adecuado. Esto implica que quienes están a cargo del seguimiento de la implementación de la estrategia digital para los gobiernos deberían ser capaces de contar con un mandato claro y ser apoyados por el marco de gobierno necesario, que provea las facultades, los mecanismos institucionales y las herramientas y los recursos de políticas para ser capaces de liderar la definición de una visión, dirigir y coordinar acciones en línea con los objetivos estratégicos, y hacer responsables de los resultados a los distintos actores. Un marco de gobernanza que brinde alineación y coordinación puede ayudar a que el cambio tenga lugar más fácilmente.

Un conjunto de gobiernos de la OCDE está reconsiderando su configuración institucional (por ejemplo, como Italia y Suecia, han creado agencias digitales). Otros están evaluando maneras para incorporar ciclos de retroalimentación al diseño de los servicios y la elaboración de políticas, enfocándose en el desarrollo de capacidades para un diseño orientado al usuario, o estableciendo organismos ágiles para acompañar la estructura organizativa actual a través del cambio hacia la transformación digital de las administraciones públicas con una visión holística (por ejemplo, Australia y el Reino Unido). Estas condiciones tienen por objeto facilitar la integración del gobierno digital en agendas más amplias del sector público y fomentar la creación de sinergias con otras áreas de políticas transversales, tales como la innovación en el sector público, la prevención de la corrupción, el gobierno abierto y la simplificación administrativa, por nombrar algunas (OCDE, 2016).

Asimismo, el concepto basado en tecnologías de información y comunicación (TIC) del gobierno como plataforma es fundamental para que los países adopten enfoques de pensamiento sistémicos más estratégicos para fortalecer las interacciones, las vinculaciones y las

colaboraciones dentro de un sector público concebido como un sistema totalmente complejo. Comprender tanto el entorno propicio creado por las tecnologías digitales, como las nuevas formas de trabajar dentro de este entorno, es esencial para acelerar la concientización, crear el contexto y construir las capacidades requeridas en los líderes públicos para el despliegue de la transformación digital. Esta puede, ciertamente, ayudar a superar el pensamiento vertical, conectando una amplia variedad de elementos que interactúan entre sí (por ejemplo, los datos, las personas, los procesos y los sistemas) y aumentando la comprensión sobre el rol de interconexión de las tecnologías digitales sobre la base de teorías más sofisticadas de trabajo y cambio (OCDE, 2017). Este enfoque puede aligerar el esfuerzo de garantizar un compromiso y apoyo sostenidos a la transformación digital, entre los niveles de liderazgo político superiores dentro del gobierno central. El objetivo mencionado puede lograrse implementando mecanismos de gobernanza básicos, que puedan ayudar en:

- *El desarrollo y el uso coordinados de elementos clave* (como, por ejemplo, la identidad digital y la verificación de identidad, los pagos en línea y móviles, la provisión de servicios digitales y los documentos y archivos digitales).
- *La adopción de estándares, arquitecturas y normas comunes*.
- *El desarrollo de iniciativas para la adquisición de tecnologías de información y comunicación*, agrupando la demanda, permitiendo ahorros y promoviendo la adopción de soluciones de mayor interoperabilidad en todo el sector público.
- *La adopción de pautas comunes e iniciativas compartidas en relación con la provisión de servicios digitales*, alentando el desarrollo de plataformas más centradas en el ciudadano.
- *El establecimiento de organismos institucionales transitorios y flexibles con mandatos específicos,* con la competencia, la

visión y la visibilidad política para conducir la transformación digital y ayudar a actores clave dentro de la gobernanza actual a transitar el cambio.

La Recomendación del Consejo de la OCDE sobre las Estrategias de Gobierno Digital destaca la necesidad de los gobiernos de reexaminar su marco de gobernanza y sus configuraciones y estrategias institucionales para adaptarse a esta realidad cambiante. No hacerlo podría significar un uso menos eficiente de los recursos públicos, una pérdida acelerada de la confianza pública en el gobierno y la percepción de que el mismo está desconectado de las necesidades de la sociedad y es incapaz de aprovechar las tendencias tecnológicas para promover políticas e implementar medidas que maximicen el bienestar social y económico.

A fin de cuentas, **lo más importante en relación con la gobernanza no es el diseño institucional, sino el propósito funcional.** La configuración actual, ¿permite a las instituciones del sector público y a los funcionarios públicos coordinar y colaborar de maneras nuevas con herramientas nuevas? ¿Se apoya en un consenso amplio (por ejemplo, les permite a los gobiernos alcanzar metas estratégicas clave tales como aquellas definidas por una agenda digital nacional)? ¿Permite optimizar la creación de valor, combinando problemas y necesidades/preferencias de usuarios con soluciones que brinden la mejor opción para satisfacer todos estos elementos?

3. Los datos como un recurso ilimitado y sus implicancias con relación a las políticas

Como parte de su travesía hacia una transformación digital completa, los gobiernos deberán prepararse para un futuro en el cual los datos se encontrarán en el centro de la digitalización del sector público.

Por esta razón, resulta importante que los gobiernos tomen medidas para sentar las bases requeridas como parte de su estrategia de transformación digital. Un marco de gobernanza de datos que mejore la gestión de los datos en relación con el rendimiento, la responsabilidad y la previsión puede ayudar a los gobiernos a avanzar en su capacidad de utilizar datos para diseñar e implementar políticas y proveer servicios de una mejor manera. Esto puede promover medidas coherentes a lo largo del sector público destinadas a modernizar la arquitectura de datos y construir interfaces de programación de aplicaciones (API), para que los usuarios puedan emplear inteligencia artificial sobre los datos que los gobiernos ya reúnen; la dirección y el seguimiento de inversiones en recursos adecuados para operar en un entorno orientado a los datos; y colaboraciones con empresas del sector privado cuando no se cuenta con conocimientos y experiencia a nivel interno (por ejemplo, para desarrollar sistemas de IA).

Una transformación digital exitosa requiere ciertamente un sector público que sea consciente y capaz de administrar de manera estratégica la cadena de valor de datos. Esto incluye reconocer la importancia estratégica de utilizar y manejar datos para transformar el diseño, la provisión y el seguimiento de políticas públicas. Un **sector público orientado a los datos** comienza con el reconocimiento de los datos como un recurso clave para los gobiernos, posibilitado mediante el gobierno digital. Un uso inteligente de los datos puede permitir servicios bien orientados, dirigidos a necesidades específicas y centrados en el usuario. El análisis de los datos permite pasar de un diseño jerárquico de servicios públicos generales a la formulación de un diseño de servicios con objetivos bien definidos y una implementación de políticas y provisión de servicios sobre la base de necesidades, y aumentar, de este modo, la accesibilidad, el alcance y la efectividad de los servicios públicos. Así, un sector público orientado a los datos puede incrementar

a un nivel de calidad deseado la competencia de los gobiernos en la provisión de los servicios que necesitan los ciudadanos, y contribuir de manera significativa a la confianza pública en los gobiernos.

No obstante, a medida que las capacidades de los gobiernos para brindar un mayor apoyo a la gestión de datos como un activo estratégico clave vayan creciendo, deberán garantizar un uso ético de los datos, al igual que una protección de su privacidad y seguridad, puesto que la confianza puede verse amenazada si los datos son utilizados de una manera no ética (OCDE, 2019), y lo mismo aplica al empleo de algoritmos e inteligencia artificial que utilizan datos. Asimismo, los gobiernos deberán ajustar sus leyes, políticas y prácticas para alinearlas a las tendencias emergentes sobre el uso y el acceso de los datos vinculadas a la evolución de los datos masivos (*big data*).

El contexto actual les ofrece a los gobiernos la oportunidad de capturar y utilizar datos para predecir, comprender y responder mejor a las necesidades y expectativas de las sociedades (por ejemplo, a través de análisis predictivos y el empleo de sistemas de vigilancia integral), lo cual les permitiría, por ejemplo, no sólo incrementar su poder y control sobre las poblaciones, sino, también, entrar en nuevas dinámicas de interacciones. El gobierno y la gestión de los datos no sólo son relevantes para uso interno del gobierno y para mejorar la toma de decisión pública, sino también como una herramienta de participación para partes interesadas externas y como una plataforma para la creación conjunta de valor público. Mediante la reutilización de los datos del gobierno, los desarrolladores y las compañías privadas pueden diseñar nuevos servicios, que pueden ser alternativos, complementarios o no estar relacionados con los servicios públicos existentes. Las organizaciones de la sociedad civil (OSC) y los académicos pueden utilizar datos abiertos para debatir sobre políticas públicas relevantes o asuntos de diseño de servicios, y ayudar a impulsar el rendimiento público

y una buena gobernanza. Asimismo, la reutilización de los datos abiertos por parte de emprendedores sociales en temas que les preocupan profundamente puede colaborar con la creación de valor social. Aun así, el trabajo de la OCDE sobre los datos abiertos muestra que existe un potencial sin explotar para los gobiernos y los sectores públicos como fuentes de reutilización de datos (OCDE, 2020b).

La capacidad de los gobiernos y los sectores públicos de adaptarse determinará su relevancia y competitividad en el nuevo contexto digital. Esto implica crear las condiciones para que las instituciones públicas abran, compartan, reutilicen e integren procesos de datos y tareas para estimular la colaboración, la creatividad y la confianza. Esto exige gobiernos pacientes, resistentes y persistentes, que reconozcan la importancia de utilizar todos los recursos (incluyendo los datos) de maneras transformadoras, gracias a los nuevos usos de los datos inteligentes (es decir, datos que tienen una semántica útil asociada a los mismos) en combinación con las tecnologías digitales.

Finalmente, la digitalización es un factor clave para una supervisión rigurosa del gasto social, en tanto permite a los gobiernos garantizar controles bidireccionales, una mayor responsabilidad por la calidad del servicio y un empleo óptimo de los recursos a través del uso de datos. Al mejorar la gestión de los datos y emplear nuevas técnicas de procesamiento de datos, los países están tratando de personalizar mejor los beneficios sociales. Por ejemplo, en India, las tecnologías digitales facilitaron un enfoque más orientado al ciudadano para la auditoría de los programas de asistencia social de los esquemas de jubilaciones, pensiones por viudez y pensiones por discapacidad, que tradicionalmente se enfocan en la detección de pagos indebidos a personas que no reúnen las condiciones necesarias en los esquemas de pensión. La Institución de Auditoría Suprema de la India invirtió activamente en el análisis de datos y empleó datos externos para verificar

si beneficiarios aptos estaban siendo excluidos, lo que resultó en una auditoría de rendimiento considerablemente más exhaustiva, esclarecedora y orientada a las necesidades de los grupos vulnerables relevantes (OCDE, 2017a). De manera similar, Francia ha empleado la *minería de datos* para identificar y combatir el fraude en las asignaciones familiares y los beneficios sociales, y alcanzó un aumento del 56% en la detección de irregularidades en 2014 (CAF, 2015).

4. Asistiendo a las instituciones en la transición de un gobierno electrónico a un gobierno digital

4.a. Talento digital

A medida que los gobiernos evalúan y planifican el futuro del personal de su sector público, necesitan herramientas que los ayuden a medir la madurez digital de su entorno para poder tomar decisiones con fundamento y adoptar políticas para garantizar su preparación y avanzar hacia el final del espectro de la transformación digital.

Luego de establecer un medio seguro y alcanzar un alto nivel de madurez digital en el que los funcionarios públicos puedan aprender, desarrollar y poner en práctica capacidades y competencias digitales, es importante identificar las habilidades correctas a desarrollar o requerir en un candidato. Si bien debemos reconocer que ciertos aspectos de lo que se identifica como «competencias digitales del usuario» (procesamiento de textos, navegación en internet, comunicación por correo electrónico y programas de planillas de cálculo) deberían representar un punto de referencia para las habilidades de la era del gobierno electrónico en el sector público, y ya son reconocidas y apoyadas por un mayor número de funcionarios públicos, las competencias digitales han pasado de ser «opcionales» a convertirse

en «decisivas». Estas deben ser complementadas con habilidades y competencias transversales, tales como la capacidad de comunicarse en forma eficaz a través de tecnologías con y sin conexión a internet. Existen tres preguntas complementarias que ayudan a comprender estas habilidades: ¿cómo están definidos los distintos roles?, ¿qué perfiles deberían componer un equipo? y ¿qué habilidades son necesarias en el gobierno?

A pesar del hecho de que la mayoría de los gobiernos en todo el mundo no parecen contar con un sector público plenamente equipado con las competencias necesarias, los líderes políticos cada vez son más conscientes de la necesidad de garantizar una presencia adecuada de talentos y habilidades digitales dentro del sector público. Los países están recolectando y generando cada vez más bases de prueba cuantitativa y cualitativa para evaluar la fuerza laboral del sector público y colaborar en su evolución como una herramienta para forjar y fomentar una transformación digital exitosa del sector público. Capturar datos relacionados con los recursos humanos del sector público, evaluar la situación actual en términos de carencias de habilidades y comprender la importancia de adoptar un enfoque coherente en relación al tema será, más que nunca, esencial para permitir a los gobiernos operar en un entorno transformado digitalmente.

Los gobiernos que se encuentran más maduros desde una perspectiva digital están adoptando estrategias que ayudan a las autoridades a:

- Evaluar el ámbito laboral desde un punto de vista «digital».
- Identificar las habilidades, los perfiles y los roles necesarios para establecer una «fuerza laboral digital».
- Planificar cómo desarrollar, reclutar y retener a esta «fuerza laboral digital».

Enfocarnos en estos tres componentes es esencial para permitirles a los gobiernos hacerse las preguntas correctas al momento de evaluar sus recursos humanos. En primer lugar, es fundamental comprender el entorno de la organización en su totalidad desde un punto de vista cultural, organizativo y de liderazgo, ya que permite establecer un marco para el contexto más amplio. En segundo lugar, las competencias y las categorías de puestos de trabajo actuales son una indicación importante de cómo se concibe el talento digital y de la capacidad de evaluar las necesidades presentes. En tercer lugar, el modelo existente sobre reclutamiento, retención y capacitación es una señal importante del enfoque estratégico general y la capacidad para vincular políticas digitales con reformas de gestión de recursos humanos más amplias.

La experiencia de los miembros de la OCDE y los países asociados a dicho organismo nos lleva a la identificación de las siguientes recomendaciones clave en relación con el establecimiento de un sector público adecuadamente provisto de talentos:

- Los organismos necesitan enfoques de liderazgo, culturales y organizativos como los mencionados anteriormente.
- Los organismos necesitan contar con una definición de competencias y categorías de puestos de trabajo que incluyan estos elementos.
- Los organismos deben disponer los medios para garantizar que su fuerza laboral sea suficientemente digital y continúe siéndolo.

Las tecnologías digitales están efectivamente originando nuevas y complejas situaciones, que requerirán que los funcionarios de mayor rango y quienes son responsables de la elaboración de políticas demuestren una comprensión plena de los asuntos en juego y del impacto de la tecnología en sus operaciones y las oportunidades que brinda.

Esto permitirá determinar de qué manera los procesos de elaboración de políticas y normativas deberían evolucionar. Por ejemplo, a pesar del evidente potencial de innovación tecnológica en términos del beneficio a largo plazo en la eficiencia y la productividad (por ejemplo, disminución de costos de transporte y comunicación, logística y cadenas de suministro globales más eficaces y reducción de gastos de comercialización, todo lo cual abrirá nuevos mercados e impulsará el crecimiento económico), la cuarta revolución industrial también corre el riesgo de crear nuevas formas de división digital y producir una mayor desigualdad. Esto es particularmente cierto no sólo en su potencial para alterar los mercados laborales (Brynjolfsson y McAfee, 2011), sino también los escenarios futuros, en formas que no podemos prever en este momento (Schwab, 2015). Es probable que el resultado general sea una combinación de mayores oportunidades, por un lado, y nuevas formas de desigualdad, por el otro, y que los líderes digitales deban ser conscientes de estas consecuencias, entre otras.

4.b. Facilitadores clave: identidad digital

Desarrollar habilidades para colaborar con la transformación digital implica, también, equipar al sector público con facilitadores digitales clave. Una vez implementada la gobernanza necesaria y habiendo brindado una visión clara, los facilitadores específicos, tales como la identidad digital (ID), se vuelven una prioridad. Los gobiernos en todo el mundo están realizando un gran esfuerzo por establecer la identidad personal en una era digital, ya que es complejo desarrollar políticas y marcos legales que combinen elementos de identificación física y digital.

A medida que los países desarrollan servicios a los que se puede acceder en línea y son brindados a través de un uso compartido y una reutilización más inteligente de los datos en todo el sector público, es

esencial que los países cuenten con un mecanismo que valide y verifique que una persona es quien dice ser. Históricamente, esto fue posible a través de pruebas y verificaciones que tienen lugar mediante un contacto personal, como ocurre con las firmas y las muestras físicas. Sacar el máximo provecho de la transformación que hace posible la ID es más que simplemente digitalizar interacciones analógicas. La ID debe ser comprendida como un elemento de infraestructura de gobierno central y una facilitadora para una provisión de servicios mejorada.

Países como Austria, Canadá, Dinamarca, Estonia, India, Italia, Corea, Nueva Zelanda, Noruega, Portugal, España, Reino Unido y Uruguay han priorizado el desarrollo y la implementación de enfoques de identidad digital (ID) que contribuyen a la transformación de sus gobiernos (OCDE, 2019a). Buenas lecciones aprendidas de estos países indican que adoptar el enfoque correcto en relación con el diseño de un marco para el desarrollo de la ID implica cubrir los cimientos para la identidad en términos de la infraestructura, políticas, gobernanza y soluciones técnicas sobre identidad nacional existentes. Estos factores tienen un impacto importante en su adopción dentro del sector público y entre los ciudadanos, y en las maneras en que la ID puede crear una mayor transparencia en la labor del gobierno y empoderar a los ciudadanos a través de un mayor control de sus datos.

En particular, el análisis comparativo de mejores prácticas aplicadas en distintas partes del mundo indica que es esencial lo siguiente (OCDE, 2019a):

- Garantizar que el hincapié en la ID dentro de la estrategia de transformación digital de un gobierno sea sustentable mediante la provisión de un compromiso financiero y político de largo plazo.
- Identificar o crear un rol de rango superior, responsable de diseñar y producir identidad de acuerdo con la visión establecida por la estrategia de transformación digital del gobierno.

- Considerar el diseño de una gestión de identidad (tanto física como digital) como un proceso integral que abarque toda la vida del ciudadano, desde su nacimiento hasta su fallecimiento.
- Priorizar el desarrollo de una solución de ID para permitirle al ciudadano tener el control de sus datos y ser capaz de otorgar, revocar o brindar permisos de acceso y uso de esos datos.
- Identificar servicios del sector privado prioritarios para el empleo de una ID nacional y establecer una asociación de trabajo para garantizar que las soluciones funcionen tanto para el sector privado como para el sector público.
- Establecer el marco legal y regulatorio adecuado para administrar el uso de las credenciales de ID para acceder a servicios del sector privado, particularmente cuando ello abra la posibilidad de una reutilización de los datos personales.
- Explorar con socios regionales de qué manera la interoperabilidad de la identidad puede facilitar servicios transfronterizos.
- Utilizar la expansión de la identidad digital como una oportunidad para brindar a los ciudadanos una alfabetización digital y una capacitación sobre competencias digitales.
- Incluir la ID como un tema explícito en los controles de gastos, los procesos de control de calidad, el diseño de lineamientos y la capacitación y el desarrollo de competencias. Esto tiene por objeto maximizar la toma de conciencia y la adopción dentro del gobierno y evitar el desarrollo de soluciones duplicadas.
- Asignar fondos para satisfacer las necesidades de los equipos del gobierno a fin de que vean la ID como un servicio confiable y valorado. Esto debería garantizar el diseño de una solución técnica fácil de implementar y asistida regularmente por materiales de referencia, asesoramiento y, de ser necesario,

consultorías. Debería incluir también el apoyo necesario a dichos equipos en la elaboración de análisis claros de costo-beneficio y fundamentos para la identificación de rendimientos de inversión, al plantear argumentos comerciales para una determinada implementación y adopción.

- Revisar los mecanismos a través de los cuales las agencias públicas acuerdan intercambiar datos y brindar pautas y formularios estándar para contribuir a un proceso más eficiente. Esto debería complementar los esfuerzos destinados a implementar estándares de interoperabilidad entre los sistemas preexistentes y los recientemente desarrollados.
- Identificar **indicadores de desempeño clave** relativos al tiempo y al costo involucrados en la provisión de los servicios no compatibles con la ID, para brindar un punto de referencia que permita medir, comparar y demostrar los beneficios de implementar la ID. Publicar esta información como **datos de gobierno abierto** y dentro de los paneles de control, detallando la calidad de la provisión de los servicios.

5. Convergencia de canales de provisión de servicios

La provisión de los servicios constituye el punto de contacto fundamental entre un Estado y sus ciudadanos, residentes, empresas y visitantes. La manera en que los servicios son diseñados y brindados tiene un impacto significativo en la eficiencia alcanzada por los organismos públicos, en la satisfacción de los ciudadanos con su gobierno y en el éxito de una política en cuanto al cumplimiento de sus objetivos. Junto con la integridad de un gobierno, la confiabilidad y la calidad de sus servicios, constituyen factores importantes para afianzar la confianza en el gobierno. La calidad de estas interacciones entre el Estado

y los ciudadanos no sólo define la experiencia de gobierno de los ciudadanos, sino que también influencia las oportunidades a las que estos acceden y las vidas que construyen.

La transformación digital de economías y sociedades está conduciendo a presiones externas para que los gobiernos mejoren la provisión de sus servicios, motivando al mismo tiempo al sector público a impulsar enfoques de diseño para satisfacer más eficazmente las necesidades de los ciudadanos. En este contexto, los usuarios son inflexibles con los servicios que consideran malos al compararlos con experiencias de servicios de alta calidad, ya sea del sector privado o de otros sectores del gobierno. Para satisfacer estas expectativas de calidad cada vez más elevadas, los gobiernos deben enfocarse en comprender la totalidad de la travesía de un usuario a lo largo de múltiples canales, al igual que los procesos internos desarrollados por los empleados públicos, con el fin de identificar posibilidades de transformación de la experiencia completa. Hacer esto puede requerir el ajuste y rediseño de procesos, la definición de estándares comunes y la construcción de infraestructuras compartidas para crear los cimientos necesarios para la transformación. También puede demandar el aseguramiento de interoperabilidad de los distintos organismos públicos para facilitar los flujos de datos que harán posible la generación de servicios integrados de canales múltiples.

Si bien la transformación digital ha afectado todos los aspectos de la vida diaria y reemplazado muchas de nuestras interacciones humanas, el gobierno debe continuar garantizando que los servicios que brinda sean accesibles para todos. Esto significa hacer más que simplemente migrar procesos analógicos a internet. Esta digitalización va de la mano con el establecimiento de culturas digitales por diseño, que transforman los comportamientos de un organismo. El desafío para los gobiernos en todo el mundo es construir una nueva relación entre el ciudadano y el Estado, y el gobierno digital es crucial en la promoción

de un enfoque abierto y orientado al usuario que repiense y rediseñe las interacciones en lugar de simplemente trasladar la burocracia de un canal a otro.

Las iniciativas del gobierno digital implican reconocer el rol del diseño en la satisfacción de las necesidades de los ciudadanos en todos los canales, tanto aprovechando los beneficios de la digitalización como protegiendo a quienes dependen de las transacciones en persona. Dicho diseño necesita ser complementado con recursos prácticos y asistencia técnica para ayudar a los equipos a evitar las limitaciones y los gastos de transformar los servicios uno por vez. Un gobierno digital que cuente con los requisitos para ser **digital por diseño** y un **gobierno como plataforma** podrá llevar la transformación a todos los niveles jurisdiccionales, incluyendo el local, desde los servicios de gobierno de más alto perfil y más sofisticados, hasta los servicios menos desarrollados y equipados (OCDE, 2020c).

La Recomendación de la OCDE enfatiza que el entorno de gobierno digital es aquel ampliamente orientado al usuario, con usuarios que expresan sus exigencias y necesidades y participan en el diseño de los servicios, contribuyendo de este modo a dar forma a la agenda de políticas del gobierno, sus resultados y la naturaleza de los servicios personales integrados (OCDE, 2016). Como resultado, un enfoque de gobierno digital representa una importante evolución respecto del modelo de provisión de servicios de la era del gobierno electrónico.

El enfoque principal de las etapas iniciales del gobierno electrónico consistía en ofrecer nuevos canales de relación directa con los usuarios para un acceso más conveniente a la información y los servicios públicos haciendo un mayor uso de las «tecnologías de la información y comunicación, particularmente la internet, para alcanzar un mejor gobierno» (OCDE, 2003). La intención era brindar servicios adaptados a las necesidades individuales, maximizando el valor para los

ciudadanos y las empresas, reduciendo a la vez los costos o mejorando la eficiencia para la administración (OCDE, 2005). Si bien los gobiernos eran conscientes de la necesidad de una reingeniería de los procesos, el apuro por poner los servicios en línea derivó en que la mayoría de los servicios conservaron la estructura y los límites institucionales del gobierno. Conceptos tales como «área administrativa» y «atención al público» todavía eran concebidos como independientes y se prestaba una atención insuficiente a la participación del ciudadano en el desarrollo y la provisión de los servicios. La apertura de puntos de acceso en línea (ventanillas únicas para múltiples trámites) generó importantes oportunidades para simplificar el acceso a los servicios y volverlo más conveniente, incluso a pesar de que generalmente no se correspondía con una provisión de servicios verdaderamente unificada.

De hecho, los gobiernos muchas veces perdieron la oportunidad real de mejorar la integración entre el área administrativa y los procesos administrativos, con vistas a incrementar su eficiencia y productividad y ofrecer, a la vez, experiencias de servicios ágiles para los usuarios. Por otro lado, mientras los países buscaban evolucionar en la provisión de servicios en línea desde un enfoque centrado en el gobierno a un enfoque centrado en el ciudadano (o el usuario) –siendo este último enfoque el más consciente de las necesidades de los usuarios y el que busca anticiparse a esas necesidades–, a menudo seguían estando muy orientados a la provisión de los servicios, ya que no tenían la urgencia de llevar a los usuarios al centro del proceso del diseño y la provisión de los servicios. Esto con frecuencia resultaba en un obstáculo para el uso de los servicios del gobierno electrónico por parte de los usuarios (OCDE, 2009).

A pesar de los ideales, el resultado de la evolución de la provisión de los servicios fue, en muchos casos, un conjunto desordenado de diferentes canales de servicio y redes de provisión. En ocasiones,

las ventanillas únicas brindaban una selección de servicios agrupados en torno a un conjunto de necesidades en particular, mientras mantenían a la vez sitios web que también ofrecían los servicios individuales. En otros casos, organismos más pequeños colaboraban entre sí para combinar sus esfuerzos, mientras organismos de mayor tamaño, con los recursos para operar independientemente, dirigían sus propias oficinas, sitios web y centros de atención telefónica.

El proceso de digitalización del gobierno electrónico con frecuencia ha conducido a una multiplicación del número de canales de interacción disponibles. Si bien en la mayoría de las administraciones públicas de muchos países al menos ciertos canales tradicionales continúan disponibles (por ejemplo, las transacciones presenciales, la asistencia telefónica y las cartas), la adopción y la diversificación de canales digitales a lo largo de la última década ha sido notable. Pocos ejemplos pueden ser tan ilustrativos en términos de amplitud y potencial como es el caso del teléfono inteligente. Ya desde 2011, la OCDE resaltaba cómo, en un contexto de avances sin precedentes de las tecnologías de comunicación móvil, los gobiernos estaban convirtiéndose en gobiernos «móviles», reconociendo el valor de los dispositivos móviles para una gobernanza resolutiva orientada al logro de mejoras medibles en el desarrollo social y económico, la provisión de servicios públicos, la eficiencia operativa y una participación activa del ciudadano (OCDE, 2011).

Existe una complejidad considerable de ajustes exigidos para la provisión de servicios según estas tendencias. Pero, también, importantes oportunidades para que los gobiernos pongan a los usuarios de los servicios en un primer plano desde el principio, dejando que sus necesidades sean los motores de las decisiones relativas al contenido de los servicios y los canales de provisión de los mismos. Este es el elemento central de los enfoques de provisión de servicios orientados al usuario.

Estos enfoques implican un alto nivel de atención a la experiencia del usuario en sus interacciones con la administración, al igual que el reconocimiento de los gobiernos y su capacidad para hacer participar a segmentos relevantes de la población en el momento relevante del diseño y la provisión de los servicios.

La agenda del gobierno digital de varios países ha comenzado a asumir este legado en sus aspectos técnicos y de infraestructura, adoptando un enfoque orientado al usuario y reconociendo que si el ciudadano estuviera colocado en el centro de un enfoque en particular, nada de este confuso desorden existiría. Un número significativo de los países de la OCDE ha desarrollado estrategias de provisión de servicios de canales múltiples en formatos que preservan, en la medida de lo posible, la preferencia de canales de los usuarios. La multiplicación de canales maximiza la elección y las posibilidades por parte del usuario, pero la experiencia perfecta en todos los canales se basa en el intercambio eficaz de datos entre plataformas. Esto continúa siendo un desafío en muchos casos. Superar este desafío es parte de lo que caracteriza a la transición de un gobierno electrónico a un gobierno digital: utilizar eficazmente los datos compartidos como la base para la provisión de servicios a través de canales múltiples. No obstante, este enfoque también subraya limitaciones existentes de servicios específicos de cada sector, de interoperabilidad de datos y de enfoques colaborativos y sistémicos. La naturaleza transformadora del gobierno digital reside en su necesidad de un enfoque integral orientado al rediseño de los servicios de interacción directa con el ciudadano y de los procesos de las áreas administrativas que yacen detrás de los mismos. También reside en la capacidad de cambiar las prácticas subyacentes de elaboración de políticas, para que se orienten al ciudadano y se basen en la interacción y la colaboración de un número mayor de actores, de adentro y fuera del sector público.

En términos prácticos, el gobierno digital brinda una oportunidad para desarrollar servicios integrales punta a punta, que entiendan la interacción que se da al resolver un asunto determinado que involucra procesos analógicos (tales como una carta inicial), las transacciones presenciales, los contactos telefónicos y los servicios digitales. En consecuencia, el enfoque del gobierno digital relativo al diseño y la provisión de servicios no implica un enfrentamiento entre lo digital y lo analógico, sino una estrategia y una metodología que priorizan la comprensión de las necesidades del usuario y el diseño de enfoques que puedan satisfacerlas.

6. Midiendo el cambio

El gobierno digital es una etapa clave en el camino de la transformación digital, que permite a los gobiernos avanzar sobre lo ya logrado gracias a sus inversiones en el gobierno electrónico. Es importante medir y evaluar la evolución en su maduración para calcular y direccionar medidas futuras. El presente artículo ha destacado los numerosos desafíos vinculados a la transición hacia un gobierno digital. Esta complejidad parece reflejarse en los resultados de la versión piloto del Índice de Gobierno Digital 1.0 de 2020 (OECD, 2020d), cuyo propósito es ayudar a medir y comprender de qué manera los gobiernos se encuentran realizando la transición de un gobierno electrónico a un gobierno digital. El IGD muestra que, por el momento, los países están avanzando lentamente hacia niveles plenos de madurez digital.

Conclusiones

Las tendencias de la transformación digital en las vidas de las personas tendrán importantes implicancias en la creación de expectativas en relación con los gobiernos y el ecosistema en el cual operan. Los

gobiernos solo pueden dar forma a la digitalización de manera constructiva y maximizar los beneficios para el público si revisan en profundidad sus estructuras organizativas y procesos de negocio, desarrollan nuevas competencias y aprovechan las que existen fuera del sector público, a fin de superar la mentalidad analógica y ser capaces de utilizar activos estratégicos –incluyendo datos y tecnología– para anticiparse a las prioridades de la sociedad y resolverlas.

Si demuestran que son hábiles para evolucionar en forma constante para adaptarse a un mundo de cambios disruptivos, sometiendo sus estructuras a niveles de apertura y eficiencia que les permitan mantener su margen competitivo, los gobiernos lograrán sobrevivir con éxito. Los resultados del IGD 1.0 de 2020 muestran que hay mucho terreno que los gobiernos deben cubrir si desean alcanzar una mayor madurez en su gobierno digital y avanzar así en su transformación digital.

Referencias bibliográficas

Brynjolfsson, E.; McAfee, A. (2011). *Race Against the Machine, How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly. Transforming Employment and the Economy*. Lexington, Massachusetts: Digital Frontier Press, Lexington.

Downe, L. (2020). Good Services: How to Design Services that Work. Amsterdam: BisPublishers.

OECD (2003). *The E-Government Imperative. OECD Digital Government Studies*. París: OECD Publishing.

OECD (2005). *E-Government for Better Government*. OECD Digital Government Studies. París: OECD Publishing.

OECD (2009). *Rethinking e-Government Services. User-centred approaches*. OECD Digital Government Studies. París: OECD Publishing.

OECD/International Telecommunication Union (2011). *M-Government: Mobile Technologies for Responsive Governments and Connected Societies*. OECD Publishing. http://dx.doi.org/10.1787/9789264118706-en.

OECD (2014). *Recommendation of the Council on Digital Government Strategies*. OECD.

OECD (2016). *Digital Government in Chile: Strengthening the Institutional and Governance Framework*. OECD Digital Government Studies. París: OECD Publishing, . http://dx.doi.org/10.1787/9789264258013-en.

OECD (2017). *G20 Compendium on the Use of Open Dta for Anti-Corruption*. G20 Anti-corruption Working Group. París: OECD Publishing.

OECD (2017a). *Going Digital: Making the Transformation Work for Growth and Well-being*. [DSTI/CDEP/GD(2017)2], https://one.oecd.org/document/DSTI/CDEP/GD(2017)2/en/pdf.

OECD (2019). *The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studies*. París: OECD Publishing, https://doi.org/10.1787/059814a7-en.

OECD (2019a). OECD Digital Government Studies. París: OECD Publishing, https://doi.org/10.1787/9ecba35e-en.

OECD (2020 próximo a publicarse). *The COVID-19 Crisis: A Catalyst for Government Transformation?* OECD.

OECD (2020a, próximo a publicarse). *Manual sobre la gobernanza de gobierno digital.* OECD.

OECD (2020b). *The OECD 2019 Open Useful Reusable Data (Ourdata) INDEX © OECD 2020*.

OECD (2020c), *Digital Government in Chile – Improving Public Service Design and Delivery*. OECD Digital Government Studies. París: OECD Publishing, https://doi.org/10.1787/b94582e8-en.

OECD (2020d próximo a publicarse). *Policy Paper - OECD Digital Government Index*. OECD Publishing.

Schwab, K. (2015). The Fourth Industrial Revolution. What it Means and How to Respond in Foreign Affairs, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

BARBARA UBALDI. Directora Interina de la División de Gobiernos Abiertos e Innovadores y Directora de la Unidad Gobierno y Datos Digitales del Departamento de Gobernanza Pública de la OCDE. Lidera las evaluaciones de países, el trabajo sobre el uso de tecnologías emergentes en los gobiernos para mejorar su apertura, eficiencia e innovación, y es responsable de monitorear la implementación de la Recomendación de la OCDE sobre Estrategias de Gobierno Digital y del Índice de *Nuestros Datos* de la OCDE y el Índice de Gobierno Digital. Se desempeñó durante ocho años como Oficial de Programas dentro del Departamento de Asuntos Económicos y Sociales de la Organización de las Naciones Unidas, y adquirió una amplia experiencia trabajando en gobiernos digitales, tecnologías de la información y la comunicación (TIC) y en la gestión del conocimiento para el desarrollo. Ganadora de una beca Fulbright. Licenciada en Administración Pública de la Northeastern University de Boston. Fue incluida por la plataforma Apolitical en el listado de las 20 figuras más influyentes del mundo en el campo del gobierno digital durante 2018 y 2019.

CAPÍTULO 7

Aprendizajes y recomendaciones para una efectiva transformación digital

Eduardo Martelli

Introducción

Resulta claro que el único camino de los gobiernos para incorporarse definitivamente al siglo XXI es digitalizando todos sus procesos y manejando la información –que es su principal activo– a través de las herramientas que la revolución informática ha puesto a su disposición.

Este trabajo intenta echar luz sobre por qué han sido tan difíciles los procesos de transformación digital, y qué aprendizajes y recomendaciones se pueden aportar desde una óptica práctica. Asimismo, durante el recorrido permitirá ver cómo generar las oportunidades para lograr tal transformación, qué trampas deberán sortearse, cuáles son errores conceptuales frecuentes (v.g., cómo elegir soluciones informáticas que habitualmente bloquean su concreción y complican la simplificación); qué estrategias deben adoptarse para no fracasar (cómo adoptar una real interoperabilidad); cómo la transformación digital debe conducir a que el Estado haga un uso inteligente de sus datos;

y, finalmente, cómo toda esta transformación impacta sobre la cultura organizacional, de modo que conduzca a una nueva administración pública.

La «aventura» de digitalizar íntegramente los procesos de una organización estatal trae beneficios en múltiples niveles. Por un lado, permite capturar sus datos y procesar la información –que es su principal activo– a través de herramientas que harán posible una completa tramitación a distancia, incorporando a ciudadanos y empresas a sus procesos. Por otro, se logra automatizar, sobre la base de los datos recogidos, muchas de sus decisiones con la aplicación de tecnologías de *machine learning*. Y finalmente, se implementa el *big data* en el análisis de datos, en pos de entender el comportamiento digital de la organización[1]. En última instancia, esta transformación digital redundará en una mejor toma de decisiones en sus políticas y permitirá la agilización, simplificación y desburocratización de sus procesos.

Hablamos de generar un nuevo paradigma de gestión, en donde los conceptos y valores clave vinculados a la nueva administración pública serán: seguridad, calidad, inteligencia, adaptabilidad al cambio, innovación y capacidad de aprendizaje (Ramió, 2017).

Desafortunadamente, el proceso de digitalización en el Estado se ha visto habitualmente retrasado por una conjunción de diversos motivos, tales como: miedo al cambio, autoprotección jurídica, retención de poder o información y corrupción. Esto se ve reflejado en el arraigo de procesos burocráticos en soporte físico de papel y la recurrente resistencia a la despapelización. Así, el valioso caudal de datos

---

1 El concepto de *digital behaviour* fue introducido por el gobierno del Reino Unido para representar el análisis de datos y comportamiento administrativo bajo operaciones digitales.

residentes en papel resulta poco accesible, poco transparente, no reutilizable e ineficaz. Estas condiciones han convertido al Estado en un «Estado bobo», opaco y muy permeable a prácticas corruptas.

Pero ¿cuál ha sido el factor preponderante en el atraso en la transformación digital de los trámites administrativos? ¿Qué explica la alta tasa de fracasos en los proyectos de reforma del Estado? Seguramente la respuesta haya que buscarla en la creencia generalizada de que tanto la reingeniería como la simplificación son etapas previas a la digitalización. Esta equivocación ha aumentado sus costos y generado la necesidad de adoptar decisiones políticas y jurídicas que indudablemente demoran todo el proceso o, directamente, lo frustran.

Asimismo, si se quiere abordar bien la problemática y no fracasar, resulta importante preguntarnos: ¿cuál es el motivo del arraigo de esta creencia generalizada? La respuesta reside en las recurrentes decisiones informáticas equivocadas con respecto a cómo se debe abordar el proceso de digitalización, al elegir soluciones informáticas del tipo ERP (*enterprise resource planning*) para digitalizar los procesos en el Estado, que, aunque exitosas en el ámbito privado, no se adaptan bien a la lógica del ámbito estatal. Esta creencia se ha visto reforzada por asesores, prestigiosas consultoras internacionales e infinidad de *papers* que pregonaron un paradigma erróneo, al no comprender cabalmente la naturaleza y magnitud del problema que implican la tramitación y los formalismos que se requieren en el Estado.

La buena noticia es que existen otras soluciones informáticas del tipo GDE (gestión documental electrónica), que permiten procesos de digitalización mucho más económicos, flexibles y rápidos de implementar, ya que no precisan realizar reingenierías ni simplificaciones previas. Enfocando el documento como la pieza central de su estrategia, se logra alcanzar su autenticidad y protocolización, el cumplimiento de las reglas del derecho administrativo de sus contenedores

(expedientes, carpetas, legajos, registros, etc.) y la captura de los datos a través de formularios inteligentes.

La gran diferencia entre sistemas del tipo ERP y los del tipo GDE es que los primeros utilizan solo bases de datos con registros de información totalmente estructurados[2], haciendo rígida y costosa su implementación. En cambio, los segundos contienen ambos tipos de datos: estructurados y no estructurados[3]. Estos últimos son, por lejos, los más comunes en los Estados –notas, informes, actas, dictámenes, certificados. Por ende, los sistemas más aptos para integrarse a la lógica de la administración pública son los que se basan en datos no estructurados, y estos son los del tipo GDE.

La experiencia recogida durante ocho años de gestión en el Gobierno de la Ciudad Autónoma de Buenos Aires (en adelante GCABA) y cuatro años en el Gobierno de la Nación Argentina (en adelante GNA) –donde se adoptaron soluciones del tipo GDE– permite identificar varios aprendizajes que pueden resultar de interés para todos aquellos que tengan una responsabilidad directa o indirecta en procesos de transformación digital de las administraciones públicas[4].

---

2 Los datos estructurados son los definidos campo a campo en una base de datos, donde, para su carga, se necesitan programas que controlen y «apunten» a esos campos (espacios) definidos de la base de datos y, por ende, su valor es interpretado a través de diccionarios de datos. Por lo que un ERP requiere de la definición previa de cada uno de los campos a utilizar y su valor correspondiente, típico de los sistemas transaccionales de las agencias de impuestos o de los bancos, compañías de seguros y comerciales.

3 Los datos no estructurados son los que se cargan en un «espacio digital» en forma libre, como se realiza en un documento de Word, que controla muchas funciones, pero los datos son de texto libre y su interpretación es solo a través de la lectura de personas o por programas de *machine learning* - inteligencia artificial.

4 Para dimensionar esta experiencia, es preciso indicar que el GCABA contaba en 2014 con 125.000 empleados/funcionarios y 1.300 procesos. Por su parte, el GNA, en 2017, agrupaba a 420.000 empleados/funcionarios y no menos de 4.200 procesos.

El foco de cualquier proceso de transformación digital también debe estar puesto en hacer fluir la información, de forma tal de dotar de eficacia y eficiencia a la gestión de toda la organización, pero principalmente a la capa superior de autoridades, para que tomen mejores decisiones, con más agilidad y, en consecuencia, en mayor volumen; y a su vez, permitir que llegue a la ciudadanía en forma de más servicios de calidad y de forma transparente. Al mismo tiempo, para ser eficaz debe ser integral, no debe dejar fuera a ninguna institución estatal. Es decir, la transformación de la gestión documental –del papel a la electrónica– es una condición necesaria, aunque no suficiente, para modernizar el Estado y hacer fluir apropiadamente la información.

Debemos entender que la gestión sobre la base de la «tecnología» en papel dificulta la mejora de cualquier servicio o prestación por parte del Estado. Llevada al extremo, la tiranía del papel puede generar una imposición en grado extraordinario de un poder, fuerza superior por la que el Estado se centra en los propios fines y no en los de los ciudadanos a los cuales debe servir (Clusellas, Martelli, Martelo, 2016).

La implementación de sistemas del tipo GDE no representa un proceso inspirado en una visión eficientista. Responde a una inspiración profunda de acompañar la reforma administrativa para orientarla a la optimización, la simplificación de trámites para el ciudadano y el uso inteligente de los datos. En razón de su naturaleza, de su forma particular y de su duración, la despapelización viene de la mano de una revolución tan radical, que muchas veces es difícil de percibir en su verdadera dimensión.

Esta transformación puede parecer simple en teoría, pero en la práctica su implementación es por demás complicada y requiere de una alta dosis de voluntad política y jurídica, ya que conduce a políticas y procesos de agilización, simplificación y desburocratización –no

son sinónimos, como veremos más adelante–, que persiguen esencialmente complejos objetivos, a saber:

- Profundizar una administración pública al servicio del ciudadano, en un marco de eficiencia, eficacia y calidad en la prestación de servicios.
- Aumentar la transparencia, confianza, buena fe y colaboración eliminando controles innecesarios.
- Facilitar el acceso del ciudadano a los servicios que brindan los organismos del Estado, mediante el uso de herramientas tecnológicas de autenticación y que posibiliten un acceso remoto.
- Simplificar los trámites administrativos, haciéndolos más sencillos y menos complicados.
- Eliminar cargas al ciudadano en los casos en que se necesite presentar determinada información, dato, documento o certificado que deba ser emitido por otra entidad o jurisdicción del sector público nacional.

La tendencia al fracaso en la eliminación del papel en la tramitación es global. De hecho, ha habido un sinnúmero de esfuerzos en pos de la «despapelización» gubernamental, pero los mismos han sido, en su gran mayoría, parciales o incompletos, dados los errores en las herramientas informáticas elegidas y el alcance de sus objetivos. Hay honrosas y contadas excepciones, como las de Estonia, Dinamarca o Noruega.

El último componente a analizar en pos de alcanzar el éxito en procesos tan complejos como lo es la transformación digital exitosa del Estado, es cómo lograr dotarlo del sentido de urgencia. Pues, como lo hemos visto una y otra vez en distintos procesos de reforma, si no cuentan con una dosis de urgencia, los cambios importantes

encuentran grandes barreras que sortear y toman mucho tiempo. Lo cual es aplicable a casi cualquier tipo de organización, pero representa un problema agravado en el caso de los gobiernos, ya que los mismos cuentan con períodos de tiempo acotados a sus mandatos y lo urgente suele postergar lo importante. **En los gobiernos, el recurso más escaso es el tiempo**.

1. Crisis y oportunidad

La experiencia de la pandemia del COVID-19 nos revela claramente dos de los aspectos tratados: a) hasta qué punto la implementación de sistemas del tipo GDE representó un activo central para que las administraciones públicas pudieran tener cientos de miles de servidores públicos realizando a distancia –«teletrabajo»– sus tareas habituales de carácter administrativo; y b) que la urgencia manifestada por administraciones públicas que no poseen este tipo soluciones informáticas y que han casi detenido su operatoria ha generado una notable oportunidad de cambio de paradigma en pos de la transformación digital. Tema no menor, ya que la digitalización de los gobiernos de la región no ha tenido un desarrollo muy alentador. Solo seis de los países de América Latina están entre los 50 más digitalizados del mundo (Roseth, Reyes y Santiso, 2018).

La naturaleza de las crisis, las cuales crean una ventana de oportunidad para la transformación digital, puede variar enormemente. Dos buenos ejemplos de ello son Estonia, donde a fines de la década de 1990 la nación estaba emergiendo de un pasado soviético que dejaba muy poca infraestructura administrativa detrás, y el Reino Unido, que a finales de la década de 2000 estaba saliendo de una recesión importante y la necesitaba para reducir un déficit fiscal sustancial. Si bien el contexto político general puede ser diferente en cada caso, la

crisis es una oportunidad de creación de nuevas instituciones digitales (Bracken y Greenway, 2018).

A la hora de implementar procesos de transformación digital existen cuatro factores clave de éxito, donde el cuarto es el sentido de la urgencia:

a. En primer lugar, la innovación debe basar toda la lógica y la estructura de los sistemas sobre el documento (y sobre los procesos, en una segunda fase). No se trata de replicar en soporte digital lo que otrora se hacía en papel, sino de confluir hacia un rediseño permanente de sistemas y procesos. El denominador común de todos los procesos es el derecho administrativo y su protocolización.
b. En segundo lugar, se debe reunir un equipo interdisciplinario para los aspectos tecnológicos y jurídicos. A su vez, voluntad política para la implementación.
c. En tercer lugar, el proceso de cambio debe ser integral en otro sentido. No debe darse ninguna cabida al papel (ni siquiera por excepción).
d. En cuarto lugar, debe darse al proceso un sentido de urgencia total, entendiendo que el recurso más escaso en el Estado es el tiempo.

Finalmente, debemos entender que los efectos últimos de este cambio, sin lugar a dudas, trascienden el nivel técnico y afectan profundamente la cultura organizacional. Si bien esta transformación cultural tiende a demorar años, la progresiva y masiva incorporación ciudadana a los nuevos modos de tramitación va generando nuevas conductas en la organización, mejoras en la agilidad de los trámites, el control de las operaciones y la transparencia (Clusellas, Martelli y Martelo, 2014).

El Edificio Uspallata: la nueva sede del Gobierno de la Ciudad Autónoma de Buenos Aires es un ícono ambiental y completamente paperless. Ya no posee archivos donde guardar expedientes en papel.

2. Cómo sortear las trampas burocráticas para alcanzar una transformación digital inteligente

En los últimos años, la estructura de los Estados y sus administraciones ha crecido a un ritmo sostenido en muchos países. Ello se

debe, en parte, al incremento de las demandas sociales, la búsqueda de respuestas a problemas complejos y la necesidad de proveer mejores servicios a la ciudadanía. Sin embargo, también hay crecimientos que no se explican por ninguna de estas razones.

El crecimiento no siempre es orgánico. Es usual encontrar funciones obsoletas, superpuestas y con excesivo personal en su dotación, que deben ser revisadas no solo por el gasto excesivo que insumen.

Si bien ha habido innumerables intentos de reducción de la estructura estatal, numerosos estudios han demostrado que el tamaño *per se* de los Estados poco indica sobre los niveles de eficiencia alcanzados.

Ahora bien, si la tendencia habitual parece que es tener Estados grandes y complejos para dar respuestas a las cada vez más sofisticadas y heterogéneas demandas sociales, la orientación de los gobiernos debe focalizarse en tratar de simplificar la tramitación.

Uno de los aprendizajes más destacados recogidos en la tarea de transformar digitalmente la administración pública nacional y subnacional guarda relación con la importancia de batallar contra ciertas prácticas que conspiran contra la reforma de la administración.

En ocasiones, los procesos administrativos de los gobiernos no persiguen la resolución eficiente del trámite en sí mismo, sino el refuerzo de la formalidad y la autoprotección del funcionario de turno. Cuando esto sucede, se generan procesos innecesariamente engorrosos, con etapas formales que no agregan valor, lentifican el logro de resultados y quitan transparencia. Un ejemplo significativo de este tipo de procesos resultó ser el de la designación de un nuevo empleado público en la administración pública nacional. Un primer análisis reveló la existencia de 35 pasos obligatorios y una demora que podía alcanzar hasta 140 días. El grado de autoprotección jurídica resultaba irracional frente al grado de necesidad y urgencia que, con frecuencia, acompañaba la incorporación de personal. En términos de

eficiencia, el control no resultaba proporcionado al hipotético daño que se buscaba evitar[5].

Otra práctica muy arraigada guarda relación con la invocación del principio de equidad para denunciar o bloquear procesos de transformación digital. Un ejemplo de este tipo de prácticas resultó ser la objeción interpuesta a un trámite administrativo bajo la apelación a la supuesta incapacidad de los adultos mayores para incorporarse al mundo digital. Analizada la cuestión, resultó que este segmento representaba menos del 5% de la interacción administrativa cuya digitalización se pretendía. El desarrollo posterior permitió comprobar, además, que en la práctica estas poblaciones se incorporan perfectamente y llegan a ser, en ocasiones, los mejores usuarios.

Estos ejemplos revelan la necesidad de estar prevenidos frente a algunos errores o peligros que amenazan recurrentemente la instancia de diseño normativo de la innovación pública. Se mencionan otros problemas típicos:

a. Con frecuencia, se presume la necesidad de derogar normativa que supuestamente impide la modernización en algún aspecto de un proceso. Al mismo tiempo, se presume la ineludible necesidad de crear normativa nueva que habilite las innovaciones pretendidas. Esto se trata de un mito porque, en la mayor parte de los casos, la reforma puede hacerse apelando a la normativa vigente, eventualmente procurando una interpretación más abierta y menos sesgada que la existente. Por influencia de este mito tan arraigado, hemos visto casos de nuevas normativas que no incluían ningún tipo de eliminación de pasos del proceso en cuestión y pretendían promover innovación.

5 Ver Decreto 355/2017, Decreto 733/2018 y sus Resoluciones Complementarias.

b. Cuando una nueva normativa resulta necesaria, es importante no sucumbir frente a la tendencia de crear normativa parcial y complejizar, de este modo, las exigencias burocráticas. Cuando esto sucede, los empleados administrativos deben realizar un esfuerzo de «bordado» o *patchwork*, que involucra los nuevos artículos vigentes, los artículos derogados o los parcialmente derogados. Esto resulta engorroso y muy poco práctico. Por el contrario, se trata de promover, tal como recomienda la OECD, que cada vez que se cree una normativa, se eliminen dos normas anteriores en el mismo acto de creación (OECD, 2011).
c. Es importante no ceder ante la tentación de impulsar la creación de registros, matrículas habilitantes, certificaciones necesarias para algún proceso sin haber hecho un previo análisis de impacto en el mercado. Es indispensable identificar cuánto costará, cuánto demorará, qué beneficios va a traer la innovación para la producción o para el ciudadano. Puede resultar un paso obvio, pero sorprende ver la cantidad de veces en que resulta omitido.
d. Es imperioso que, al crear normativa procedimental, se determinen los plazos máximos de su implementación o cumplimiento, algo que generalmente no sucede. Asimismo, se debe propender, en los casos en que fuere posible, a normativas en las que el silencio de la administración sea entendido como otorgamiento o concesión de lo requerido.
e. Cuando estas tendencias negativas se extienden y toman cuerpo en la administración pública, podemos decir que estamos en presencia ya no de tendencias aisladas, sino de una verdadera «enfermedad de la burocracia».

3. Desburocratización, agilización y simplificación

Como hemos visto, en la transformación digital, más que hacer una verdadera reingeniería, debemos buscar modificar malos hábitos y comportamientos que no agregan valor a un proceso y lo vuelven lento y engorroso para el ciudadano.

En este marco, es preciso distinguir entre desburocratización, agilización y simplificación, ya que estos tres términos han sido usados muchas veces como sinónimos y sus alcances son muy distintos. Cada uno de estos esfuerzos requiere distintas acciones y opera de distinta manera sobre la estrategia de la transformación digital.

La **desburocratización** implica la eliminación completa de una tarea o un conjunto de tareas. Por ejemplo, dar de baja un trámite, descartar un registro o suprimir un organismo. Hasta cierto punto, su implementación puede resultar la forma más sencilla de reforma, pues su análisis es global y requiere solo de nueva normativa y voluntad política.

La **agilización** implica buscar, a través de herramientas informáticas, la reducción de los tiempos de un trámite dado y la captura de sus datos, sin entrar en una discusión sobre si la lógica del trámite es correcta o no. Si bien puede considerarse que esta forma de resolver el problema es muy superficial, con frecuencia resulta la manera más provechosa –si no la única– de encarar una reforma integral de la gestión pública.

La **simplificación**, en cambio, implica un cambio normativo o una reingeniería del proceso, o ambos en forma simultánea. Para lograrla, no sólo debe repensarse la lógica de la cadena de valor, sino también promoverse cambios normativos. Es sabido que estos, en el Estado, conllevan grandes discusiones y requieren consensos muchas veces difíciles de alcanzar.

La ausencia de una línea de base sobre los trámites vigentes (cuántos son, cuánto tardan, qué dependencias intervienen) constituye una de las mayores dificultades con las que se enfrenta quien desea promover la transformación digital en la administración pública. Al aplicar un proceso de agilización, no es necesario avanzar en primer lugar con un inventario total de los trámites del Estado, tarea de por sí titánica. El inventario se va autogenerando y obtenemos un mapa de los procesos y los datos del Estado con solo desarrollar la tarea. Al ir informatizando las distintas reparticiones, en cada uno de sus trámites va surgiendo espontáneamente y objetivamente el camino recorrido (*workflow*), quiénes lo usan, cuánto tarda su tramitación, qué documentos requiere y, lo que es más importante, se capturan todos los datos del trámite para su posterior utilización en el análisis de su comportamiento digital y simplificación.

La agilización permite transparentar toda la tramitación, conocer en todo momento dónde está cada trámite, quién lo tiene a su cargo, cuánto tarda, contar con sus datos, etc., con lo cual se logra un extraordinario cambio de conducta organizacional y garantizando la transparencia de las actuaciones para que no puedan ser modificadas o posdatadas, dificultando la discrecionalidad y la corrupción.

El propio tamaño de la organización suele ser un importante obstáculo para el proceso de simplificación, pues quienes poseen la voluntad política decisoria que requieren los cambios normativos, en general, no tienen el grado de conocimiento detallado necesario para expresar una determinación de este nivel operativo. Entonces, para simplificar se arman comisiones en las que muchos opinan, pero en las que ninguno tiene una real capacidad resolutiva. De ello resultan prolongados períodos de debate que engendran soluciones de compromiso que casi nunca resultan las óptimas.

La experiencia recogida indica claramente la conveniencia de avanzar siempre primero en el camino de la agilización, como requisito previo para un eventual un proceso de simplificación. Este paso previo resulta imprescindible, porque permite contar con la información necesaria para desarrollar un debate racional, basado en datos ciertos y no en presunciones y consideraciones de orden emocional.

4. Estrategia tecnológica de abordaje de la transformación

A nivel teórico, es muy razonable primero racionalizar y simplificar, y posteriormente digitalizar. El problema es que en la práctica resulta muy complicado y, en muchas ocasiones, paraliza el proceso. La reingeniería de procesos es muy compleja y, además, suele enfrentarse a dinámicas de resistencia al cambio por parte de los empleados públicos (Ramió, 2019).

Esto exige abordar la simplificación de un modo completamente diferente al modelo habitual, sostenido por las más prestigiosas consultoras internacionales –KPMG, PWC, EY, Deloitte, entre otras. Su error reside en que parten de la base de que la digitalización se debe promover a través de sistemas transaccionales clásicos (en adelante *ERP*, por sus siglas en inglés). Debido a que su implementación y modificaciones posteriores son muy costosas, cuando se aborda este tipo de reformas, se procura un abordaje de la integralidad de los procesos, desde el inicio y hasta su estado final.

Sin embargo, cualquiera con cierta experiencia en la gestión pública latinoamericana sabe que lograr la redefinición completa de un proceso es normalmente muy dificultoso y lleva mucho tiempo. Es más sencillo operar por aproximaciones sucesivas, sin perder de vista –una vez más– que el tiempo siempre resulta el recurso más escaso

con el que cuentan los gobernantes, debido a la finitud de los mandatos. Esta variable raramente es tenida en cuenta en su real dimensión. Lamentablemente, los funcionarios permanentes no tienen la posibilidad de llevar adelante estos cambios.

Por esta razón, al momento de promover una transformación digital de la administración, se sugiere considerar *softwares* de gestión que operen bajo la forma de una red de módulos integrados. Esa fue la filosofía que impulsó la creación de un sistema del tipo GDE, que fue implementado tanto en el GCABA como en el GNA.

Este sistema puso a disposición de todos los usuarios una plataforma informática para el procesamiento completo de todos los documentos oficiales en formato digital y con firma digital, más todos los trámites en forma electrónica. Esta plataforma incluyó la gestión de todos los registros, las comunicaciones internas y externas, más un conjunto de herramientas como servicios API (interfaz de programación de aplicaciones) y diseño de formularios activos del tipo SDK (kit de desarrollo de software).

El aspecto diferencial de un sistema del tipo GDE como plataforma de gestión administrativa reside en que pone el foco en la generación y gestión de documentos en forma independiente del expediente u otro contenedor electrónico. Finalmente, un expediente no es más que un contenedor de una colección de documentos bajo un determinado protocolo y ciertas reglas (Clusellas, Martelli y Martelo, 2014).

La innovación de este enfoque centrado en los documentos y su estructura modular permitió una puesta en marcha de los sistemas en forma extremadamente rápida, habilitando la identificación de cada documento a partir de su numeración y la caratulación de todas las actuaciones en contenedores digitales, del tipo expedientes, carpetas, legajos, registros, etc.; y empalmando la operatoria en papel con una digital en una forma natural y no traumática, donde la regla básica debe

ser que observen todas las reglas del derecho administrativo, tanto para la confección de los documentos como para los contenedores documentales que se deseen usar.

En suma, la ventaja competitiva de un sistema del tipo GDE sobre los tradicionales del tipo ERP consiste, precisamente, en que garantizan flexibilidad, al permitir la incorporación gradual de distintos trámites y módulos para soluciones específicas.

Otro beneficio importante de los sistemas modulares sobre los tradicionales del tipo ERP tiene que ver con el control. Los del tipo ERP con los que se ha tratado de abordar el gobierno electrónico en décadas pasadas son muy difíciles de auditar, pues para ello se deben tener conocimientos muy avanzados en informática. En consecuencia, las administraciones públicas suelen crear sistemas paralelos montados sobre expedientes en papel para documentar las transacciones y permitir su posterior auditoría.

Entonces, aunque los sistemas transaccionales clásicos resuelven la eficacia y la eficiencia de la administración, aun a un alto costo en tiempo y dinero, no resuelven por sí mismos la transparencia en forma sencilla, exponiendo a las administraciones públicas a la corrupción y discrecionalidad. No solo un auditor, también un ciudadano, tiene el derecho a leer en forma sencilla y práctica las razones que fundan una decisión administrativa. Por ello, las «pistas de auditoría» deben ser de muy fácil acceso, para que la transparencia no resulte una quimera.

Además, los sistemas transaccionales del tipo ERP solo permiten leer en pantallas o impresos que reflejan la información que se guardó en una base de datos. Estos registros son relativamente sencillos de modificar, aunque se tomen recaudos. En cambio, un documento firmado digitalmente que registra una transacción es algo inmodificable y al alcance de cualquiera, siendo muy sencilla su comprensión

por parte de cualquier usuario, ya que solo requiere que sepa leer; no hace falta ser un experto informático. En un sistema del tipo GDE, las actuaciones se pueden leer sin un programa intermediario y su seguridad está autocontenida en la firma digital de sus documentos y los expedientes, en un *blockchain*.

Como se menciona en la Introducción, la gran diferencia entre sistemas del tipo ERP y los del tipo GDE radica en que los primeros utilizan solo bases de datos con registros de información totalmente estructurados; en cambio, los segundos contienen ambos tipos de datos, estructurados y no estructurados.

Otra destacable ventaja de los sistemas del tipo GDE reside en que pueden integrarse a los sistemas del tipo ERP tradicionales ya existentes a través de servicios API, lo que permite, de este modo, documentar –generar un documento firmado digitalmente– todas las transacciones que hasta ese momento se registraban solo como un registro en la base de datos y en un expediente papel paralelo. En consecuencia, los sistemas del tipo GDE no son antagónicos, sino complementarios a los del tipo ERP, cuestión que por lo general no es bien entendida, ni por los funcionarios con capacidad de decisión ni por los aquellos funcionarios de áreas de sistemas propensos a mantener el *statu quo*. Un buen ejemplo de esta posibilidad de integración es la articulación entre los sistemas de Compras y Contrataciones (Compr.Ar y Contrat.Ar) y la Ventanilla Única de Comercio Exterior (VUCE) con GDE y Aduana.

En contextos de utilización de sistemas del tipo GDE en lugar de los del tipo ERP, al llevar adelante una reforma administrativa, los pasos a seguir se invierten en relación con lo usualmente conocido (Clusellas, Martelli y Martelo, 2019). De los cinco pasos que lo componen, los tres primeros son propiamente de agilización y recién los dos últimos plantean la reingeniería del proceso.

1. **Despapelización:** instrumentar un sistema **único** de gestión documental electrónica y procesamiento completo de todos los trámites estatales en forma totalmente electrónica.

2. **Reclasificación documental:** revisar los documentos incluidos inicialmente y reconvertir en formularios controlados. Esto permite la estandarización y captura de datos a gran escala, su procesamiento y la fijación de flujos de información con decisiones programadas (*workflows*-motor de reglas).
3. **Simplificación registral e interoperabilidad:** obligar a compartir información entre organismos a través de comunicaciones oficiales o por «servicios de sistemas» (en lo posible del tipo API-REST), procurando evitar que el ciudadano deje de actuar como un «cadete» del Estado.
4. **Revisión jurídica documental:** promover la eliminación de la exigencia de documentación irrelevante, redundante o innecesaria para algunos trámites, o que pudiere ser suplida por declaraciones juradas. En el caso más extremo, determina la eliminación completa del trámite (desburocratización).
5. **Análisis de la información y reingeniería de los procesos**: realizar el estudio de los pasos de un trámite sobre la base del servicio que se quiere lograr, comparándolo con su punto de partida (de existir información confiable al respecto) y planteando un nuevo modelo de tramitación, con la consecuente necesidad de nueva normativa o reglamentación.

Esta secuencia de pasos no implica que, si la importancia de un proceso lo amerita, no se puedan transitar en paralelo. Dado el caso, se tratará de una excepción y no de la norma a seguir.

5. Desafíos de interoperabilidad en la transformación digital

Cualquier transformación digital exitosa del Estado requiere de una real interoperabilidad de los datos y documentos de todos sus integrantes.

Una buena parte de las gestiones y problemas administrativos son comunes o similares en su naturaleza a todas las administraciones, tanto en nivel nacional como provincial o municipal. La naturaleza federal de la Argentina en ocasiones permite avanzar solo mediante esquemas colaborativos centrados en el intercambio de información. Existen en el país numerosas iniciativas provinciales y municipales de tramitación electrónica. Sin embargo, a la hora de considerar la solución de problemas comunes a todas las administraciones, los esquemas colaborativos existentes resultan por lo general incompletos, ineficientes y se prestan a la adulteración. Por ejemplo, la información de personas fallecidas constituye un dato clave para la operación de la Administración Nacional de la Seguridad Social. El dato debe ser capturado por el Registro Nacional de las Personas, como órgano rector de la información e identidad ciudadana. Sin embargo, existe una demora de hasta 120 días para obtenerlo a través de los registros civiles locales, que todavía hoy inscriben todas sus actas en libros papel, incluyendo las defunciones. Las excepciones son el GCABA y la provincia de Buenos Aires, que lo hacen íntegramente en documentos electrónicos con firma digital.

Debe procurarse avanzar más allá, siempre respetando las autonomías provinciales y municipales, pero comprendiendo los enormes beneficios que conlleva avanzar en esquemas colaborativos más extendidos. El desafío de la interoperabilidad no se aplica exclusivamente a la relación intergubernamental. También tiene vigencia puertas adentro de cada administración pública[6].

---

6 Basta recordar que en 2016, la Administración Pública Nacional Argentina estaba compuesta de 23 ministerios, 103 secretarías, 197 subsecretarías, 121 organismos descentralizados o autárquicos, que empleaban 570.000 funcionarios públicos y fuerzas de seguridad a lo largo de todo el territorio argentino.

La fisonomía de la administración pública es la de una inconmensurable estructura de compartimentos estancos. La consecuencia natural, si cada una de ellas procurara sus propias soluciones tecnológicas, sería la conformación de una típica estructura de «silos», en la que resulta muy difícil compartir datos.

Avanzar en la aplicación del criterio de interoperabilidad implica, por el contrario, lograr que los diferentes organismos y dependencias públicas estén interconectados con sistemas compatibles y tengan acceso inmediato y simultáneo a la información y a los datos disponibles para poder operar sobre ellos. Esto permite acceder a los siguientes beneficios:

I. Tener una visión integral e integrada del funcionamiento estatal.
II. Simplificar y agilizar procesos administrativos internos y trámites ciudadanos. El ciudadano deja de ser cadete de la Administración Pública Nacional y se eliminan los gestores e intermediarios en los trámites.
III. Facilitar el acceso ciudadano a información clave y de interés público. Propicia la rendición de cuentas y la transparencia de la gestión de gobierno.
IV. Utilizar en forma inteligente la información disponible.
V. Favorecer la toma de decisiones y la generación de respuestas concretas a problemas complejos, como consecuencia de la obtención de datos agregados y de información de mayor calidad.
VI. Alentar la cooperación entre distintos niveles de gobierno y agencias de la administración pública.
VII. Estimular la cooperación nacional e internacional entre organismos públicos y privados en pos de producir nuevas herramientas (Clusellas, Martelli y Martelo, 2019).

6. El cambio de paradigma hacia un Estado inteligente

La información como tal se empezó a medir en *bits* recién en los años sesenta (porque la compañía Bell aspiraba a cobrar por ella). Para el año 2003, toda la información acumulada en la historia alcanzaba los 5 exabits (Maney, Hamm y O'Brien, 2011). En 2015 se generaban 5 exabits cada 10 minutos (Harari, 2016). En los últimos dos años se generó el 90% de la información total de la humanidad (Delgado, 2016).

En paralelo a este crecimiento exponencial de la información, vemos que la evolución del cerebro humano se ha mantenido relativamente estable desde hace 150.000 años. Resulta sumamente claro que la disponibilidad de información actual supera su capacidad de procesamiento y, por ende, este debe apoyarse en herramientas –computadoras– que lo ayuden a sacar provecho de semejante caudal de información. En términos de impacto, este desafío informático, que elevará la inteligencia humana a un nivel completamente diferente, implica algo equivalente a lo que fue el dominio del fuego hace 150.000 años (Harari, 2014).

El desafío planteado al encarar la transformación digital del Estado ya no puede solo aspirar a volver más simple, ágil, eficiente y digital la burocracia estatal, sino a volverla inteligente. Es preciso superar el concepto de gobierno electrónico (*e-government*) para llegar a un *i-government*, que tenga la capacidad de sacar provecho a la enorme cantidad de información con la que cuenta el Estado.

Cuando una administración pública alcanza el primer gran objetivo de lograr un gobierno electrónico, adquiere una capacidad de acumulación de enormes volúmenes de información digital. El desafío inmediato que se plantea entonces es saber cómo utilizarla. Para usar una figura: los archivos pasan, de ser «cementerios», a ser «yacimientos de datos». En consecuencia, estos quedan accesibles para su explotación mediante las herramientas de *big data* y *machine learning*,

que actualmente se encuentran accesibles de un modo jamás visto, con costos y programas abiertos que están revolucionando el mundo del procesamiento de datos.

Son estas y otras herramientas informáticas las que permiten acceder a un gobierno inteligente. Es «inteligente» aquel gobierno que toma sus decisiones programadas y no programadas basándose en información confiable, y no en meras presunciones o preconceptos; que logra medir los impactos de sus políticas y aprovechar esta medición para retroalimentarse positivamente, convirtiendo la información en un activo de la organización que genere un círculo virtuoso. Este nuevo Estado moderno debe resultar simple, ágil, confiable, cercano, transparente, participativo y, por todo esto, inteligente.

Para lograr usar inteligentemente los datos y la información acumulada por el e-Government y transformarlo en un i-Government, es preciso avanzar por aproximaciones sucesivas:

a. garantizar interoperabilidad de todo el Estado (interoperabilidad documental y de datos);
b. tomar decisiones sobre los procesos (simplificación);
c. estructurar información no estructurada y retroalimentar procesos como una forma de «aprendizaje» con decisiones automáticas, mediante tecnologías de inteligencia artificial - *machine learning* (*big data* - comportamiento digital);
d. incorporar nuevas tecnologías (como *blockchain*) que aseguren intangibilidad y trazabilidad (libros y registros digitales).

El proceso implica, entonces, pasar de tener **«datos»** a tener **«información»**, de tener «información» a tener **«conocimiento»**, y de tener «conocimiento» a aplicar **«inteligencia»**.

Para avanzar en esta dirección, es preciso sortear un estimulante desafío técnico: ¿qué hacer con esta masa gigantesca de datos no estructurados? En la actualidad, es posible realizar un *full index* de todos

los datos no estructurados a un costo razonable. Logrado este paso, con una combinación de técnicas de *big data*, lenguajes naturales (NLP por sus siglas en inglés, *natural language processing*) y lógicas de inteligencia artificial, se puede lograr estructurarlos y procesarlos como datos estructurados, y obtener los resultados que se alcanzan con los sistemas transaccionales clásicos y mucho más.

Hasta ahora ha costado muchísimo persuadir a los funcionarios para que avancen en esta dirección. Por lo general, no poseen formación informática. En ocasiones, si sus asesores informáticos han estudiado y trabajado toda su vida sobre sistemas transaccionales de información estructurada, se convierten en los primeros detractores. Es clave recordarles lo ya dicho, a saber: que los sistemas de este tipo no son antagónicos, sino complementarios a los tradicionales.

Una vez que tenemos los sistemas y los datos, ¿qué nos falta? Resulta indispensable armar equipos interdisciplinarios que, a través de las mencionadas herramientas, analicen el comportamiento digital de la organización. Estudiar los comportamientos para detectar desvíos implica, por ejemplo, identificar tempranamente si un empleado favorece o desfavorece a determinados ciudadanos o empresas. Implica verificar cómo cumplen las reparticiones u organismos con métricas predeterminadas y acordadas de calidad de servicio. Todo ello conduce, a su vez, a dar cumplimiento al compromiso asumido por los gobiernos de consolidar un gobierno abierto. Esto aumenta la capacidad institucional del Estado en difundir sus actos y disponer las bases de datos para su reutilización.

Este modelo de Estado inteligente promueve la cultura de la eficiencia pública, pone énfasis en los resultados y en la calidad de los servicios. Promueve la flexibilidad en la utilización de los medios, pero es exigente en la prosecución de sus fines. Posibilita la inteligencia en

la utilización de los datos y la interoperabilidad; está basado en sistemas de rendición de cuentas tendientes a aumentar la transparencia y estimula la participación ciudadana.

La complejidad de la tarea exige que la transformación digital aquí descripta deba ser impulsada desde un poderoso centro de gobierno que tenga capacidad para traccionar al conjunto. La experiencia recogida demuestra que esta es la única forma de impulsar este tipo de cambios trascendentes sobre una burocracia tan estructurada y rígida.

La implementación de sistemas modulares transversales contribuye a la mejora de la transparencia y la lucha contra la corrupción. Además de agilizar los procesos y mejorar el acceso a la información, combate en forma directa una de las principales amenazas contra el ejercicio responsable y transparente de la gestión pública, que es la discrecionalidad en las actuaciones y en los procesos de toma de decisión, muchas veces presente en la cultura del papel.

En este sentido, la disposición al cambio de los trabajadores del aparato estatal, políticos y funcionarios de carrera resulta de importancia fundamental para el éxito en la implementación del nuevo sistema de gestión y de los fines que persigue.

Algunos directivos públicos creen que los funcionarios de ventanilla son susceptibles a la corrupción y, por lo tanto, se inclinan por limitar su intervención y su poder de decisión. Esto genera indefectiblemente mayor burocratización y demora en los tiempos de resolución de un trámite. La creencia se completa con la presunción de que, del otro lado, el ciudadano estará expuesto a abusos si se facilita mucho el acceso a los servicios públicos y trámites. Lo cierto es que el canal digital de tramitación a distancia (TAD) y los modelos decisorios automáticos de *machine learning* limitan las oportunidades de corrupción

porque un trámite digital es uniforme para todos los usuarios, fácilmente rastreable e impersonal.

La vara de la «vergüenza tecnológica» sigue siendo notablemente baja en la mayoría de las organizaciones grandes y antiguas. Existe el riesgo de que demasiados funcionarios se sientan cómodos mostrando un nivel de incompetencia en tecnología que sería inaceptable en otras áreas como finanzas, economía o política. Es preciso que todo funcionario esté medianamente informado sobre estos conceptos, incluso cuando su tarea no tenga que ver directamente con la implementación de procesos tecnológicos.

7. Un cambio cultural

El alcance real de la transformación digital se mide según el grado en el que son transformados y simplificados los procesos y la generación de información en línea y asequible.

Con respecto a la modernización del trabajo administrativo, es común ver a muchos funcionarios locales que toman como ejemplo narrativo a Estados tecnológicamente muy avanzados. Sin embargo, se trata de una referencia que queda en la idealización y que después no se ve que inspiren en lo concreto planes de acción de transformación de mediano y largo plazo.

Asimismo, resulta clave promover nuevos modelos de comportamientos que contribuyan a superar la recurrente tendencia a trabajar «como se hace siempre» en la administración. Para lograrlo, resultará fundamental descubrir técnicas de implementación que contribuyan a arraigar el contenido de esta nueva cultura organizacional.

La uniformidad relativa de las opiniones contrarias a la digitalización nos muestra que ha existido una eficaz tarea de educación negativa, por lo que no es poco el imponer un lenguaje común de tramitación electrónica y reforma administrativa.

Pero no debemos ignorar que los comportamientos, las actitudes y las categorías de pensamiento son más difíciles de modificar. A pesar de la fuerza de convicción que puedan tener las autoridades reconocidas y altos mandos, no se deben minimizar los obstáculos que entraña la transformación digital. Estos deben ser enfrentados con paciencia y perseverancia. ¿Cuántos abogados, por ejemplo, aún se resisten a la utilización de la firma digital? La reforma administrativa es una revolución paradigmática en cualquier gobierno, y como tal, será siempre pasionalmente resistida.

Para avanzar con la resiliencia necesaria, ningún funcionario a cargo de la transformación digital debe olvidar que el fin último es el servicio público y la completa dedicación al interés general. Aunque cualquier reforma administrativa constituye una conquista que estará siempre amenazada de regresión, el cambio es posible y conlleva siempre algo de irreversibilidad.

Referencias bibliográficas

Bracken, M. & Greenway A. (2018). *How to Achieve and Sustain Government Digital Transformation*. Washington, USA: IDB.

Clusellas, P., Martelli, E. y Martelo, M. J. (2014). *Gestión Documental Electrónica. Una transformación de raíz hacia el Gobierno Electrónico en la Ciudad de Buenos Aires 2009-2014*. Buenos Aires: GCABA.

Clusellas, P., Martelli, E. y Martelo, M. J. (Nov 2016). *Ending the Tyranny of Paper in Argentina*. IEEE – ITProfessional, NJ, USA.

Clusellas, P., Martelli, E. y Martelo, M. J. (2019). *Un Gobierno Inteligente, El cambio de la Administración de la Nación Argentina 2016-2019.* Buenos Aires: NA.

Delgado, A. (2016). *Digitalizate*. Barcelona: Libros de Cabecera S L.

Harari, Y. N. (2014). *Sapiens. De animales a dioses.* Barcelona: Penguin Random House.

Harari, Y. N. (2016). *Homo Deus. Breve historia del mañana.* Barcelona: Penguin Random House.

Maney, K., Hamm, S. y O'Brien, J.M. (2011). *Trabajando por un mundo mejor*. New Jersey: IBM Press –Pearson plc.

Moriconi Bezerra, M. (2011). *Reforma, política y administración pública. Por qué fracasan las reformas administrativas*. México: Universidad Metropolitana de México.

Ramió, C. (2017). *La administración pública del futuro (Horizonte 2050). Instituciones, política, mercado y sociedad de la innovación*. Madrid: Tecnos Madrid.

Ramió, C. (2019). *Inteligencia artificial y administración pública. Robots y humanos compartiendo el servicio público*. Madrid: Los Libros de la Catarata.

Roseth, B., Reyes, A. y Santiso, C. (2018). *El fin del trámite eterno*. Washington: IDB.

EDUARDO MARTELLI. Licenciado en Administración de la Universidad de Buenos Aires. Ha ejercido su actividad profesional en forma independiente, en empresas privadas y en la gestión pública. Fue Director Ejecutivo de varias compañías de Seguros, Subsecretario de Modernización del Gobierno de la Ciudad Autónoma de Buenos Aires, Secretario de Modernización Administrativa en el Gobierno Nacional y Director del Correo Argentino.

Actualmente es consultor de la Auditoría General de la Ciudad Autónoma de Buenos Aires, la CAF, Acys Argentina y otras instituciones.

Líder en el desarrollo e implementación de los proyectos Gestión Electrónica, Compras, Obras Públicas, Reforma Administrativa del Gobierno Nacional, a cargo de Firma Digital y la Oficina Nacional de Contrataciones.

Asimismo, tiene una extensa participación como expositor sobre estos temas, tanto en Argentina como en otros países. Publicó dos libros y diversos artículos sobre digitalización y reforma del Estado.

CAPÍTULO 8

Datos masivos para la toma de decisiones públicas: aportes para un debate imprescindible

Diego Pando
Eduardo Poggi

Introducción

Dado el veloz e intenso desarrollo de las tecnologías de información de los últimos años, los datos han pasado de ser escasos a ser masivos a partir del volumen de producción, la velocidad en que son transmitidos, la variedad de fuentes (los propios sistemas de los organismos públicos, otras fuentes públicas y fuentes no tradicionales como redes sociales, satélites, cámaras, sensores, etc.) y la variedad de tipos (números, textos, imágenes, audios, videos).

En este sentido, el objetivo del presente trabajo consiste en plantear la importancia de la generación, extracción y uso de datos para mejorar el proceso de toma de decisiones públicas, explicitar sus principales desafíos e identificar algunas de las (todavía escasas y aisladas) experiencias desarrolladas por organismos públicos de América Latina.

1. Los datos como materia prima

Existen cada vez más evidencias en relación con los crecientes retos que enfrentan los Estados para estar en sintonía con las profundas transformaciones políticas, económicas y sociales en las que nos encontramos en esta década de 2020 que comienza. Estas transformaciones conllevan problemas multidimensionales y de baja estructuración, cada vez menos susceptibles de tratamientos segmentados o sectoriales.

En este escenario, el cambio tecnológico es particularmente relevante, por su velocidad e intensidad. El uso intensivo de las tecnologías digitales no solo ha llegado a la esfera personal, alterando comportamientos, formas de vivir y de relacionarse, sino también y fundamentalmente, a las organizaciones y las industrias en general. Este cambio tecnológico ha modificado, y seguramente modificará mucho más, la gestión pública, ya que produce importantes efectos en los procesos de intermediación que no aportan valor y cuestiona (y rompe) esquemas más o menos asentados de diseños y arquitecturas organizacionales estatales.

Las diversas herramientas tecnológicas de la denominada cuarta revolución industrial (robotización, inteligencia artificial, *blockchain*, internet de las cosas, entre otras) tienen como novedad más importante la generación, extracción y uso de un tipo particular de materia prima: los datos. En la última década, el fenómeno del volumen, la velocidad y la variedad de datos, conocido genéricamente como *big data*, constituye un insumo central e inédito para el desarrollo de las diversas tecnologías de la denominada cuarta revolución industrial, a partir de las cuales el aparato estatal puede, de manera decisiva, mejorar su eficacia y eficiencia y, de esta manera, estar en sintonía con las profundas transformaciones políticas, económicas y sociales características de nuestras sociedades.

Desde ya, el desarrollo de las tecnologías de la cuarta revolución industrial está dado principalmente por la interrelación entre ellas y por la combinación de una serie de factores que exceden lo tecnológico (culturales, organizacionales, legales, éticos, entre otros). Estos procesos de desarrollo y profunda transformación no son nuevos, la humanidad ha pasado y asimilado varios. Sin embargo, lo que ha variado en los últimos años es la velocidad con la cual se producen, dando menos tiempo a los distintos actores a acomodarse.

En particular, hoy el mundo genera tantos datos que su procesamiento está fuera del alcance humano, por lo cual muchas veces no queda más remedio que delegar su gestión en algoritmos. Es más, el control de lo que hacen o dejan de hacer dichos algoritmos también escapa a las capacidades humanas, con lo cual se «delegan» en metaalgoritmos que evalúan los demás algoritmos. Como si esto fuera poco, la forma en que estos algoritmos son desarrollados tiene características disruptivas con las prácticas establecidas de trabajo, lo que implica enormes desafíos (Harari, 2018).

2. Hacia el paradigma *data-driven*

La inteligencia artificial (IA) es el área de la ciencia de la computación que pretende crear máquinas inteligentes que funcionen y reaccionen como humanos. La caracterización de un sistema como de IA debe basarse en la existencia y utilización conjunta de cinco capacidades: descubrir, predecir, justificar, actuar y aprender. De todas las tecnologías que conforman la cuarta revolución industrial, los denominados algoritmos de la IA son los que suelen llamar más la atención, en particular por sus roles de «directores de orquesta».

La IA tiene tantos años como la informática clásica. Intentar que objetos tengan un comportamiento que podríamos calificar como

inteligente es contemporáneo al interés para realizar muchos cálculos aritméticos en poco tiempo. Desde su inicio como disciplina, la informática clásica ha utilizado el paradigma conocido como *model-driven*, o guiado por modelos, en el cual un grupo de humanos ante un problema elabora un método de solución sistemático, que describe con el más mínimo detalle y graba en una computadora para que lo memorice y lo vuelva a repetir al pie de la letra cada vez que se le pida. La materia prima necesaria para elaborar estos algoritmos (usualmente denominados «programas») es 100% humana. Esta es la forma predominante en que se han desarrollado sistemas de información desde los inicios de la computación. De esta forma están elaborados, por ejemplo, los programas que generan balances a partir de asientos contables, que emiten recibos de sueldos o gestionan nuestros correos electrónicos o cuentas bancarias.

Pero el *model-driven* no es el único paradigma para determinar el comportamiento de las computadoras. En los últimos años, y fundamentalmente a partir del gran caudal de datos, tomó fuerza el paradigma *data-driven* o guiado por datos, en el cual se utilizan algoritmos genéricos que toman grandes cantidades de datos y los exploran para descubrir regularidades, patrones, reglas predictivas y similitudes que permitan de alguna manera encontrar y/o explicitar «conocimiento» oculto en los datos.

En este paradigma *data-driven*, la materia prima para la elaboración de algoritmos (en este caso denominados «modelos») son los datos. Este fenómeno del *big data* mencionado en el apartado anterior, sumado a los avances de la informática así a como las nuevas investigaciones (principalmente en las áreas de lingüística, psicología, biología y sociología), está en la base de los actuales modelos que, por ejemplo, traducen textos de un idioma a otro, predicen el clima, evalúan el otorgamiento de créditos bancarios, detectan correos indeseados,

predicen la intención de voto, descubren mutaciones en virus, entre otras infinidades de aplicaciones de uso cotidiano.

La aproximación *data-driven* es la base del aprendizaje automático, área de la IA (una especie de hija predilecta) que se hizo más famosa cuando salió del ámbito académico y llegó al mundo de la gestión con la denominación minería de datos de la mano de otras disciplinas como la estadística, la econometría, la matemática aplicada, la gestión de datos, la visualización, la teoría de juegos, la genética, etc. Con los años y las modas, todo esto fue sintetizado bajo el nombre de **analítica de datos**, concepto que utilizaremos en este trabajo (aunque también se lo puede encontrar en la literatura como ciencia de datos (Donoho, 2017)).

Los protocolos, metodologías y prácticas profesionales de la informática clásica y de la analítica de datos son diferentes. Si bien tienen, obviamente, puntos en común (ambas usan datos y usan computadoras para su trabajo, por ejemplo), la lógica es diferente: la primera desarrolla programas que manipulan datos, mientras que la segunda manipula los datos para inferir modelos.

En la informática clásica, el objetivo primario de los programas es almacenar representaciones digitales de eventos: tal día, a tal hora, tal persona pagó $X en concepto de cancelación de tal factura de tal servicio. Dichos datos son utilizados posteriormente por la organización dueña del sistema (o, por lo menos, de los datos) para obtener información que minimice su incertidumbre a la hora de detectar morosos, generar su balance contable, pagar impuestos, etc. En este uso tradicional, los datos de la organización son utilizados para generar información para la toma de decisiones.

Sin embargo, y de acuerdo con lo dicho, el mundo de los datos cambió radicalmente. Ahora, a los datos generados por los sistemas de información organizacionales se deben sumar los datos registrados por millones de personas, sensores, cámaras, teléfonos inteligentes,

cajeros automáticos y cualquier otro dispositivo interconectado, a través de los cuales se dejan huellas digitales que quedan a disposición de las organizaciones, con la posibilidad de ser transformadas en información.

A diferencia de una encuesta sistemática, los datos de *big data* son anárquicos y espontáneos (Sosa Escudero, 2019). Es decir, los datos no fueron generados por el propósito de crearlos, como en las respuestas a una encuesta tradicional, sino como resultado de otra acción (compartir un mensaje en redes sociales, pagar con una tarjeta de crédito, entrar a un sitio web, etc.). Tradicionalmente, los datos digitales se conciben como una planilla electrónica con columnas homogéneas que en las filas contienen caracteres, fechas, cantidades, importes, códigos, etc. Hoy los datos digitales toman a la vista formas diferentes: las cámaras dejan imágenes o videos; los diferentes sensores dejan innumerables formas de representar lo que miden; las personas dejamos textos, hipertextos con abreviaturas, emoticones, palabras mal escritas e infinidad de formas de expresión visual que no aparecen en los diccionarios. Internamente, todos estos formatos digitales terminan siendo números que una computadora interpretará como pueda o como la semántica que le demos la guíe.

Hoy los datos tienen un valor potencial, aunque la forma en que van a ser utilizados no esté clara. Tradicionalmente, un dato se solicitaba y se almacenaba con un fin bien determinado, incluso se calculaba el beneficio que produciría descontándole los costos de obtenerlo y guardarlo. En analítica de datos, los resultados más interesantes se dan por la combinación de datos de orígenes diversos que ningún grupo de desarrolladores definió jamás. Las combinaciones más extrañas de datos han dado resultados sorprendentes. La mezcla de las más diversas fuentes es lo que permite a los modelos descubrir conocimiento escondido en los mares (o ríos caudalosos) de datos.

3. Principales características de las prácticas de analítica de datos

Las prácticas y productos de la analítica de datos (AD) tienen características propias que las distinguen de la informática clásica y de otras disciplinas predictivas, como la estadística. En este apartado describimos las características que consideramos más importantes para el tema que nos ocupa.

La primera de estas características podríamos denominarla **caja negra**. En los inicios de la AD, los algoritmos descubrían reglas interpretables por las personas. Utilizaban miles de datos como materia prima y relacionaban atributos que permitían predecir con buena precisión si, por ejemplo, de acuerdo con los antecedentes financieros de una persona, correspondía el otorgamiento de un crédito. En general, los modelos generados por los algoritmos eran entendibles por humanos y tenían capacidad de explicación de por qué habían tomado una decisión y no otra.

Actualmente los algoritmos de la AD producen modelos incomprensibles. Los datos que dan forma a estos algoritmos son miles de millones y los atributos se cuentan de a miles. Y los modelos que se descubren a partir de estos datos son tan complejos que muchas veces escapan a toda capacidad humana de interpretación y los algoritmos tampoco son capaces de explicar por qué tomaron una decisión o de explicitar el conocimiento descubierto.

La capacidad de explicación de las decisiones tomadas sobre la base de las técnicas de AD no es una premisa de diseño. Los modelos que producen son cada vez más opacos y complejos. Los originales árboles de decisión se han convertido hoy en enormes «bosques aleatorios» o complejos cálculos bayesianos o redes de redes (neuronales) conocidas como *deep learning*. El riesgo es claro: si delegamos

decisiones importantes en algoritmos de esta naturaleza, perdemos capacidad para explicar la racionalidad que las sustentan.

La segunda característica de la AD es el **autoaprendizaje**. La definición clásica del aprendizaje automático (base de la AD, como mencionáramos en el apartado anterior) dice que el modelo aprende si, a fuerza de repetir una tarea, la realiza cada vez mejor a partir de analizar la evidencia (su experiencia). Esta definición requiere de un modelo, de una tarea, de la evidencia que va dejando su propio accionar y de una medida de performance que le permita medir qué tan bien está haciendo su tarea. Los modelos pueden estar sujetos a cambios continuos, leves o profundos, dependiendo de cómo cambien los datos, o lo que estos representan. Si la evidencia cambia, los sistemas detectarán que los modelos deben adecuarse a las nuevas circunstancias.

Por lo tanto, el comportamiento de los modelos generados inductivamente no es permanente, dado que por su propia naturaleza se adecuan a las nuevas situaciones. La diferencia principal de los algoritmos de AA respecto a los algoritmos de la informática clásica es que su comportamiento no solo depende, sino que puede modificarse a partir de los datos que recibe.

La AD va cambiando continuamente y va automatizando sus propios procesos, lo cual genera una **creciente distancia de las decisiones algorítmicas** (tercera característica). Esto no es ajeno a los cambios que se van produciendo en la industria. Hace unos pocos años, los mineros de datos aplicaban metodologías de desarrollo en las que preparaban los datos, generaban modelos, los testeaban, realizaban cambios y volvían a empezar hasta encontrar un óptimo. Este proceso iba dejando evidencia digital que puede usarse para alimentar modelos que observan la generación de modelos. Por lo tanto, la práctica de la AD va cambiando rápidamente y se van automatizando los propios procesos de elaboración de modelos.

Buena parte de la producción de modelos de AD se va alejando cada vez más de la manipulación humana y van dejando que otros modelos denominados metaalgoritmos vayan tomando el mando. Por lo tanto, los controles, las intervenciones, los ajustes, etc., quedan fuera del alcance de las capacidades humanas y son delegados en otros modelos que toman las decisiones.

La cuarta característica son los **sesgos**. Como hemos dicho, la materia prima de los algoritmos son los datos. Los datos son representaciones de hechos pasados generados de determinada forma. Muchos de estos datos fueron representaciones de acciones humanas, con toda su impronta de creencias, costumbres, valores, conocimiento y estados de ánimo. Decisiones tomadas en el pasado por humanos en un contexto definido fueron abstraídas en pocos datos que representan el hecho. Luego esos datos son tomados por algoritmos que los usan para definir su comportamiento, a imagen y semejanza de sus predecesores.

Precisamente esta es la idea base: los algoritmos aprenden del pasado para hacer mejores tareas que hoy realizan las personas, con lo positivo y lo negativo que ello puede implicar. Por ejemplo, si en el análisis de candidatos para ocupar una posición hay en la evidencia una predisposición a elegir hombres antes que mujeres, esto quedará plasmado en el algoritmo.

Si al caudal de datos aportados por el *big data*, cuya veracidad debe ser puesta a prueba, le sumamos las características explicitadas en este apartado, obtenemos una combinación de riesgo potencial alto y disruptivo para las prácticas burocráticas típicas de los aparatos estatales. El ámbito privado, en particular la industria, tiene menos restricciones y riesgos que el sector público, al mismo tiempo que ha ido generando con los años prácticas, protocolos y estructuras organizacionales para mantener las características de la AD bajo control. Es decir, una empresa puede utilizar los modelos basados en datos con las

características descritas para, por ejemplo, verificar que un producto cumple con la calidad adecuada o no, un cliente es rentable o no, cuál empleado debe recibir un bono y cuál no, con restricciones y riesgos mucho más acotados en comparación con un organismo público, que tiene lógicas y requisitos mucho más exigentes al momento de decidir, por ejemplo, si un beneficio es denegado a un ciudadano o si un trabajador es ascendido. Como es de imaginar, los riesgos relacionados con los problemas de transparencia, la falta de procesos explícitamente definidos y los sesgos negativos son altísimos en el ámbito público en comparación con el privado.

4. El impacto de los datos en las estructuras organizacionales

En los últimos años, las organizaciones con mayor uso intensivo de tecnologías de la información (TI) fueron reconfigurando roles a partir de la revolución en el mundo de los datos. Así, la TI se ha insertado de tal forma en el quehacer organizacional que la provisión de servicios de base tecnológica ha ido mutando para mantenerse acorde a la demanda.

En este contexto, el rol del CIO (*chief information officer* o responsable de tecnología) se ha orientado cada vez a la compleja gestión de infraestructura y provisión de servicios de TI (sistemas de información incluidos). Por otro lado, se creó el rol de CDO (*chief data officer* o responsable de datos) a partir de la consideración de que los datos son un activo tan importante en las organizaciones que su gobierno y su tratamiento requieren de una estructura específica que, junto al CIO, reporta a la máxima autoridad de la institución. Asimismo, se creó el rol de CISO (*chief information security officer* o jefe de seguridad), por considerar que la protección de los datos deja de ser un problema de

las áreas de TI para tener incumbencia institucional. El CISO suele articularse también con el CIO y el CDO (Deloitte, 2016).

Finalmente apareció el rol de CDxO (*chief digital transformation officer* o jefe de transformación digital), al considerarse que la apropiación de nuevas tecnologías es la que guía y transforma la gestión de, incluso, las funciones esenciales de cualquier organización. Este rol es el responsable de imaginar el futuro de la organización a partir de la apropiación de tecnologías, las cuales pueden ser nuevos sistemas de información (potestad del CIO), nuevos servicios basados en datos o la incorporación de *gadgets* que provee la industria de TI (Alexa de Amazon, Watson de IBM, el Sistema Quirúrgico Da Vinci, por nombrar solo algunos ejemplos) y pueden alimentarse con la evidencia institucional para determinar su comportamiento (potestad del CDO).

En particular el CDO pasa a comandar las prácticas propias de la AD, cuya misión es llevar y mantener la institución en un paradigma *data-driven*. Grandes y medianas empresas privadas, e incluso organismos públicos, han apropiado las prácticas de AD y las utilizan para sustentar sus decisiones basadas en evidencia, aprovechando la masiva cantidad de datos digitales que poseen en sus reservorios organizacionales.

Una tarea relevante del CDO es la denominada gobernanza de datos. Las enormes cantidades de datos deben ser organizadas, limpiadas, ordenadas, clasificadas y validadas. Como toda materia prima, los datos deben pasar por un riguroso control de calidad, dado que el uso de los datos directos de la fuente suele tener resultados malos.

La AD, responsabilidad de CDO, tiene una fuerte relación con las áreas bajo los CIO y los CISO. La infraestructura, la capacidad de almacenamiento y procesamiento y los datos organizacionales utilizados por AD son potestad del CIO. Todo el contexto de los datos, sobre todo cuando se trata de datos sensibles o bajo la protección de leyes

específicas, deben estar bajo la mirada del CISO. Y, como hemos visto, muchas de las innovaciones que puede proponer un CDxO también estarán moldeadas por los datos institucionales administrados por el CDO.

5. Experiencias

Siguiendo a Aguerre (2020), la IA es un tema que ha aumentado considerablemente la atención de los responsables políticos durante los últimos años, incluso en América Latina, una región que hasta el momento no es considerada productora ni exportadora mundial de IA. Sin embargo, la región aún muestra un bajo nivel de adopción de políticas, marcos o estrategias explícitas en comparación con América del Norte, Europa y Asia (Aaronson, 2019). En este sentido, la fuerte asimetría entre países desarrollados y en desarrollo en materia de gobernanza de datos representa un desafío importante, en tanto que los países en desarrollo son generadores de datos pero no productores de soluciones (Ciuriak, 2018).

Cabe señalar que Argentina, Chile, Colombia, México y Uruguay son los únicos de la región que hasta el momento han desarrollado planes estratégicos de IA, los cuales se encuentran en diferentes etapas de madurez, tanto en su validación como en las discusiones y en su implementación (Aguerre, 2020).

A pesar de que normalmente cuentan con volúmenes de datos superiores a los del sector privado, las organizaciones públicas no acompañaron en la misma medida la evolución de las técnicas relacionadas con la AD. En este sentido, y yendo más allá de las conocidas formas de recolectar, publicar y utilizar datos por parte de los gobiernos, las cuales sirvieron para generar aplicaciones para enfrentar la pandemia del COVID-19, las experiencias documentadas sobre AD en el sector

público latinoamericano son pocas, aisladas y producto más bien de iniciativas individuales de determinados organismos.

5.a. Transformación organizacional

La Administración Federal de Ingresos Públicos de la Argentina (AFIP) es un caso interesante de transformación organizacional para la apropiación de las prácticas de AD. Esta organización fue adoptando en los últimos años estructuras y roles en sintonía con los nuevos desafíos. Así, el área responsable de la seguridad informática se escindió del área gestionada por el CIO y pasó a depender de la máxima autoridad del organismo. De forma análoga, el área responsable de inteligencia de negocios siguió el mismo camino, al crearse la Dirección de AD. Durante 2019 hubo un intenso trabajo para conformar el área con profesionales de diversas formaciones y cubrir roles orientados a la gobernanza de datos, generación de modelos y producción de reportes inteligentes. Diversos proyectos de fiscalización inteligente basada en la evidencia digital fueron desarrollados en esta Dirección de AD (Poggi, 2020).

La AFIP no es el único organismo que ha seguido este camino. La relevancia del rol de los *chief data officers* en las entidades públicas se manifiesta en varios países que están en una permanente búsqueda para encontrar y capacitar a los expertos en datos. A modo de ejemplo, se estima que en los próximos dos años, de acuerdo con el Departamento Nacional de Planeación del Gobierno de Colombia, el 90% de sus organismos tendrán al menos un proyecto de aprovechamiento de datos (Barros, 2020).

5.b. Apropiación de gadgets inteligentes

La interacción entre personas y robots nunca ha sido tan frecuente como en el presente. En efecto, las personas se han ido acostumbrando

a que determinadas «máquinas inteligentes» las atiendan y resuelvan sus asuntos en diversas tareas de la vida cotidiana, desde trámites financieros y transacciones comerciales hasta servicios ligados a la atención médica. En particular los asistentes conversacionales virtuales (ACV) juegan un papel de suma importancia en los esfuerzos del fisco por aumentar el cumplimiento voluntario e incrementar la recaudación de impuestos (De Oliveira y Muñoz, 2020).

Este es un caso típico de adopción de *gadgets*, concepto que designa la combinación de *hardware* y *software* producido por un fabricante externo que puede ser entrenado para cumplir funciones propias de un organismo.

La digitalización de la atención al contribuyente permite superar problemas que presenta el modelo tradicional, tales como la baja cobertura (número de contribuyentes que pueden ser atendidos); los largos tiempos de espera (presenciales o por teléfono); los altos costos del personal asignado, incluida su capacitación permanente; y la limitada efectividad de las respuestas a las consultas, lo que genera frustración en la mayoría de los contribuyentes (De Oliveira y Muñoz, 2020).

Los ACV constituyen la puerta de ingreso al mundo de la IA, fortaleciendo conceptos y creando una red interna de conocimiento y soporte para estas nuevas tecnologías. Los ACV también pueden ser utilizados internamente para responder a las consultas de los empleados en el área de gestión de las personas y brindar asistencia a los usuarios internos y externos de otros sistemas.

El uso de ACV es una novedad en la región. En el estado de Piauí (Brasil), por ejemplo, la asistencia virtual del ACV Teresa está disponible las 24 horas del día y los siete días de la semana en el ámbito tributario.

A grandes rasgos, se puede decir que los beneficios de los ACV son los siguientes:

- Ofrecer servicios a los ciudadanos sin interrupciones.
- Brindar informaciones consistentes, lo que evita el riesgo de interpretaciones distintas o incompletas.
- Aumentar la productividad de la atención a los usuarios, ya que es posible atender más casos en el mismo tiempo. Esa mayor productividad permite, al mismo tiempo, liberar una parte del personal para que realice otras tareas.
- Eliminar los tiempos de espera (presenciales y telefónicos) por indisponibilidad de operadores.
- Proporcionar respuestas cada vez más precisas y, en consecuencia, mejoras crecientes en la satisfacción de los usuarios, puesto que los ACV basados en la IA recopilan datos y aprenden con las interacciones realizadas.

Sin embargo, deben considerarse también los desafíos potenciales del uso de los ACV. Así, los problemas más usuales hacen referencia a la dificultad de improvisar, el suministro de respuestas erradas cuando el ACV termina perdido en la conversación (*lost in translation*), la dificultad para retener al usuario y limitaciones para procesar el sarcasmo y otros rasgos propios de la comunicación humana. Pese a ello, con la debida experimentación y planificación, la IA ofrece oportunidades para mejorar los servicios y la atención a la ciudadanía.

Otras aplicaciones similares surgieron empujadas por la pandemia del COVID-19 en marzo de 2020. Por ejemplo, el Gobierno de la Ciudad de Buenos Aires implementó un *bot* de Whatsapp que responde preguntas sobre prevención, síntomas e información general de los servicios de la ciudad sobre COVID-19. A nivel nacional, en Argentina se implementó sobre Whatsapp y Facebook Chatbot una línea de ayuda automatizada con el objetivo de proporcionar respuestas a las preguntas más frecuentes, evitar la información errónea y proporcionar consejos para prevenir la propagación de COVID-19.

Otro caso de utilización de *gadgets* es la utilización de PredPol por el Ministerio del Interior de Uruguay. En un contexto de lucha contra la inseguridad y de incorporación de tecnología a la policía local, el Ministerio del Interior de Uruguay obtuvo la licencia del *software* PredPol, desarrollado por la empresa del mismo nombre, que tuvo origen en un proyecto de investigación conjunto entre el Departamento de Policía de Los Ángeles y la Universidad de California. A partir de los datos brindados, PredPol elabora mapas prospectivos que predicen mediante un algoritmo dónde ocurrirán las incidencias delictivas de las próximas 24 horas. A través de esta información se despliegan los recursos de patrullaje para cubrir las áreas de concentración delictiva. La base a partir de la cual PredPol realiza sus predicciones es el registro de los datos de criminalidad del Ministerio del Interior. PredPol cuenta con acceso a las coordenadas y la hora de los eventos delictivos pasados, pero no a los datos de víctimas y autores de delitos, ni tácticas y estrategias policiales. Este tipo de programas generan un «circuito de retroalimentación», que lleva a que los agentes sean enviados repetidamente a las mismas zonas de la ciudad, generalmente las que concentran mayor cantidad de minorías raciales, independientemente de la verdadera tasa de criminalidad en esa área. Estos programas detectan patrones en los datos de los que se alimentan, para luego repetirlos en futuras predicciones. Por lo tanto, y esto vale para todos los sistemas que dependen de algoritmos, la información que devuelva será sólo tan buena como los datos ingresados. Un algoritmo es una máquina de encontrar patrones y repetirlos. Aplicada sin cuidado, su lógica es la del círculo vicioso, con el consecuente riesgo, en este caso, de convertirse en un legitimador del viejo olfato policial (Scrollini, 2018).

5.c. Desarrollo de modelos predictivos

La provincia de Salta (Argentina), en alianza con la empresa Microsoft, desarrolló dos herramientas con el objetivo de realizar la

predicción de deserción escolar y embarazo adolescente no deseado. Ambos casos fueron construidos sobre la base de conjuntos de datos brindados por el Ministerio de Primera Infancia de la provincia. Este algoritmo permitió identificar a 397 niños en peligro de abandonar la escuela y 500 mujeres que podrían estar en riesgo de un embarazo no deseado. El caso generó polémica en Argentina debido a: 1) los datos de entrenamiento de los algoritmos fueron utilizados como datos de evaluación, lo que llevó a resultados sobredimensionados; 2) los datos utilizados no comprendían una distribución de todos los posibles casos, sino que se enfocaban en un determinado grupo social desfavorecido; 3) la pregunta original planteada no podía ser respondida a través de los algoritmos seleccionados. El caso refleja la ausencia de un marco de experimentación para llevar adelante la política, así como la importancia de la transparencia del código para poder generar una discusión pública (Scrollini, 2018).

Reflexiones finales

Con menos restricciones y riesgos que el sector público, el sector privado en general va incorporando robots, utilizando algoritmos opacos que automodifican su comportamiento y delegando en opacos artefactos decisiones que tradicionalmente recaían en personas.

Por su parte, tal como hemos presentado en este trabajo, las experiencias en el sector público latinoamericano son escasas, limitadas y aisladas. La mayoría de las organizaciones públicas muestra debilidades estructurales y retrasos en adoptar incluso cambios básicos. Como hemos visto, los datos son cada vez más un insumo fundamental, aunque el sector público, siendo dueño y administrador de los reservorios más grandes de datos, todavía no afronta su gestión con prácticas organizacionales adecuadas.

Si bien es cierto que la gestión pública no debe ir detrás de modas y debe darse tiempo para pensar las respuestas adecuadas a los cambios que se generan en la sociedad, estos tiempos son cada vez más cortos y los riesgos que se presentan son cada vez más altos.

Además de los desafíos que implica la apropiación de las nuevas tecnologías en la gestión, el sector público debe regular la utilización de los algoritmos por parte del sector privado, fundamentalmente en lo que respecta a dos dimensiones que tienen un sustrato de carácter ético (Barros, 2020): 1) privacidad, es decir, conciliar la precisión de los modelos con un adecuado uso de datos, en especial cuando se trata de datos sensibles de las personas; y 2) justicia, es decir, asegurar que los algoritmos se comporten de forma «justa», sin introducir sesgos negativos, o al menos teniendo en cuenta la existencia de estos sesgos e intentando minimizarlos.

Finalmente, pero no por ello menos importante, el sector debe posicionarse como un actor fundamental en el desarrollo de la infraestructura de base. Así como tuvieron un lugar predominante los ferrocarriles y las autopistas, cuestiones tales como las redes de comunicación segura, la identificación digital, los contratos digitales, los robots colaborativos y, en general, los dispositivos inteligentes, deberían ocupar un lugar relevante en la agenda pública, dadas las potencialidades y los desafíos existentes.

Referencias bibliográficas

Aaronson, Susan (2019). Data is a development issue, CIGI Paper Nº 223. Disponible en https://www.cigionline.org/publications/data-development-issue.

Aguerre, Carolina (2020). «Estrategias nacionales de IA y gobernanza de datos en la región», en C. Aguerre, (Ed.). *Inteligencia Artificial en América Latina y el Caribe. Ética, gobernanza y políticas*. Buenos Aires: CETyS, Universidad de San Andrés.

Barros, Alejandro (2020). Inteligencia Artificial, cuidado con los sesgos. Disponible en https://www.alejandrobarros.com/inteligencia-artificial-cuidado-con-los-sesgos/.

Ciuriak, Dan (2018). Frameworks for Data Governance and the Implications for Sustainable Development in the Global South, 2018. Disponible en SSRN: https://ssrn.com/abstract=3266113.

De Oliveira Junior, Emilio y Muñoz, Andrés (2020). La atención virtual al contribuyente permite la continuidad del negocio tributario y es estratégica en tiempos del coronavirus. Disponible en https://blogs.iadb.org/gestion-fiscal/es/asistentes-virtuales-tributarios-continuidad-de-negocios-durante-coronavirus/.

Deloitte (2016). «The evolving role of the chief data officer in financial services: From marshal and steward to business strategist». Disponible en https://www2.deloitte.com/ba/en/pages/financial-services/articles/the-evolving-role-chief-data-officer-financial-services.html.

Donoho, David (2017). «50 Years of Data Science», *Journal of Computational and Graphical Statistics*, 26:4, 745-766, DOI: 10.1080/10618600.2017.1384734.

Harari, Yuval Noah (2017). *Homo Deus. Breve historia del mañana*. Buenos Aires: Editorial Debate.

Harari, Yuval Noah (2018). *21 lecciones para el siglo XXI*. Buenos Aires: Editorial Debate.

Poggi, Eduardo (2020). «En ciencia de datos hay una conversación constante con la información», entrevista realizada para *Neurona BA*, Buenos Aires, marzo. Disponible en http://neurona-ba.com/en-ciencia-de-datos-hay-una-conversacion-constante-con-la-informacion/.

Scrollini, Fabrizio (2018). Automatizar con cautela. Datos e Inteligencia Artificial en América Latina, ILDA. Disponible en https://idatosabiertos.org/publicaciones/automatizar-con-cautela-datos-e-inteligencia-artificial-en-america-latina/.

Sosa Escudero, Walter (2019). *Big Data*. Buenos Aires: Siglo XXI Editores.

DIEGO PANDO. Politólogo, Máster en Administración y Políticas Públicas por la Universidad de San Andrés (Argentina) y Doctor en Ciencia Política y de la Administración por la Universidad Complutense de Madrid (España). Presidente de la Asociación Argentina de Estudios de Administración Pública (AAEAP). Decano de la Facultad de Políticas Públicas y Gestión Ambiental de la Universidad Metropolitana para la Educación y el Trabajo (UMET). Profesor de grado en la Universidad de San Andrés, en donde dirigió el Programa de Gobierno Electrónico y codirigió el Programa de Formación en Competencias para la Alta Dirección Pública. Profesor de posgrado en diferentes universidades. Publicó cuatro libros, varios capítulos en libros y diversos artículos en revistas especializadas en administración y políticas públicas. Además, se desempeñó como consultor en organismos internacionales (BID, UNESCO, CAF, CLAD, entre otros), en cuestiones relacionadas con la utilización de tecnologías de información para fortalecer capacidades de gestión pública.

EDUARDO POGGI. Cuenta con 40 años de experiencia profesional en proyectos de tecnología de la información, fundamentalmente orientada al sector público latinoamericano. En la última década se orientó a la gestión de datos públicos: datos abiertos, interoperabilidad y ciencia de datos. Acredita unos 25 años de docencia de grado y posgrado en aprendizaje automático, minería de datos y gestión de TI pública en general. Licenciado en Ciencias de la Computación por la UBA (FCEN), Magíster en Administración y Políticas Públicas y especialización en Negocios y Tecnología por la Universidad de San Andrés. Actualmente se desempeña como asesor en la Dirección de Analítica de Datos de la AFIP de Argentina. Docente de posgrado y consultor internacional.

CAPÍTULO 9

La gestión de los recursos humanos ante la transformación digital. Experiencia en la administración pública nacional de la Argentina

Pablo Legorburu

Introducción

Para que una transformación digital resulte exitosa, es decir, que se haya implantado en el modo de operar y de pensar en una organización, no es suficiente la sola incorporación de recursos tecnológicos. El aspecto más relevante y permanente de toda transformación tiene que ver con la modificación de conductas individuales y organizacionales, lo cual implica, en un nivel más profundo, el cambio de patrones culturales. Este último aspecto compromete a las personas individual o grupalmente en la dimensión de sus valores, sus hábitos y su particular idiosincrasia.

Por eso se torna imprescindible dirigir la mirada sobre la gestión de los recursos humanos en el abordaje integral de la transformación digital en la administración pública.

Organizaciones internacionales como la OCDE destacan que una de las principales dimensiones de esta transformación cultural que

acompaña la progresiva instauración de un gobierno digital tiene que ver con la «orientación al usuario», esto es, que sus necesidades impulsen las decisiones para diseñar mejor los servicios públicos. En definitiva, no es otra cosa que el propósito y la orientación general de la acción pública hacia el cuidado de los bienes y la protección de los derechos de los ciudadanos.

Ahora bien, la idea de «orientación al usuario» no suele constituir el paradigma dominante de las administraciones públicas. En general y a lo largo de los años, su actividad se ha estructurado a partir de procesos y procedimientos complejos, centrados en la legalidad, que adquieren dicha complejidad precisamente por haber incorporado modificaciones sucesivas, que los han tornado altamente «burocráticos», en el sentido peyorativo del término.

Asimismo, la progresiva especialización de las políticas públicas y la descentralización de los organismos a su cargo han agregado nuevos procedimientos, comprometiendo a mayor cantidad de actores, que necesitan –o creen necesario– incorporar sus propias intervenciones e instrumentos normativos para gestionar sus servicios públicos. Cada paso del proceso y cada nueva norma involucran nuevos actores con nuevas visiones o interpretaciones. Visto desde el servidor público, el devenir de estos procesos tiene una historia cargada de significados. Disociado de ello, desde la perspectiva del ciudadano, la burocracia administrativa se asemeja al movimiento de un cuerpo pesado, lento, incomprensible y engorroso.

La historia viva encarnada en las administraciones públicas abarca y trasciende a los funcionarios de turno. Por eso, todo proceso de transformación cultural, como lo es una transformación digital, debe acoger la historia y asimilar su legado, pero no debe quedar cautivo en ella, sino trascenderla con la mirada en el futuro, promoviendo una evolución en la cultura.

En este contexto cultural de las administraciones públicas, la incorporación de tecnología, si bien *per se* produce un impacto en la cultura de la organización, no constituye un fin en sí mismo: se convierte en la oportunidad para, a la luz del nuevo paradigma de «orientación al usuario», cuestionar, replantear y recuperar el sentido de determinadas tareas y los procedimientos para llevarlas a cabo. También, para revisar las modalidades de registro de la información suministrada y sus niveles de integridad, seguridad, accesibilidad y transparencia, o la pertinencia de los ámbitos asociados a las tomas de decisiones. En suma, aspectos que, con ocasión de la incorporación de innovaciones tecnológicas, normalmente transversales, involucran un gran número de actores y obligan a un esfuerzo enorme para el manejo efectivo del cambio.

Semejante desafío compromete fuertemente a los responsables de la gestión de recursos humanos de los organismos públicos y a los funcionarios que deben diseñar sus políticas y proveer herramientas. Para que su tarea no se desarrolle de manera aislada, es preciso asegurar que su acción se vea acompañada por la de los restantes referentes de gestión de las políticas públicas.

No hay transformación digital posible sin una estrategia de gestión que involucre a las personas, sus motivaciones, su desarrollo, participación, evaluación e incentivo. Es necesaria, por lo tanto, una estrategia integral de la gestión de los recursos humanos de la administración pública.

Este capítulo no pretende aportar una orientación para el desarrollo específico de dicha estrategia, esfuerzo que excede los alcances de este texto y ameritaría un desarrollo más profundo y extenso. Con una aspiración más discreta y orientada, pretende pasar revista a algunos aspectos centrales que, en el marco de una transformación digital de la administración pública y sobre la base de la experiencia recogida por el autor, actúan como insumos o como componentes relevantes de dicha estrategia.

El trabajo, que tiene como alcance a la Administración Pública Nacional de la Argentina, con foco en sus áreas centrales, intentará poner en evidencia aquellos aspectos de la gestión de los recursos humanos que resultan más relevantes para acompañar un proceso exitoso de transformación digital, sus marcos de acción particulares, así como algunas variables explicativas de su éxito o fracaso identificadas en la experiencia de gestión del autor como secretario nacional de Empleo Público entre diciembre de 2015 y diciembre de 2019.

Para el desarrollo del capítulo se seguirán los siguientes lineamientos.

En un primer apartado se intentará generar conciencia sobre los desafíos que entraña la transformación digital, a partir de las condiciones contextuales: la dimensión y conformación de la administración pública, el marco jurídico laboral, y la idiosincrasia cultural que determinan el entorno en que se desarrolla la gestión de los recursos humanos. En ocasiones, tanto los funcionarios como los académicos desconocen el tamaño que caracteriza las administraciones públicas y las dificultades que esto supone para la gestión cotidiana. Evidentemente, no es lo mismo una dotación de 500 personas que un universo de varias decenas de miles de agentes. Tampoco lo es promover una transformación cultural en organizaciones relativamente homogéneas o heterogéneas, centralizadas o descentralizadas. Asimismo, se procurará describir de manera sencilla y general los rasgos principales del régimen laboral del servicio público civil, que posee diferencias importantes respecto del régimen de empleo en el sector privado. Se hará alusión a un aspecto determinante del empleo público, que se desarrolla de manera independiente por su naturaleza y significatividad: el régimen de estabilidad. Sobre la base de estas condiciones contextuales, ensayaremos algunas respuestas que faciliten la conducción de una transformación digital.

Seguidamente se describirán brevemente las bases y componentes de la Estrategia Integral de Gestión del Empleo Público, como marco de referencia de los programas, proyectos e iniciativas para el fortalecimiento y jerarquización del servicio público.

En el tercer apartado se intentará aportar lineamientos, orientaciones generales o específicas y recomendaciones sobre algunos aspectos relevantes de la gestión de los recursos humanos que, surgidos a partir de la reflexión y experiencia en la gestión, han demostrado ser de utilidad o aspirar a serlo, como respuesta a algunos de los desafíos planteados en el primer apartado.

Por último, se destacarán algunos hallazgos y conclusiones del informe «La transformación digital en el sector público», de la OCDE, con relación a la gobernanza del proceso y las habilidades a desarrollar en el servicio público.

1. Desafíos del contexto y respuestas posibles

1.a. Con relación a la dimensión, estructura y funcionamiento de la administración

En la República Argentina, el sector público nacional está constituido por la Administración Pública Nacional y otras entidades autárquicas y no gubernamentales del Poder Ejecutivo, las universidades nacionales, las empresas estatales y los poderes Legislativo y Judicial. Este conjunto conforma un universo de 739.149 puestos de trabajo (BIEP, Sep. 2019).

A su vez, la Administración Pública Nacional está integrada por el Servicio Civil, las Fuerzas Armadas y las Fuerzas de Seguridad, que totalizan 382.737 cargos. El Servicio Civil se organiza en áreas centrales, esto es, el conjunto de ministerios y secretarías y organismos

descentralizados, que abarcan un total de 187.964 agentes. Es este último universo, al cual llamaremos en adelante el Servicio Civil, sobre el cual dirigiremos nuestra mirada a lo largo de este capítulo.

No solo es su dimensión en términos absolutos lo que hace compleja la gestión de los recursos humanos, sino otros aspectos de la estructura, funcionamiento y características de los organismos que lo componen. En primer lugar, la dispersión geográfica de los ámbitos físicos en los cuales las entidades y sus funcionarios desarrollan su actividad: un extenso territorio nacional. En segundo lugar, la gestión es descentralizada, es decir, que cada jurisdicción o entidad (ministerio, secretaría, organismo descentralizado) es responsable de la ejecución de su presupuesto y de la gestión de su personal; en algunos casos, con mayor autonomía en la administración de sus recursos o para observar las políticas emanadas desde la autoridad central de las políticas del empleo público.

Esta distribución y delegación de responsabilidades en la administración tiene ventajas en términos de la cercanía y foco para la implementación de las políticas públicas sustantivas. Sin embargo, representa un desafío de enorme complejidad cuando se trata de desplegar una gestión de recursos humanos homogénea, equitativa y coordinada, que promueva y afiance los cambios en las conductas y comportamientos de las personas para una transformación digital a lo largo de todo el gobierno.

La descentralización y la relativa autonomía de los organismos han producido a lo largo del tiempo diferencias marcadas en la idiosincrasia, tradiciones y sentidos de pertenencia. Este crisol de culturas promueve una visión de silos o compartimientos estancos en los servidores públicos e impide el desarrollo de un sentido de integración dentro de un ámbito más amplio, el Estado como un todo, en tanto ámbito para el posible desarrollo de una carrera pública.

En este escenario vasto, descentralizado y heterogéneo, ¿cómo garantizar la transformación y que ella alcance a todas las áreas del Estado? ¿Cómo generar interoperabilidad a partir de ella? ¿Cómo asegurar gobernanza?

Lo dicho nos permite identificar un primer desafío: si se intenta promover una estrategia para la transformación digital, se requiere una autoridad rectora de empleo público que cuente con la jerarquía, visibilidad y competencias transversales suficientes a la hora de promover proyectos, programas e iniciativas que motoricen cambios, y en condiciones de ejercer un rol efectivo de coordinación y control.

1.b. Con relación a los regímenes laborales

En la Argentina, el empleo en el Estado nacional está regulado por leyes y convenios colectivos:

- La Ley 25.164, o Ley Marco de Regulación del Empleo Público Nacional, establece los requisitos y los impedimentos para el ingreso a la Administración Pública Nacional, los deberes y prohibiciones del empleado público, y el régimen disciplinario. No obstante, algunos organismos descentralizados están regulados por la Ley 20.744 o Ley de Contrato de Trabajo, que es la norma que regula el trabajo en el sector privado.
- El Decreto Nº214/06 homologatorio del Convenio Colectivo de Trabajo General de la Administración Pública Nacional, que consagra los mecanismos de selección, evaluación y promoción en la carrera administrativa. Existen, además, dentro del marco del convenio general, numerosos convenios sectoriales.

Con diversas denominaciones, las modalidades de empleo existentes dentro del marco de estos ordenamientos legales son:

- El régimen de personal permanente, con estabilidad en el empleo.
- El régimen de personal no permanente o transitorio, sin estabilidad en el empleo, cuya designación o contratación puede ser cancelada en cualquier momento mediante decisión fundada.

Fuera de las relaciones laborales de empleo, existen modalidades de contratación de servicios personales y profesionales, bajo las figuras de locación de servicios o de obra, generalmente utilizadas para la implementación de programas o proyectos especiales, de plazo determinado. En algunos casos, la contratación de personas para tales funciones se realiza de manera indirecta a través de convenios con instituciones o entidades especiales, como por ejemplo, las universidades nacionales.

Los marcos de referencia definidos por las leyes, decretos y convenios colectivos establecen las modalidades del ingreso, las funciones y categorías reconocidas, los derechos y las obligaciones, las jornadas de trabajo, así como las condiciones para la promoción y la movilidad. Estos marcos fueron pensados para el mundo laboral del siglo pasado, y son esencialmente rígidos, muy poco dinámicos, con frecuencia muy difíciles de adaptar cuando se busca incorporar modificaciones, actualizaciones o innovaciones en el marco de la negociación colectiva. Esta falta de flexibilidad genera, por ejemplo, dificultades para la reconversión de roles a los efectos de garantizar recursos con las capacidades necesarias.

La revolución digital a la que asistimos en el siglo XXI atraviesa y modela todos los aspectos de nuestra vida social, laboral y económica. Ha llevado a las organizaciones a flexibilizar sus estructuras y modos de organización, a innovar en sus procesos de producción y gestión, a desarrollar ambientes y modos de trabajo colaborativos, a adoptar metodologías

ágiles que se orientan a mejorar el rendimiento y la productividad, y a adoptar culturas más horizontales, basadas en una comunicación directa y fluida, en entornos cercanos que promueven la confianza y el compromiso. Lograr estos cambios supone fuertes liderazgos, que actúen con mucha responsabilidad y autogestión y rendición de cuentas.

El segundo desafío de la transformación digital en la gestión de los recursos humanos tiene que ver con la exigencia de incorporar esta visión y filosofía, fuertemente orientada a la efectividad. Se requiere introducir y difundir la gestión por proyectos, y no solo la gestión de procesos atados a funciones estáticas; se necesita agilidad para el armado y rearmado de equipos, con entrada, salida y reubicación dinámicas.

Hacen falta nuevas modalidades de organización, de contratación, de desarrollo, compensación e incentivo, que permitan captar, motivar y retener empleados altamente calificados, con las competencias para operar la transformación digital. Modalidades que no están reñidas con los valores del servicio público.

1.c. Con relación a la estabilidad del empleo público

El Estado como organización, y a través de las instituciones que lo conforman, tiene como finalidad principal la administración y el cuidado de los bienes y derechos de los ciudadanos. En el desarrollo de este cometido, debe dar cuenta permanentemente a los ciudadanos, fundando las razones de cada acción a través de actos administrativos firmados por funcionarios competentes que se hacen responsables. Estos actos, junto con sus antecedentes, van configurando la memoria institucional. En su esencia, el Estado es una organización pensada para perdurar, para mantener el orden jurídico en la sociedad. Por su empeño de asegurar la legalidad, tiende a ser conservadora y no disruptiva, y a suavizar el impacto de los cambios, incorporándolos con mayor gradualidad y a veces con menor radicalidad.

En este marco, la estabilidad en el empleo público, que en la Argentina tiene jerarquía constitucional, es coherente con la finalidad de preservación y trascendencia de políticas públicas cuya implementación, ciclo de maduración, efectos y evaluación exceden los tiempos de la gestión de un gobierno. La estabilidad asegura la conservación en el tiempo, más allá de los archivos y sistemas, de la memoria y aprendizaje institucional.

Esas políticas son operativizadas por funcionarios de carrera, en cuya formación se han invertido recursos y que a lo largo de los años han adquirido valiosa experiencia en sus áreas de competencia. Ellos deben actuar profesionalmente y por encima de identificaciones partidarias. Por lo tanto, deben ser protegidos frente al riesgo de una excesiva discrecionalidad y, algunas veces, hasta prepotencia, por parte de los funcionarios políticos que conducen el Estado en el marco de la conformación de mayorías circunstanciales en la sociedad.

Como consecuencia de esta finalidad esencial del Estado de conservación de la memoria y el aprendizaje, la innovación como valor y práctica en la cultura del Estado, con los riesgos que conlleva, estará siempre en tensión con los modos legalistas y burocráticos de la administración. Este señalamiento nos permite identificar un tercer desafío para la gestión de los recursos humanos.

Como contracara de la protección justificada y razonable que el instituto de la estabilidad consagra, los servidores públicos quedan expuestos a la indiferencia o desidia de sucesivas gestiones políticas, el abandono de instrumentos de gestión basados en el mérito y la capacitación, la distorsión de la evaluación de desempeño, donde todos aparecen «buenos» por igual, la falta de aplicación del régimen disciplinario, la escasez de ejemplos virtuosos en los cargos más altos de la conducción del Estado que reflejen valores de compromiso, austeridad y transparencia. Todos estos factores han resultado en el progresivo

deterioro de la motivación y las capacidades de los servidores públicos. Y lo que es aún peor, rescatando desde ya las excepciones, que existen en gran número, se ha erosionado la cultura de trabajo y el valor del servicio público. Con la complicidad del abandono del liderazgo por parte de autoridades y mandos medios, la estabilidad se ha distorsionado convirtiéndose para muchos en un punto de llegada y refugio de las consecuencias de un pobre desempeño.

Esto plantea un enorme desafío de transformación cultural y de reinstalación de una serie de valores y buenas prácticas en la gestión de los recursos humanos: recrear la meritocracia, promover la gestión por resultados, reconocer los logros y establecer incentivos. En suma, forjar una cultura organizacional que sea terreno fértil para la transformación digital.

2. Estrategia integral de gestión del empleo público

El objetivo final perseguido por la estrategia, integral y dinámica es promover una transformación cultural sustentable hacia una administración pública de alto desempeño.

Dicha estrategia se inserta en una **visión**: la de un Estado eficaz y confiable, que brinda servicios y protege derechos, y del cual los ciudadanos se sientan orgullosos. Persigue, como **misión**, la construcción de un Estado moderno, que incorpora la tecnología hacia adentro y en su vinculación con los ciudadanos, y que se gestiona bajo altos estándares de desempeño. Y se sostiene en los **valores** que se busca encarnar en la cultura del Estado: integridad, transparencia, calidad, innovación, servicio, eficiencia, cercanía, aprendizaje, rendición de cuentas.

La implementación de la estrategia, orientada a la visión, buscando el cumplimiento de su misión, y sostenida en los valores públicos, ocurre a través de **acciones** concretas, traducidas en programas y

proyectos que modelen nuevos modos de funcionamiento y de gestión en el sector público, y que aseguren la sustentabilidad y permanencia de los cambios.

Por eso decimos que la implementación de la estrategia integral de recursos humanos es un proceso de transformación cultural sustentable, de instalación y puesta en práctica de valores en las acciones del servicio público. Cada programa, proyecto o iniciativa encuentra su significado y, a la vez, convierte en práctica algunos de los valores mencionados para, en el tiempo, consolidar una nueva cultura de servicio público y fortalecer la confianza de los ciudadanos en su gobierno.

El modelo sugerido para ordenar la estrategia se compone de 5 dimensiones, que comprenden 12 ejes de trabajo que ordenan las diferentes iniciativas. Su valor es transmitir la integralidad del abordaje, y visualizar la necesidad de atender todas las dimensiones y ejes.

Gráfico 1. Modelo sugerido para ordenar la estrategia - 5 Dimensiones

Fuente: elaboración propia.

12 EJES DE TRABAJO

1. Conducción
   - 1.1 Visión y liderazgo: una visión y estrategia clara, entendida por todos, junto con un equipo de liderazgo que guíe las decisiones.
   - 1.2 Gestión por resultados: objetivos medibles y con una metodología de seguimiento que guíe su cumplimiento.
2. Estructuras
   - 2.1 Estructura organizacional: que permite un proceso ágil de comunicación y toma de decisiones.
   - 2.2 Organización de la fuerza laboral: una organización que cuenta con el número y perfil correcto de personas en las áreas adecuadas.
3. Personas
   - 3.1 Gestión del talento: personas con talento que son atraídas, motivadas y fidelizadas.
   - 3.2 Desarrollo de competencias: un plan de desarrollo de habilidades profesionales y personales para lograr objetivos.
   - 3.3 Gestión del desempeño: el desempeño es evaluado y tiene consecuencias en el crecimiento profesional.
   - 3.4 Gestión de compensaciones: un sistema que permite atraer y fidelizar a los mejores empleados.
4. Cultura
   - 4.1 Integridad: personas con comportamiento íntegro que velan porque se respeten las normas inherentes a la ética pública y la transparencia.
   - 4.2 Cultura organizacional: un entorno innovador, con personas comprometidas con la organización, donde se facilita la colaboración para el logro de objetivos.

5. Procesos y sistemas
   5.1 Agilidad administrativa: procesos eficientes, que agregan valor y automatizan tareas que simplifican la vida del ciudadano.
   5.2 Sistemas de gestión: que acompañan a la organización para facilitar la toma de decisiones y la gestión de los empleados.

Conviene reiterar aquí un breve párrafo, ya anticipado en la introducción: los alcances y desafíos propios de cada dimensión, así como la descripción de los programas, proyectos e iniciativas que podrían desplegarse como contenido de cada uno de los ejes, exceden las pretensiones del capítulo, ya que ameritaría un esfuerzo analítico más profundo y exhaustivo.

En el próximo apartado se identificarán algunos lineamientos, orientaciones y recomendaciones para afrontar los desafíos mencionados en el primer apartado.

3. Lineamientos, orientaciones y recomendaciones para afrontar los desafíos de la transformación digital

3.a. Con relación a las estructuras para la gobernanza y la gestión

¿Cómo asegurar la gobernanza de la transformación digital en el Estado? ¿Qué estructuras conviene crear para asegurar su implementación transversal en toda la organización?

Como política estratégica, la gobernanza de la transformación digital requiere un liderazgo sólido y claro, una estructura que lo visibilice, y funcionarios dotados con las competencias y recursos necesarios para ejercer un rol efectivo de coordinación transversal. Desde luego, también debe asegurarse la colaboración activa de los referentes y

actores clave de cada organismo, impulsados por el compromiso político e institucional de la máxima autoridad del gobierno.

Por su naturaleza de jurisdicción con mirada y alcance transversal al gobierno, la Jefatura de Gabinete de Ministros ha sido la unidad históricamente encargada de llevar adelante las transformaciones que impactan en los modos de funcionamiento de la Administración Pública. Iniciativas como el mejoramiento de los procesos de negocio, la calidad en los servicios brindados al ciudadano y la incorporación de nuevas tecnologías han sido impulsadas y promovidas generalmente desde esa unidad de la organización.

Si bien distintos formatos son viables y potencialmente exitosos, ya que lo esencial son el liderazgo del proceso, las competencias y el poder para alinear las políticas, la elección por uno u otro diseño organizacional refuerza el mensaje, hacia dentro y fuera del Estado, de la importancia otorgada a la transformación como política pública estratégica.

En la Argentina, en diciembre de 2015 se creó el Ministerio de Modernización, como entidad visible y autoridad de aplicación de la transformación digital a lo largo de toda la administración pública nacional. Paralelamente, a comienzos de 2016, se aprobó el Plan de Modernización del Estado, como mandato presidencial para la implementación de una estrategia integral que permitiera transformar el funcionamiento de la administración pública hacia adentro de la organización estatal y en relación con los ciudadanos. Dicho plan se orientó fundamentalmente a: promover el gobierno digital, abierto y transparente, aumentar la calidad de los servicios incorporando tecnologías de la información y comunicaciones, simplificar procesos de negocio y procedimientos, ofrecer al ciudadano servicios y acceso a información por medios electrónicos, y jerarquizar los recursos humanos a través de una estrategia integral.

Este Ministerio, como marco institucional para el liderazgo y la gobernanza del proceso de transformación digital, fue el órgano rector responsable por la toma de decisiones en materia de las políticas públicas de infraestructura, innovación, digitalización, datos y empleo público.

Si bien por objetivo, misión y responsabilidades el Ministerio de Modernización tenía competencias e impacto transversales (dada la autonomía administrativa y presupuestaria de cada jurisdicción), se demanda en ocasiones el apoyo político a través de normas de carácter superior para asegurar el acompañamiento y compromiso de toda la administración.

Las estructuras y las instituciones en el Estado son jerárquicas, lo cual resulta necesario para deslindar las responsabilidades de la gestión de las políticas y de la ejecución del presupuesto; los diseños matriciales no son frecuentes y en general, aunque existan, suelen no estar formalizados.

Por otro lado, como innovación en términos de estructuras, en 2017 se aprobó la creación de una nueva figura o modalidad: la «Unidad de Proyecto Especial»; esto es, una estructura *ad hoc*, creada para una finalidad y con una duración transitoria establecida desde su creación y aprobación, con los cargos o «vacantes» de base y de conducción para el cumplimiento de su finalidad, generalmente el gerenciamiento de un proyecto o programa transitorio. Creada una UPE y aprobado su presupuesto anual o plurianual, las contrataciones de los recursos humanos directos, el mecanismo para su ingreso y egreso, la jornada laboral y los horarios, la concurrencia a las oficinas, y las retribuciones, pueden administrarse con mayor flexibilidad a los fines de captar los perfiles especializados necesarios. Constituye, asimismo, una plataforma para estructurar en el Estado la gestión por proyectos.

No obstante, también es necesario consolidar en la administración equipos profesionales permanentes en el marco de la carrera pública,

en áreas de desarrollo, infraestructura y soporte, lo que obliga a atender a la criticidad de estos recursos, como veremos más adelante en el apartado III.e., en un marco ágil de promoción, rotación y estímulo.

3.b. Con relación al Nomenclador y el Directorio de Competencias

Para asegurar que el Estado cuente con las capacidades que requiere, sean conocimientos o habilidades, debe asegurarse su visibilidad en un Nomenclador de Puestos y Funciones y un Directorio de Competencias, que incorpore las actualizaciones necesarias.

El Nomenclador clasifica los puestos según las funciones existentes y requeridas por la organización en agrupamientos, familias y subfamilias. Constituye un insumo necesario para una gran cantidad de responsabilidades propias de la gestión de los recursos humanos: el desarrollo de los perfiles para los procesos de búsqueda y selección, la definición de los planes de capacitación para el puesto (itinerarios formativos) e individuales, el diseño de la evaluación de desempeño basada en competencias, el esquema de salario y compensaciones, entre otras. Se trata de un instrumento dinámico, por lo que debe actualizarse periódicamente, para incorporar los cambios en las funciones requeridas.

En orden a actualizar el Nomenclador y el Directorio, la Oficina Nacional de Empleo Público (ONEP), órgano técnico rector en estas materias en el Estado nacional, realizó entre 2017 y 2018 un detallado relevamiento en todos los organismos de los roles TIC existentes. Esta revisión no se abordaba desde la década del 90, por lo cual es de imaginar su gran desactualización, producto del profundo cambio en los «saberes y habilidades» que hoy definen la pertenencia a un puesto «informático» en comparación con los propios de aquel tiempo. Muchos de los conocimientos y destrezas que entonces conformaron

el puesto «TIC» hoy no solo resultan básicos, sino que son prácticamente necesarios para cualquier empleado.

De ese análisis surgió la definición de las nuevas funciones requeridas, lo que permitió la aprobación de la nueva familia de puestos TIC, que fue incluida en el Nomenclador.

En el cuadro que sigue se detallan las sub-familias y puestos definidos para la nueva familia TIC, cuyas categorías funcionales están alineadas con los estándares internacionales vigentes en los países más avanzados en el diseño de los servicios digitales.

Cuadro 1. Familia de puestos TIC: 8 sub-familias y 22 puestos

SUB FAMILIA	PUESTOS
Seguridad Informática y Ciberseguridad	Analista de Procesos y Normativas
	Analista de Ciberseguridad
Arquitectura de Servicios	Arquitecto de Soluciones TIC
	Analista Funcional
Desarrollo	Gestor de Proyectos de Desarrollo Informático
	Desarrollador
	Asegurador de Calidad
Implementación de Soluciones y Soporte	Gestor de Proyectos de Implementación
	Analista Técnico de Implementaciones
	Mesa de Ayuda y Soporte a Usuarios
	Soporte Técnico Informático
Gestión de Aplicaciones	Gestor de Aplicaciones Específicas
	Gestor de Aplicaciones de Soporte
Gestión de Infraestructura	Referencias de Infraestructura
	Administrador de Infraestructura
	Administrador de Redes
	Administrador de Telecomunicaciones
Gestión de Operaciones	Referente de Operaciones
	Operador de Centro de Datos
	Operador de Infraestructura
Datos	Analista de Datos
	Especialista de Datos

Fuente: Oficina Nacional de Empleo Público. Secretaría de Empleo Público – Ministerio de Modernización.

3.c. Con relación a la capacitación

Desarrollar el talento digital en el Estado significa contar con las personas adecuadas dotadas de los conocimientos y habilidades necesarias. Las capacidades de los servidores públicos son fundamentales para la prestación sostenible de servicios digitales. El desafío de la capacitación es, por lo tanto, asegurar la adquisición de las competencias requeridas para las distintas funciones y desarrollar capacidad institucional.

¿Cuáles son esas habilidades requeridas en el sector público para una transformación digital? Siguiendo los lineamientos de la OCDE, diremos que un gobierno digital requiere habilidades digitales diversificadas bajo cuatro dominios fundamentales, que identifican los diferentes roles y públicos específicos:

1. Habilidades de usuario digital: implica capacitar de manera transversal y universal a los servidores públicos para poder utilizar adecuadamente las tecnologías digitales y aprovechar al máximo las herramientas de productividad digital; en el caso del Estado nacional, esto supone comenzar por las herramientas más elementales, en un proceso de «alfabetización digital» que garantice un piso en relación con el conocimiento y uso de las nuevas tecnologías y sistemas. En este sentido, cabe destacar el gran impacto y aporte que significó la implementación transversal de la plataforma de tramitación electrónica de expedientes en el Estado nacional a partir de 2016, que operó como catalizador para un aprendizaje de habilidades digitales de usuario masivo, forzoso y en muy corto plazo, impulsando el cambio cultural.
2. Habilidades digitales especiales o complementarias: son las vinculadas con usuarios o servicios específicos (verticales),

que se transforman profundamente a través de la digitalización o que utilizan los datos como activo estratégico (por ejemplo: la recaudación de impuestos, el diseño de servicios, la comunicación del sector público).

3. Habilidades profesionales: en áreas y funciones especializadas, organismos rectores e impulsores de la incorporación de nuevas tecnologías e innovación digital, resulta indispensable atraer, desarrollar y mantener especialistas para roles estratégicos. Es el caso, por ejemplo, de los gerentes de sistemas de IT, programadores, diseñadores web, analistas de datos, especialistas en inteligencia artificial, y otras disciplinas de la frontera del avance de la revolución digital.
4. Gestión digital y habilidades de liderazgo: difundir a lo largo del sector público un pensamiento digital por default es responsabilidad de los líderes, mandos medios y enlaces de promoción de la transformación digital, quienes deben ser capaces de reconocer las oportunidades, beneficios y desafíos que dicha transformación trae al sector público. Exige formar sus competencias para estar atentos a encontrar, fomentar y desarrollar el talento, brindar a todos la capacitación básica en transformación digital, así como apoyar redes y comunidades de práctica que rompan los silos organizativos. En definitiva, lograr que operen de impulsores y promotores de los fundamentos del gobierno digital: abierto por defecto, impulsado por datos, enfocado en el ciudadano.

Derivado del Nomenclador de puestos TIC que mencionamos en el punto anterior, el Instituto Nacional de la Administración Pública (INAP), órgano rector del sistema de capacitación en el Estado nacional, desarrolló los itinerarios formativos para esos puestos, de acuerdo con sus roles y complejidades diferenciadas. Cabe destacar que dichos

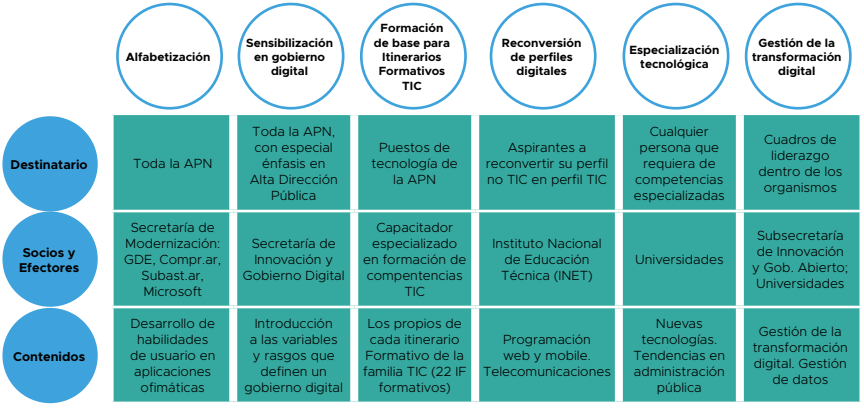
itinerarios formativos son, junto con el Nomenclador de Puestos, el Diccionario de Competencias y el Sistema de Valuación de Puestos, los ladrillos con que se construye la carrera pública y el vínculo visible entre la estrategia de capacitación y el plan de carrera.

Asimismo, y como pilar de dicha estrategia de capacitación orientada a desarrollar y fortalecer las habilidades digitales para los cuatro dominios identificados por la OCDE, el INAP ideó el «Programa de Habilidades para la Transformación Digital», que se organizó a partir de seis objetivos estratégicos:

i. Alfabetización digital: desarrollo de habilidades de usuario en aplicaciones ofimáticas.
ii. Sensibilización en gobierno digital: introducción a las variables y rasgos que definen un gobierno digital.
iii. Formación de base para itinerarios formativos TIC: contenidos propios de cada uno de los 22 IF (puestos) de la familia TIC.
iv. Reconversión de perfiles digitales: programación web y *mobile*; telecomunicaciones.
v. Especialización tecnológica: nuevas tecnologías; tendencias en la administración pública.
vi. Gestión de la transformación digital: gestión de la transformación digital y gestión de datos.

En el gráfico que sigue se detallan los destinatarios específicos, los socios del aprendizaje y los contenidos temáticos propios para cada uno de los seis objetivos, vinculados con el dominio informático, la gestión de la innovación y el desarrollo del liderazgo para el Estado nacional argentino.

Gráfico 2. Programa de habilidades para la transformación digital



Fuente: Instituto Nacional de la Administración Pública. Secretaría de Empleo Público – Ministerio de Modernización.

3.d. Con relación a los incentivos

¿Cómo establecer incentivos para la atracción y retención de los perfiles TIC que se necesitan en el Estado?

En la Argentina , y en general en la región, el mercado laboral para los puestos relacionados con las especialidades TIC se caracteriza por una alta demanda, gran dinamismo y altos índices de rotación. Por otro lado, es muy valorado el *expertise* práctico en aplicaciones o lenguajes específicos, con independencia muchas veces de la titulación académica, lo que hace que ya desde los puestos con menor experiencia, las remuneraciones estén por encima de la media del mercado y no se apliquen los requisitos de titulación válidos para otras áreas o responsabilidades. Por otro lado, el estilo y las modalidades de trabajo suelen ser más informales y descontracturados, y las motivaciones no remiten necesariamente al desarrollo de una carrera ligada a una organización. Antes bien, los profesionales del mundo de la tecnología

privilegian más la orientación y el interés hacia «el proyecto», valoran especialmente el nivel del desafío profesional, la oportunidad para nuevos aprendizajes, o la contribución e impacto social de la tarea.

Dadas estas características particulares, compatibilizar los intereses de los empleados y la organización es un gran desafío cuando se trata del Estado. Como describimos anteriormente en el apartado 1.b., las modalidades de empleo existentes en el Estado son el régimen de planta permanente y el régimen de planta transitoria. Por fuera de estos, actúan las modalidades de contratación de servicios profesionales. Asimismo, en el apartado 3.a. mencionamos la Unidad de Proyecto Especial como figura organizacional de duración transitoria asociada con objetivos específicos, y no con los de funciones o roles más permanentes en la organización.

Atraer y retener el talento digital en el Estado, necesario para producir una transformación digital, requiere en la Argentina, como en muchos otros países de la región, de una alta dosis de creatividad y flexibilidad en el uso de herramientas de estructura organizacional y de empleo. Requiere, también, poner en juego estímulos monetarios y no monetarios, rotación entre áreas o proyectos y oportunidades de formación profesional. Son aspectos pocas veces regulados por los convenios colectivos, que fueron pensados para las relaciones laborales propias de los métodos de producción del siglo pasado y para el desarrollo de carreras extendidas, pero no para los nuevos paradigmas y desafíos de la economía del conocimiento en tiempos de la revolución digital.

Dentro de los incentivos monetarios, existe en la administración desde hace muchos años un concepto salarial especial, la «función informática», aplicable a quienes cumplen tareas asociadas con alguna disciplina informática. Con el tiempo, el uso de este suplemento se fue distorsionando, debido, por un lado, a que las funciones sobre las cuales

se había diseñado su aplicación quedaron obsoletas; y, por el otro, al utilizarse en algunos casos como mero adicional salarial, por lo que perdió su especificidad.

Como resultado de la actualización de los nuevos puestos de la familia TIC, se crearon las condiciones para que, a través de la negociación paritaria, se reformulara el concepto de pago por «función informática». Es necesario alinear su alcance y cuantía a la realidad de las nuevas funciones y experticias establecidas y, en la mayor medida posible, al mercado. Si bien este concepto aplica técnicamente, según los convenios, solo al personal bajo el régimen de estabilidad, podrá generarse su equivalente para las otras modalidades.

Debe quedar claro que se requieren en esta materia soluciones sostenibles, que pueden llevar a romper con los marcos de competencias y estructuras salariales existentes, así como innovar en el modo en que se deba gestionar, evaluar y retener estos empleados dotados de conocimientos y habilidades especiales para la transformación digital. Finalmente, es preciso lograr un adecuado balance entre los recursos propios y los tercerizados, para mantener el debido control sobre los procesos críticos.

3.e. Con relación al nuevo contexto de trabajo remoto

Por otro lado, hemos visto irrumpir en el escenario de los últimos meses la modalidad de trabajo remoto o teletrabajo, con una explosión forzosamente masiva debido al confinamiento obligatorio derivado de la pandemia COVID-19.

Pasada la emergencia, y a partir de los aprendizajes de esta implementación en gran escala, es de esperar que se sostenga su aplicación total o parcial a muchas áreas y empleados, sobre bases más racionales y de manera planificada. Es conveniente, entonces, prestar atención a su aplicación en términos de herramienta de atracción y retención de los perfiles críticos para la transformación digital.

La implementación de la modalidad de teletrabajo requiere, en el plano individual y del funcionamiento de los equipos, el fortalecimiento de nuevos conocimientos particularmente ligados con el dominio informático, el uso de nuevas plataformas digitales y el trabajo colaborativo. También se requieren nuevas competencias en relación con habilidades de comunicación multidireccional, de autogestión, de organización del tiempo y distribución de tareas equitativa, y del control de su ejecución.

El trabajo remoto demanda una mayor disciplina personal, responsabilidad y compromiso. Esto atañe muy especialmente a los líderes; ellos deben extremar sus habilidades emocionales y de comunicación, construir vínculos de confianza dentro de los equipos, atender a la planificación y fijación de objetivos con equidad, establecer la agenda de reuniones, y respetar los horarios pactados para la jornada. Cuando se logra desarrollar de manera organizada y productiva, y se logran administrar las interferencias propias de un entorno diferente, el teletrabajo trae grandes beneficios en la optimización del uso del tiempo y la conciliación de la vida laboral y personal.

Nuevos contextos requieren también, en alguna medida, la adaptación de las regulaciones para no desproteger derechos. Los proyectos de leyes o reglamentaciones para el teletrabajo regresaron en estos últimos meses a las agendas legislativas. Es fundamental que las propuestas persigan la promoción del trabajo remoto en la sociedad como un medio para lograr más empleo y de mejor calidad, y mayores oportunidades de inserción para grupos vulnerables. Para ello, debe romperse con los paradigmas rígidos de la legislación laboral, que tienden a confundir flexibilidad con desprotección, en un mercado laboral que se verá transformado inevitablemente por la revolución digital.

En términos de oportunidades para la captación de talento digital y su retención, el teletrabajo permite flexibilidad en el horario y lugar

de prestación del servicio; permite, asimismo, poner en juego el reconocimiento a la inversión en equipamiento y a los gastos operativos. En sí mismo, el teletrabajo puede verse como un beneficio.

Por otro lado, el trabajo remoto instala y fortalece una cultura de trabajo por objetivos, con foco en el cumplimiento de hitos y plazos, no solo entre los teletrabajadores, sino en toda la organización. Ello facilita el camino para el diseño y la aplicación de evaluaciones de desempeño atadas al cumplimiento de objetivos individuales asociados con los organizacionales, lo cual brinda una oportunidad adicional para reconocer y premiar a quienes mejor se desempeñen.

4. Lecciones aprendidas del informe de la OCDE

La Organización para la Cooperación el Desarrollo Económicos (OCDE), a través de la Dirección y Comité de Gobernanza Pública, lleva adelante, como una de sus líneas principales de trabajo e investigación, el proyecto de Gobierno Digital.

Los hallazgos del informe de dicho organismo sobre «La transformación digital en el sector público» (Sep. 2017) echan luz sobre algunos aspectos de la gobernanza de la transformación digital y los requerimientos para el desarrollo de un servicio público digital, necesarios para su implementación exitosa. A continuación, algunas de sus principales conclusiones.

a. Sobre la gobernanza de la transformación digital:

- ✓ La implementación y uso efectivo de las tecnologías digitales en el sector público, orientado a brindar mejores servicios en la era de la economía y sociedad digitales, depende de una efectiva gobernanza sobre las tecnologías de información y comunicación en las administraciones públicas.

- ✓ Si bien dicha gobernanza puede lograrse a través de diversos marcos institucionales conforme los diferentes contextos o características, su formulación debe contemplar necesariamente los siguientes requisitos:
  - o Un fuerte liderazgo, con claridad de roles y responsabilidades.
  - o Contar con las competencias y recursos necesarios para alinear el planeamiento, la formulación de políticas y la implementación transversalmente al gobierno.
  - o Contar con el empoderamiento y soporte político necesarios para conducir la transformación, coordinar acciones entre diferentes actores, y exigir responsabilidad por los resultados.
  - o Continuidad y coherencia en el tiempo, en el marco del sostenimiento de una agenda de gobierno digital.
- ✓ Muchas de las formas de organización, procesos de negocio, maneras de proveer servicios y procedimientos internos en la administración pública son producto de una «adaptación» del paradigma «analógico» del pasado a la actual era digital. Pero un gobierno analógico no puede atender las necesidades de la economía y sociedad digitales.
- ✓ Se requieren nuevas estructuras institucionales, marcos de gobernanza y procesos para promover una transformación hacia un sector público «orientado al usuario».
- ✓ Esas nuevas formas de organización, más horizontales y en redes colaborativas, promoverán soluciones más ágiles, económicas e innovadoras.

b. Conectar la transformación digital con la gestión de los recursos humanos:

- ✓ Servidores públicos con las habilidades digitales necesarias, y un liderazgo competente son condiciones esenciales para el éxito, sustentabilidad y dinamismo de un proceso de transformación digital en el sector público.

- ✓ Las tendencias tecnológicas demandan habilidades digitales especializadas y diversas: análisis de datos, diseño de experiencia de usuario, programación, mapeo de servicios, prototipado; todas ellas orientadas a repensar las políticas y la provisión de servicios a la ciudadanía.
- ✓ Como consecuencia, el sector público deberá asegurar un efectivo y constante acceso a la capacitación y actualización de saberes digitales, tanto a los servidores públicos como a los directivos y líderes.
- ✓ Los esfuerzos no solo deben orientarse al fortalecimiento de las habilidades digitales, sino también a sostener la enorme transformación cultural que implica la conversión a un gobierno digital.
- ✓ Las nuevas formas de trabajo emergentes, como el trabajo remoto, propician entornos digitales colaborativos, pero a la vez exigen habilidades más complejas en los servidores públicos y en su liderazgo.

Conclusiones

La transformación digital del sector público apunta al uso estratégico de las tecnologías digitales y los datos para la creación de valor público. No hay transformación digital posible sin el marco de una estrategia integral que involucre a las personas, sus motivaciones, su participación, y su incentivo.

La Administración Pública Nacional en la Argentina presenta el desafío de su dimensión, su descentralización y la heterogeneidad de las culturas, lo cual hace más complejo el despliegue de iniciativas de transformación transversales.

El ámbito público, por naturaleza, historia y tradición, presenta mayor apego a las formas burocráticas, en tensión con los valores de

agilidad, apertura e innovación promovidos por la cultura digital. Los marcos de las relaciones laborales son rígidos y poco ágiles, y su modificación está sujeta a la negociación colectiva.

La estabilidad en el empleo público es consistente con la finalidad de preservar memoria institucional y continuidad de las políticas públicas, a la vez que protege a los servidores públicos de los excesos de discrecionalidad política. No obstante, no debe entenderse como protección ante el mal desempeño, lo cual interpela a la calidad del liderazgo y la responsabilidad de los funcionarios que conducen.

La gobernanza de la transformación digital requiere un liderazgo sólido y visible; funcionarios con responsabilidades claras y dotados del poder necesario para coordinar acciones a lo largo de todo el gobierno, y con el respaldo político e institucional de la máxima autoridad del gobierno.

La demanda de talento digital y su dinamismo exigen extremar la creatividad y flexibilidad en las formas de organización y empleo, y los incentivos monetarios y no monetarios para atraer y retener el talento digital en el Estado, forzando los límites de las formas tradicionales reguladas para el servicio público.

La actualización del Nomenclador de puestos y el Diccionario de Competencias, al incorporar los perfiles TIC vigentes, visibiliza las funciones requeridas como insumo para los procesos de selección, capacitación, gestión del desempeño y esquemas salariales.

La gestión del desarrollo de habilidades digitales requiere la asociación virtuosa entre la oferta (esto es, la capacitación para el desarrollo de habilidades digitales generales y específicas en usuarios, profesionales, especialistas y líderes) y la demanda (asegurando que los perfiles de los puestos, los procesos de selección y los sistemas de evaluación consideren las habilidades digitales necesarias).

El teletrabajo flexible brinda una oportunidad para la captación y retención de habilidades digitales, a la vez que fortalece la gestión por objetivos.

La instalación de un gobierno digital conlleva modificaciones en los procesos y las operaciones y, por lo tanto, impacta en la cultura de trabajo.

La estrategia de recursos humanos debe orientar y fortalecer el cambio hacia el nuevo paradigma de una cultura de servicio público centrada en el usuario; que opera sobre plataformas digitales compartidas; que basa sus decisiones en la evidencia aportada por los datos; y que es proactiva en la búsqueda de nuevas soluciones a través de las tecnologías de vanguardia.

PABLO MARTÍN LEGORBURU. Ingeniero Civil, UBA. Máster en Economía y Administración de Empresas (ESEADE).

Desarrolló los primeros 20 años de su carrera laboral en empresas líderes del sector privado del área de ingeniería (McKee del Plata), petróleo (ESSO) y de servicios (Multicanal).

En 2007 se incorporó al sector público en el Gobierno de la Ciudad de Buenos Aires, como Director General de Administración de Recursos en el Ministerio de Educación y, posteriormente, como Subsecretario de Gestión de Recursos Humanos en el Ministerio de Modernización.

Entre diciembre de 2015 y diciembre de 2019 se desempeñó como Secretario de Empleo Público en el Ministerio de Modernización del Gobierno Nacional, siendo responsable del diseño e implementación de políticas de desarrollo de los recursos humanos, la gestión del empleo, del rendimiento, de la capacitación y la transformación cultural de los servidores públicos.

CAPÍTULO 10

Ética y gobernanza tecnológica en la era de la complejidad

Martín Parselis

Introducción

Muchas veces oímos que no hay que inventar la rueda, pero muy pocas nos preguntamos si necesitamos una rueda. ¿Por qué no utilizaríamos las tecnologías que ya existen? ¿Por qué nos preocuparíamos por cómo se hacen? ¿Por qué pensar en quiénes las hacen, si todo depende de cómo las usemos? Cada una de estas preguntas tiene respuestas extensas y diversas. En este capítulo haremos un recorrido que se inspira en estas preguntas sin pretender agotarlas, pero resaltaremos algunos aspectos clave de nuestra relación particular con las tecnologías, subrayando algunos elementos relacionados con su influencia en la esfera pública.

Avanzaremos en las relaciones humanas entre quienes hacen las tecnologías y quienes las utilizamos; y en cómo las tecnologías nos relacionan una vez que existen. Como en toda relación humana, las acciones implican a otros, y entonces debemos considerar algunos aspectos éticos involucrados en estas relaciones. Dado que muchas tecnologías

también forman parte de nuestra vida pública, además de transformarnos día a día, será necesario establecer algunas guías de acción derivadas de la ética para la gestión pública.

1. El entorno tecnológico

Alan Kay afirmó hace unos años que tecnología es todo lo que no estaba en nuestro entorno cuando nacimos. Sin dudas, es una frase muy poderosa y un atajo muy atractivo para hablar de tecnologías, dicha nada menos por quien es considerado el «padre de la computación personal». En consecuencia, para Kay, lo que consideramos tecnología depende de nuestro momento histórico. Hay varios enfoques generacionales sobre las tecnologías, aunque suelen orientarse hacia el estudio de comportamientos más que a cuestiones conceptuales (como el caso de los *millennials* y *centennials*). La frase describe algo muy cierto: todo lo que estuvo antes de nosotros forma parte de nuestro entorno, nos precede, es como si siempre hubiera estado allí, y prácticamente dejamos de verlo: se encuentra «naturalizado».

Tecnologías como las TIC, internet, la distribución de agua potable o la industria de los alimentos están naturalizadas. Entonces, ¿para qué las Naciones Unidas realizan esfuerzos por analizarlas e intentar elaborar acuerdos multilaterales para su transformación, su gestión o su regulación? Si todo aquello que naturalizamos «simplemente está», ¿por qué hay científicos que hoy discuten la mejor expresión de la ley de gravedad? Pensar en lo que nos rodea, en cómo es nuestro entorno, es un esfuerzo de «desnaturalización». Por otra parte, esta naturalización no solo es relativa a una generación, sino también a comunidades distintas. Tan así es, que la mitad de la población no cuenta con acceso a internet (como informa la International Telecommunications Unit), y poco menos de 1 de cada 3 habitantes no cuentan con acceso seguro al

agua potable (como informa la World Health Organization). Pensar en el mundo es desnaturalizar la idea de que todas las comunidades viven como nosotros.

2. Preguntarnos por la tecnología

Para explorar la tecnología necesitamos hacerla visible y dejar de considerar que está allí sin más, cuestionarla y entender los procesos y condiciones que le dan origen, además de advertir las implicancias de las tecnologías actuales y futuras. Evitarlo implica el riesgo de «llegar a perder la conciencia de la técnica y de las condiciones [...] morales en que esta se produce, volviendo, como el [hombre] primitivo, a no ver en ella sino dones naturales que se tienen desde luego y no reclaman esforzado sostenimiento» (Ortega y Gasset, 1939:107).

En la era de mayor acceso al conocimiento, y de tecnologías que atraviesan casi todas las actividades humanas en muchos lugares, no podemos, ni debemos, quitarla de nuestro horizonte cognitivo, por diversas razones. Una de ellas es la comprensión de nuestro entorno vital, algo que parece evidente; pero, además, para no condenarnos a un futuro no deseable, como lo exponen Paul Dourish y Scott Mainwaring: «La pregunta predominante, ¿qué construiremos mañana?, nos impide ver las preguntas que deberíamos hacernos sobre nuestra responsabilidad actual por lo que construimos ayer» (Morozov, 2015:19).

Si bien el fenómeno técnico presenta gran complejidad en todas las épocas, el advenimiento de la llamada cuarta revolución industrial –sobre la base de la aceleración y tecnologías que cada vez menos se producen y difunden en forma estrictamente local, sino más bien en grandes entramados globales–, cambia nuestra vida de forma cada vez más acelerada. Pensemos en una lista corta de algunas tecnologías que ya están con nosotros, como la inteligencia artificial, la robótica, internet de las

cosas, los vehículos autónomos, la impresión 3D, la nanotecnología, la biotecnología, la ciencia de materiales, el almacenamiento de energía o la computación cuántica. Todas ellas tecnologías de alcance global que desafían nuestra relación con ellas y nuestras relaciones sociales desde los afectos hasta el sentido del trabajo (Schwab, 2016).

En este escenario, la sensación de familiaridad se opone al conocimiento que tenemos sobre ellas. Eventualmente nos enteramos de algún efecto nocivo, de consecuencias no deseadas o, como en el tratamiento del COVID-19, del rol que juegan las tecnologías en la investigación dentro de la incertidumbre propia de un virus que no conocemos. En esos casos, sentimos que estamos atrapados y alejados de toda posibilidad de tomar decisiones sobre ellas. La familiaridad convive con el extrañamiento.

3. Nuestra relación con la tecnología

El estado de salud de Nietzsche empeoró en 1879, y poco después encargó una máquina de escribir como ayuda para desarrollar sus obras. Su amigo Köselitz advirtió que la expresión había cambiado, era más «estricta y telegráfica», más contundente. Entre sus intercambios epistolares, Nietzsche le responde: «Tenéis razón. Nuestros útiles de escritura participan en la formación de nuestros pensamientos» (Carr, 2011:22).

La composición de nuestro entorno influye en la forma de acceso al mundo y en la configuración de nuestro pensamiento. Es un problema que no parece nuevo, aunque dada la escala y la multiplicidad de artefactos que nos rodean, el problema parece tener una gravitación mucho más importante que en los tiempos de Nietzsche.

En la segunda mitad del siglo XX, McLuhan aseguraba que «los medios, al modificar el ambiente, suscitan en nosotros percepciones

sensoriales de proporciones únicas. La prolongación de cualquier sentido modifica nuestra manera de pensar y de actuar, nuestra manera de percibir el mundo. Cuando esas proporciones cambian, los hombres cambian» (McLuhan y Fiore, 1967:41). Ya iniciado el siglo XXI, Lash asegura que las nuevas tecnologías (digitales, informáticas, TIC) impulsaron un cambio en nuestra forma de vida; comprendemos el mundo por medio de sistemas tecnológicos y actuamos como interfaces de humanos y máquinas, como conjunciones de sistemas orgánicos y tecnológicos (Lash, 2005:42).

Desde un punto de vista general, todas las tecnologías provienen de algún proceso constituido por una red de decisiones. Como resume Broncano (2008:28), «las tecnologías tienen historia», a diferencia de los objetos naturales. Este contenido intencional puede analizarse en cada una de las tecnologías y artefactos en forma particular y también en forma global para todas las tecnologías, y ambas escalas no son independientes. Cada tecnología es resultado de, al menos, una combinación de aspectos técnicos y de aspectos culturales. Dado que no surgen espontáneamente, tienen historia: hay personas que toman decisiones en los planes de las tecnologías que están creando. Una vez creadas, accedemos a su uso según reglas que ya están definidas, y que usualmente debemos aprender. Esto significa que, como usuarios, adoptamos «gestos» que han sido pensados y diseñados por otros para utilizar las tecnologías según nuestros propios fines (Parselis, 2016:114).

Los aspectos técnicos suelen ser difíciles de abordar para quienes no están familiarizados con las profesiones técnicas (ingenieros, programadores, diseñadores). Cuando exista la vacuna contra el COVID-19 entenderemos rápidamente para qué sirve, pero es poco probable que sepamos mucho sobre su acción en nuestro organismo (si cambia ARN, si incorpora anticuerpos, de qué se trata un virus vivo, o un virus atenuado, etc.). Esta dimensión técnica utiliza lenguajes propios y se

orienta a la «función técnica» (el modo en que un automóvil es capaz de transformar combustible en movimiento, por ejemplo). A su vez, hay un diseño sobre «cómo hacerlo funcionar». Sin saber «cómo funciona» un automóvil, podemos aprender «cómo hacer que funcione» a través de elementos operativos (como pedales, volante).

Los aspectos culturales están asociados a lo que se busca, a las finalidades que guían el desarrollo de una tecnología. Cada tecnología tiene «razones» para ser desarrollada, resumidas en intereses, propósitos o motivaciones. La búsqueda de la vacuna contra el COVID-19 o el tratamiento de pacientes con plasma tiene un conjunto de motivaciones claras y, en algunos casos, también el interés por patentarlas. Pero también se asocia a una época, al conocimiento disponible y a las formas de organización para su producción. Es decir, que hay componentes culturales particulares que guían el diseño de una tecnología particular, y también elementos que se comparten socialmente, como lenguajes, conocimiento disponible, representaciones sociales o imaginarios.

La combinación entre los aspectos técnicos y culturales se producen en el contexto de diseño y producción, y también en el contexto de uso. En ambos contextos hay humanos que toman decisiones según sus finalidades. Las tecnologías son una forma de relación entre estos humanos, entre los que decidieron cómo son y los que las utilizamos. Las tecnologías se vuelven extrañas porque no podemos advertir lo que ocurre en el contexto de diseño y producción. Esto puede entenderse como una «desvinculación» entre estos contextos, producida por una serie de barreras que se describen a continuación.

Desvinculación técnica: se trata de las barreras que dificultan la comprensión de los mecanismos técnicos. Es lo que da origen a la idea de «caja negra»: no sabemos qué es lo que ocurre dentro, aunque podamos disfrutar de sus resultados. El protocolo de internet es abierto,

de dominio público y cualquiera puede estudiarlo, a diferencia de un *software* propietario. Muchas *apps* brindan algún servicio valioso, pero en muchos casos también realizan otras funciones (como la toma de datos de nuestras computadoras). Esto es aún más crítico cuando las finalidades provienen de organismos públicos, debido a que se bloquea la posibilidad de que la ciudadanía sepa qué es lo que esa tecnología hace y cómo se gestiona la información obtenida. El voto electrónico o el rastreo de casos de infectados por COVID-19 son un buen ejemplo para esta discusión.

Desvinculación cultural: por lo general, las razones por las que se desarrolla una tecnología difieren de las razones por las cuales la utilizamos. Coinciden parcialmente en una expresión técnica que, como usuarios, advertimos que nos posibilita algo. Una plataforma de venta *online* intenta conectar oferta y demanda; cuando esto ocurre, entendemos que cumple con su objetivo. Pero estas plataformas también tienen otras finalidades, asociadas con el mercado y con la toma y análisis de datos de las transacciones; y a medida que crecen, también crean servicios conexos para escalar su negocio. Nada de esto es parte de los intereses del usuario al realizar una compra. Si pensamos en algunas tecnologías ampliamente difundidas, los intereses del usuario pueden verse afectados. ¿Es posible mantenerse en el mercado laboral actual sin utilizar un celular? ¿Podemos dejar de vacunarnos por decisión propia? ¿Podríamos decidir entre alternativas de viaje con menor huella de carbono en lugar de cruzar el Océano Atlántico en avión? En estos casos «de los que no podemos salir», parece necesario que la coincidencia entre nuestras finalidades y aquellas relacionadas con el desarrollo de las tecnologías sea mayor.

Desvinculación representacional: tenemos alguna representación mental sobre las tecnologías que nos rodean, cuya construcción depende de cada uno de nosotros y de las representaciones sociales

vigentes. La palabra «escritorio» mantiene un significado tradicional (aquel objeto que tiene una tabla y cuatro patas), pero también tiene un significado que adoptamos socialmente a partir de los ochenta, cuando los sistemas operativos representaron gráficamente carpetas y archivos en un nuevo escritorio. Naturalizamos esta idea, y aprendimos cómo movernos operativamente en ese espacio representacional de la computadora. Este aprendizaje se asocia a reglas y procedimientos, que también fueron definidos por otros humanos en el contexto de diseño. Pero una computadora no funciona sobre la base de carpetas y archivos, sino en una compleja combinación de capas entrelazadas, desde procesadores físicos, pasando por varias capas de código, hasta las representaciones gráficas, como una carpeta. Esto es análogo al volante y los pedales del automóvil. Aprendemos a operar las tecnologías en forma eficiente, pueden ayudarnos a cumplir nuestros fines, pero nada de eso nos indica qué es lo que ocurre realmente mientras lo hacemos. A medida que aumenta la capacidad de procesamiento informático, aumenta la posibilidad de representar elementos simbólicos, en un lenguaje que los humanos podemos entender. No necesitamos leer códigos y programar fórmulas: con algunos botones con contenido icónico ese trabajo queda dentro de la «caja negra», y comenzamos a compartir esas representaciones socialmente. El escritorio, el pincel, la diapositiva, el engranaje, un corazón, una cámara; todos ejemplos que forman parte de lo que llamamos interfaz, y que nos guían en el uso y también en la interpretación sobre las tecnologías. Cuando extendemos estas interpretaciones a una comunidad, vemos que la forma en la que hablamos de las tecnologías usualmente se basan en este contenido simbólico. Es decir, que nuestras representaciones sociales se construyen sobre los contenidos de las interfaces, desvinculadas de lo que realmente ocurre. Esta situación puede parecer menor, pero sin embargo requiere mucha atención. Un buen ejemplo son los

alimentos: si nos quedamos con la satisfacción del deseo del «sabor a» sin ocuparnos de lo que realmente comemos, sabemos que podríamos correr el riesgo de alimentarnos mal. Cuando pensamos en tecnologías que involucran algunos aspectos ciudadanos sucede algo similar: la comodidad de un sistema de sufragio no debe opacar el conocimiento de lo que realmente ocurre con cada uno de nuestros votos; el registro de nuestros movimientos en nuestra ciudad no debe esconder el problema de la utilización de la información y, eventualmente, los riesgos para nuestra privacidad. Es razonable, entonces, que adoptemos la comodidad de las interfaces, pero no a costa de oscurecer lo que realmente está ocurriendo.

Desvinculación de la gestión de lo común: las tecnologías van más allá de su ciclo de vida; antes hay recursos, y luego hay residuos. Los elementos que posibilitan su existencia muestran complejidad en cuanto a las decisiones previas y posteriores, ya que los recursos requieren explotar algún bien (agua, energía, minerales), el descarte implica el depósito en alguna parte (que genera islas de plástico en océanos, o contaminación por metales en ríos), y su utilización consume algún tipo de energía (como la liberación de gases en relación al cambio climático). Si todo esto es necesario para que exista una tecnología, no parece adecuado que se puedan tomar decisiones particulares sobre bienes que nos involucran colectivamente. Ampliaremos este punto en el apartado sobre *commons*.

Si estas barreras son bajas, las tecnologías serán menos extrañas (Parselis, 2016:115).

4. Ética, política y tecnología

Hay humanos que toman decisiones sobre cómo son (y cómo serán) las tecnologías, y hay humanos que las utilizamos. Adoptamos

gestos y construimos representaciones sobre ellas, además de transformar hábitos sociales e interpretaciones del mundo. Nuestro entorno vital está poblado de tecnologías que han diseñado y desarrollado otros. También identificamos que la relación entre estos humanos tiene barreras que no se reducen al conocimiento técnico, y que no se trata de una relación abierta y transparente. Además, la red de decisiones involucradas en el diseño no se reduce a un humano, sino a grupos que pueden tener distintos intereses que convergen en un proyecto de desarrollo. Esta relación entre voluntades humanas es el primer punto de cualquier análisis ético y político con respecto a la tecnología. Cuando pensamos en tecnologías de las que no podremos prescindir, cabe una pregunta que está lejos de los aspectos técnicos y muy cercana a cuestiones éticas: ¿puede la voluntad de unos determinar unilateralmente las transformaciones de los otros?

Supongamos que esta pregunta es exagerada y que la libertad de acción dentro de una sociedad organizada otorga flexibilidad en las ideas que inspiran muchos de los desarrollos y emprendimientos. De hecho, disfrutamos de muchos beneficios derivados de esas libertades, desde el entretenimiento hasta los instrumentos de diagnóstico preciso de enfermedades. Veamos algunos ejemplos para juzgar mejor estas relaciones en distintos casos.

Langdon Winner vuelve sobre los puentes diseñados por Robert Moses que cruzan las vías terrestres que unen Nueva York con zonas de esparcimiento en Long Island, un caso paradigmático muy estudiado y documentado. Moses fue una persona muy influyente y responsable de muchas obras que han dado a Nueva York su aspecto moderno a mediados del siglo XX. Antes de cruzar cada puente, hay carteles que avisan a los conductores sobre la baja altura de paso. ¿Por qué se diseñarían puentes tan bajos? Si pensamos en construcciones tan antiguas como las romanas, vemos que la altura no parece ser una condición técnica en

el siglo XX. El puente romano sobre el río Tormes en Salamanca (siglo I, 350 metros de largo y 10 metros de altura) o el acueducto de Segovia (siglo II, 800 metros de largo, 28 metros de altura) demuestran que no hay ninguna limitación técnica que haya determinado la altura de los puentes de Moses. Toda la documentación se dirige a un criterio de diseño que buscaba que pasen los automóviles y no los buses; los primeros eran utilizados por las personas que podían acceder a ese tipo de vehículos personales, y los buses eran utilizados por personas más pobres, especialmente negros. En resumen, se diseñó una tecnología para que funcionara como filtro social en un entorno de libre circulación pública.

Este contenido político de las tecnologías fue estudiado desde varias perspectivas, y en todos los casos se hace ver el rol del diseño, de las personas que deciden que una tecnología sea de un modo u otro, e incluso entre qué alternativas eligieron. En el caso de los puentes conviven dos normativas, la normativa de libre circulación con una normativa *de facto* encarnada en infraestructuras. Por ello Winner afirma que hay tecnologías que se asemejan a decretos legislativos, que nos ordenan socialmente una vez que existen.

Esto nos conduce a un campo que no suele ser muy explorado, pero que es necesario diferenciar de las políticas tecnológicas. La relación entre tecnología y política tiene una historia relativamente reciente, que vemos expresada en secretarías o ministerios de Ciencia y Tecnología en muchos países (en Argentina hay una tendencia a prestar mayor atención a la ciencia que a la tecnología). Las políticas relacionadas con la tecnología suelen definir industrias clave sobre las que estratégicamente un país decide formarse, desarrollar *knowhow* y operar. Tal es el caso de la energía nuclear, la clonación, o las actividades espaciales que en Argentina tienen un desarrollo considerable, produciéndose la transferencia de la investigación científica hacia el desarrollo tecnológico.

Esta tendencia hacia políticas específicas en materia tecnológica se relaciona con modelos teóricos comúnmente «lineales» que establecen distintas relaciones entre institutos de investigación e industrias que son áreas prioritarias, lo que da lugar a instituciones públicas que fomentan y evalúan la calidad de la investigación, como el caso del Conicet y las universidades. Estos esfuerzos son relevantes para mantener mejor posicionamiento relativo con respecto a otros países y regiones, además de contribuir potencialmente a la competitividad y a la soberanía tecnológica. Se trata, sin dudas, de capacidades estratégicas para un país, que se complementan con las del sector privado y en proyectos mixtos. El *software* ha tenido un desarrollo importante en los últimos años, del mismo modo que muchas industrias han incorporado nuevas tecnologías e innovaciones muy destacadas en agroindustria.

El caso de los puentes, entre tantos otros, hace visible la relación entre los fines buscados en el diseño y sus efectos en el uso. Podríamos analizar estas relaciones en cualquier tecnología, independientemente de si se trata de un proyecto privado o público, pero dado que la responsabilidad asociada al Estado responde a intereses públicos, parece ineludible estudiar bajo qué condiciones éticas se da la relación entre los decisores y la ciudadanía. Esta relación es tan importante que Quintanilla (2020), el ideólogo de las "tecnologías entrañables" (que inspiran las distintas desvinculaciones mencionadas), ha compilado un libro sobre "filosofía ciudadana" enfocado en ciencia y tecnología.

Además de las tecnologías directamente asociadas al Estado, toda tecnología que implique el espacio público, gran escala o produzca cambios profundos en hábitos sociales, también podría ser parte de la mirada estatal, como evaluador y, eventualmente, regulador. Esto existe en normativas de impacto ecológico, por ejemplo, aunque puede extenderse a otro tipo de impactos, como ocurre en Alemania, donde 120

investigadores de la Universidad de Karlsruhe trabajan en un ente autárquico que, ante cada proyecto tecnológico que deba ser legitimado por el Parlamento, acerca sus estudios para un voto informado sobre la base de la aceptación social del proyecto. Este tipo de evaluaciones tecnológicas claramente son un aporte para una implementación de tecnologías más democráticas y debidamente consultadas con la ciudadanía. Entonces, el debate parlamentario también se nutre de la opinión de los interesados directos, y no solamente de datos económicos y técnicos.

Las tecnologías relacionan distintos actores, como instituciones, empresas y ciudadanos, a través de decisiones humanas; y, por lo tanto, son parte de una relación ética y política. Es importante diferenciar entre las tecnologías que ya existen (que ya están diseñadas, que ya no son flexibles, y que se gestionan actualmente) frente a aquellas que se están pensando o diseñando para el futuro, y que, entonces, todavía pueden cambiar.

Mientras todas estas dinámicas están ocurriendo, no debemos perder de vista que nos encontramos en un mundo que muestra niveles de complejidad muy altos con respecto a otras épocas. Esto implica que no podemos simplificar las cuestiones éticas y políticas solamente en la relación entre unos pocos actores para una sola tecnología.

5. Una nueva ética

Buena parte de nuestro entorno vital y de la posibilidad de acceso al mundo se encuentra conformado por tecnologías, y cada una de ellas tiene una historia de decisiones. Este entorno se vuelve más complejo a medida que pasa el tiempo. Es incomparable la presencia de artefactos y tecnologías en un hogar occidental promedio en los últimos cien años, aunque también es incomparable con respecto a medio

siglo atrás, época en la que nació internet. Esto es lo que marca la aceleración, que dio paso a la idea de lo «exponencial» que escuchamos cotidianamente.

Estas historias de decisiones crean en conjunto un entorno complejo y de escala. Algunas tecnologías son muy poderosas, internet es un buen ejemplo, como las tecnologías de los alimentos o la inteligencia artificial. Son tecnologías que desde su propia concepción necesitan gran difusión. Por ejemplo, y con dudas, las promesas sobre los beneficios de los coches autónomos se cumplirían si la mayoría, o todos, fueran autónomos. Estas tecnologías cambiarían radicalmente nuestras relaciones sociales urbanas y toda la movilidad dependería de una infraestructura de telecomunicaciones y datos que debería cubrir todo el territorio; sin olvidar que muchos de estos datos representan nuestra identidad y nuestros movimientos.

El poder implicado en este tipo de diseños es tomado por Hans Jonas desde un punto de vista ético y por Quintanilla (2017) desde el concepto de alienación. Dado que mayor poder implica mayor responsabilidad, una nueva ética para estas tecnologías «tiene que existir porque los hombres actúan, y la ética está para ordenar las acciones y regular su poder. Tanto más «tiene que existir cuanto mayo- res sean los poderes de la acción que ella ha de regular; y el principio regulador «tiene que ser proporcionado tanto a la magnitud como al carácter de lo que ha de regular. Por tanto, las nuevas capacidades de acción requieren nuevas reglas éticas y quizás, incluso, una nueva ética.» (Jonas, 1995:19).

Otro argumento fundamental para prestar atención a esta «nueva ética» se asocia a la posibilidad de decidir sobre nuestra forma de vida, que sin dudas está influenciada por nuestro entorno tecnológico. Las llamadas «capacidades» (en rigor, *capabilities*) propuestas por Amartya Sen se orientan a «la expansión de las capacidades de las

personas para llevar el tipo de vidas que valoran y tienen razones para valorar. Estas capacidades pueden mejorarse mediante políticas públicas, pero también, por otro lado, la dirección de las políticas públicas puede verse influenciada por el uso efectivo de las capacidades participativas por parte del público. La relación bidireccional es fundamental» (Sen, 2000:18). No basta con tener derechos, sino también con la posibilidad efectiva de su realización. Con la posibilidad de que una comunidad de diferentes tradiciones y concepciones puedan estar de acuerdo para proseguir su buena vida (Nussbaum, 1997: 286).

La garantía para la expansión de derechos efectivos también es parte del terreno público, y con el antecedente de las tecnologías que ya tenemos, la preocupación sobre las tecnologías que vendrán parece genuina. Las relaciones y desvinculaciones entre los decisores y las comunidades son el centro del problema ético; y dada la escala y potencia de las tecnologías que vienen, parece necesario incorporar activamente nuevos criterios y alternativas basadas en la «responsabilidad» de Jonas (1995), o en la «honestidad» de Parselis (2018). Esto implicar pensar modos de legitimar socialmente el desarrollo de escala o de influencia pública para que no se parezca a un decreto legislativo, para no vulnerar nuestra autonomía.

6. El regreso de los *commons*

Asistimos recientemente al lanzamiento del primer Falcon 9 tripulado de la empresa SpaceX de Elon Musk con destino a la Estación Espacial Internacional. Es la primera vez que la NASA realiza un proyecto público-privado de esta naturaleza, y existe el interés de la empresa por el turismo espacial o, dicho de otro modo: la mercantilización del espacio. Es un proyecto de gran complejidad, aunque la órbita de la Estación Espacial Internacional se encuentra «cerca». Marte se encuentra a una

distancia de entre 57 y 400 millones de kilómetros de la Tierra; la Luna, a 380 mil kilómetros; y Plutón, a 5 mil millones de kilómetros, distancia que ya fue superada por la sonda Voyager 2 en 2018, aunque debe continuar su viaje durante 30.000 años para abandonar definitivamente el Sistema Solar. Recordemos que hace apenas 11.000 años tenemos evidencias del establecimiento humano en territorios fijos, evento determinante en el desarrollo de todas las civilizaciones conocidas.

La luz del Sol que llega a la Tierra proviene de la misma estrella que la luz que llega a la Luna, a Marte y a Plutón. La atmósfera que filtra esa luz y que explica buena parte de la posibilidad de que estemos vivos cubre todo el planeta. El agua dulce fue posibilitadora de toda la evolución de la vida desde su microscópico origen hace 3,5 mil millones de años y que las mutaciones genéticas han desarrollado en especies diferenciadas, y en cada una de ellas dando identidad a cada individuo. Estas escalas de tiempo son estudiadas por lo que se denomina *big history*, una línea de trabajo bastante prolífica.

¿Tiene algún sentido pensar en la apropiación de la luz, los genes, el agua o un planeta?

En la escala humana, Jonas Salk fue consultado sobre la patente que protegería su vacuna contra la polio (otra epidemia) y su respuesta fue muy clara: ¿se puede patentar el sol? Con esta pregunta, Salk puso bajo la misma categoría algo natural como el sol y una creación artificial como su vacuna, una creación científico-tecnológica. En consecuencia, su vacuna fue de dominio público, y no podría ser apropiada por privados, y tampoco por Estados. No sabemos qué régimen de propiedad tendrán las vacunas contra el COVID-19, si es que logran desarrollarse, pero sí contamos con muchos otros ejemplos que no son naturales: el conocimiento científico, las lenguas, las tradiciones, internet.

Pensar que hay cosas que no pueden tener «dueño» parece, *a priori*, extraño, dado que estamos acostumbrados a pensar en algún tipo de

propiedad, que en Occidente suelen reducirse a las figuras de propiedad pública y propiedad privada. Los bienes «sin dueño» no podrían ser nacionales, lo que implica que ningún Estado puede legislar en forma exclusiva sobre su naturaleza y preservación. En este sentido, tanto el cambio climático como internet son dos buenos ejemplos: cualquier decisión «soberana» sobre ellos implica algún deterioro del bien en términos globales. Según Lafuente, «cuando decimos que pertenece al procomún todo cuanto es de todos y de nadie al mismo tiempo, estamos pensando en un bien sacado del mercado y que, en consecuencia, no se rige por sus reglas.» (Lafuente, 2007:1).

La economía del don formaliza este tipo de bienes. Zamagni propone la «fraternidad» como eje para la gestión de *commons*: «Mientras que en relación con los bienes de la esfera privada es necesario apelar al principio del cambio de equivalentes, y para resolver el problema de los bienes públicos se puede pensar, al menos en el nivel teórico, en la aplicación del principio de redistribución, cuando se llega a la cuestión de los bienes comunes se vuelve indispensable poner en juego el principio de reciprocidad» (Zamagni, 2014:27).

Las TIC y la informática en general abrieron una dimensión nueva de los *commons*, asociada a bienes intelectuales. No hablamos, entonces, de *commons* «dados», que se encuentran en la naturaleza, sino de *commons* «construidos» socialmente. En general son desarrollados por comunidades que no mantienen propiedad ni limitaciones de acceso a ellos, como el *software* libre y los bienes que suscriben el *copyleft*.

Existen, entonces, aspectos de la naturaleza y de la cultura no apropiables por privados ni por Estados. Puede ser evidente para la luz, aunque no lo es tanto para los genes, dado que hay industrias de alimentos que patentan intervenciones genéticas, o se practica la edición genética humana a través del método CRISPR. Puede ser evidente para internet, aunque su propiedad de neutralidad se encuentra en peligro

una y otra vez. Pero si pensamos en tecnologías que pueden cambiar decididamente nuestro futuro, parece sensato que exista algún grado de gestión comunitaria. El Tratado Antártico, el Cambio Climático, los bancos para la conservación de semillas y varios esfuerzos de la ONU se orientan a esquemas de decisión multilaterales. Es una buena aproximación al problema: existen actividades y tecnologías que nos involucran de algún modo crítico y, por lo tanto, no es posible dejar sus objetivos asociados a intereses particulares.

Estos ejemplos asociados a formas de vida y comunidades hacen más compleja la discusión, porque ya no se relacionarían solamente con las grandes escalas, sino también con las capacidades de las distintas comunidades para decidir sobre su futuro. Entonces, podremos encontrar *commons* en todas las escalas, y debemos definir jurídica y técnicamente sus bordes, para poder protegerlos contra prácticas no deseadas, como la apropiación para ser utilizados como un simple recurso. Esta demarcación también está en manos del Estado, que tiene potestad de definir qué puede ser parte de intercambios privados, qué bienes son apropiables por el Estado (como el petróleo en Argentina) y qué se puede considerar común. Esta categoría de bienes implica para un Estado no solamente su demarcación, sino también su gestión, que a nivel global ha tomado la forma de gobernanza.

Si los *commons* posibilitan y son sostenidos por comunidades, la ética de las capacidades que mencionamos parece ser la más adecuada, ya que circulan bajo la lógica de la economía del don. Procurar que diversos bienes se transformen en *commons* aumentaría la disponibilidad de conocimiento y saberes de una comunidad (Benkler, 2006).

Innerarity (2020) afirma que hemos perdido de vista este tipo de bienes por torpeza colectiva, por no ver la relación entre las acciones personales y el conjunto, y observa que nuestra capacidad organizativa no resulta apta para la cantidad de cosas que compartimos. Esto

vale para los *commons*, pero también para aquello que es público. Esto deriva en la imposibilidad de evitar los efectos catastróficos de nuestras irresponsabilidades. Visibilizar la relación entre los comportamientos individuales y lo común puede no llevar a la responsabilidad, pero no visibilizarla lleva seguramente a la irresponsabilidad, como relata Hardin (1968) en la «La tragedia de los comunes».

Pensar en capacidades y en la modificación de formas de vida es pensar en algo que pertenece a una comunidad; y por ello, las tecnologías que estamos desarrollando y gestionando deben respetar el principio del cuidado de los *commons* dados y legitimar los *commons* construidos, y esto requiere de alguna mirada estatal en las sociedades organizadas.

7. El Estado, entre la complejidad y las tendencias tecnológicas

Las tecnologías digitales que durante algunos años se imaginaron como disociadas del entorno físico cada vez están más involucradas en nuestros cuerpos y relaciones territoriales. Es decir que ya no solo influyen en nuestro universo simbólico con toda su problemática específica de espionaje, filtros burbuja, censura, privacidad, etc., sino que también se embeben en electrodomésticos y controlan algorítmicamente naves lejanas, o muy cercanas, como los coches autónomos.

Lo mismo ocurre con otras tecnologías en las que se decide como si la Tierra fuera un artefacto, en palabras de Allenby. Desde hace muy poco tiempo estamos cambiando la forma de estudiar la relación entre el desarrollo humano y los sistemas de la Tierra, abandonando gradualmente el análisis lineal para dar lugar a los sistemas complejos. Esto requiere el desarrollo de nuevos modelos, y una nueva ética (Allenby, 2005).

8. Complejidad

El conjunto de tecnologías y personas conforman redes globales materiales e informacionales. Hay componentes intermedios entre una red global y los individuos, como los Estados u organizaciones. Hay un cambio de escala entre individuos, organizaciones y esta red global. En la escala de grupos e individuos, los patrones de interrelación están influenciados por los actores de la escala intermedia, pero tienen una lógica más horizontal, especialmente en el estado de la globalización actual, que acompaña el flujo de información y mercancías con el flujo de cuerpos entre regiones y países. Los cuerpos humanos son el huésped del COVID-19, que también se ha globalizado debido a esta horizontalidad del flujo humano.

Hay redes que generan sistemas complejos caracterizados por su alto grado de incertidumbre. En un sistema complejo, la comprensión de sus componentes no permite predecir el comportamiento del todo (el comportamiento resultante se denomina emergente). El «efecto mariposa» propone que una perturbación pequeña en una parte de la red puede generar eventos significativos como emergente en otras partes.

La perspectiva de la complejidad global fue cambiando al ritmo de su estudio en sus distintas etapas (mercancías, culturas, personas…) y ha creado conocimiento, modelos y teorías. Hoy nos encontramos en una etapa de aceleración, que multiplica la incertidumbre y los riesgos propios de un sistema complejo. Ian Goldin afirma que los beneficios de la globalización ocultaron la enorme interdependencia que deriva en su propia vulnerabilidad. Se trata de otro sistema complejo, caracterizado como «fenómenos generados por partes que interactúan, cuyas conexiones causales no son fácilmente discernibles, y cuyo comportamiento con el tiempo exhibe desorden y se comporta de manera

impredecible o caótica». A mayor conectividad, mayor complejidad, mayor riesgo, y menor posibilidad de toma de decisiones informadas, lo que conduce a la pérdida de responsabilidad (Goldin y Mariathasan, 2014: 326).

El análisis de los riesgos sistémicos de este tipo de estructuras tiene muchos antecedentes, como los realizados por Urlich Beck, Anthony Giddens y, en habla hispana, José Antonio López Cerezo. Desde las primeras advertencias del «riesgo manufacturado», a principios de los años 2000, la conectividad se aceleró y la fragilidad global es cada vez mayor, lo que hace perder de vista los efectos de las acciones individuales, a la vez que se introduce más incertidumbre y peligro. Es entonces cuando la lógica de la causalidad directa es cada vez más difícil de identificar. Si además de enfrentar altos niveles de incertidumbre asistimos a una dilución de responsabilidades, tiene aún más sentido el reclamo de Hans Jonas sobre la necesidad de una nueva ética.

Además de la problemática del abandono de la lógica lineal causal, se suma la dinámica del contexto: la pasividad es un modo de actuar ante la aceleración, ya que los problemas solo empeoran cuando no se hace nada, lo que nos lleva a entender que la complejidad implica directamente a la gestión (Innerarity, 2020).

9. El contenido político de las tecnologías

La relación con las tecnologías nos modifica y nos constituye en nuestras habilidades, capacidades, posibilidades y mirada del mundo. Contribuyen a la construcción de nuestras identidades. En largos tiempos biológicos, evolucionaremos en relación con los entornos que formamos. El contenido político está presente en este entorno y define parte de nuestra forma de vida. Si retomamos la diferencia entre las tecnologías que ya existen y las tecnologías que todavía no existen,

veremos que las primeras tienen el rol de decretos, pero las segundas son flexibles y podremos modificarlas. Esto depende de mecanismos que posibiliten definir (o redefinir) el problema que pretenden solucionar y sus finalidades.

Como mencionamos, el contenido político de las tecnologías no es la política tecnológica. La política tecnológica en muchos lugares mantiene una relación virtuosa (al menos desde el punto de vista económico), en tanto que Latinoamérica muestra algunos resultados en la investigación científica que tienen enormes dificultades para ser transferidos al desarrollo tecnológico y a las empresas, salvo algunos pocos casos paradigmáticos. Este trabajo no profundiza la cuestión, pero es pertinente la diferenciación entre el contenido político de las tecnologías y las estrategias nacionales o regionales orientadas al desarrollo tecnológico, que es un modo de establecer finalidades muchas veces asociadas a cuestiones geopolíticas.

En ambos casos la administración pública tiene un rol central, incluso como «creadora de valor», en la perspectiva de Mazzucato (2019). Las políticas tecnológicas en su faceta de investigación se convierten en un activo irreemplazable para un país, del mismo modo que la transferencia hacia la industria. Pero hay un camino por recorrer en cuanto a la gestión de recursos y su relación con lo que podemos considerar *commons*. ¿Es posible encontrar modos de gestión de *commons* entre países?

En el caso del contenido político de las tecnologías, la administración pública suele estar al margen de la problemática asociada al diseño tecnológico de las empresas. Cuando hablamos de tecnologías críticas por lo que hacen, por su complejidad o por su escala, y los aspectos éticos asociados ello, resulta imperativo que existan instrumentos de evaluación amplia. Cuando mencionamos las distintas desvinculaciones entre el uso y el diseño, también hablamos del Estado. Muchas

tecnologías que se implementan como herramienta en el Estado, en infraestructuras, o como productos de circulación libre en el mercado, son opacas. ¿Es posible encontrar modos de evaluación amplia de estas tecnologías?

10. Gobernanza y cooperación

Las Naciones Unidas han abordado parte de la problemática de las tecnologías digitales a través de su programa *Digital Cooperation*, intentando consensuar directivas sobre lo que puede ser aceptable en un mundo digital interdependiente. Este es un ejemplo de algunas preocupaciones que mencionamos. Desde el punto de vista del desarrollo tecnológico, el problema de las decisiones humanas es central; por lo tanto, los responsables del diseño tecnológico, tanto como los criterios de automatización de acciones a través de la inteligencia artificial, no pueden quedar fuera de un consenso global. La cohesión social y la seguridad son parte de la discusión, y precisamente ambas cosas pueden considerarse *commons*. Finalmente, el modo de esa cooperación, el mecanismo que permitiría tomar decisiones, es crucial: si se trata de valores, capacidades y bienes que podríamos considerar comunes, es necesario que su gestión sea cooperativa. Lo mismo ocurre, sin mucho éxito, con la mitigación del cambio climático.

Sin embargo, existe una tensión difícil de abordar. La tecnología puede estudiarse a través de sus trayectorias, que parecen mostrar patrones evolutivos a veces casi «autoexplicativos», lo que alimenta de argumentos a algunos deterministas tecnológicos. La potencia de estas trayectorias puede llevarnos a pensar que es muy poco lo que podemos hacer para el gobierno de la tecnología. Las miradas más optimistas podrían sintetizarse en la pregunta que se hace Kevin Kelly: ¿qué quiere la tecnología? Y se responde a sí mismo de un modo ambivalente:

«La tecnología quiere lo que queremos: la misma larga lista de méritos que anhelamos. Cuando una tecnología ha encontrado su papel ideal en el mundo, se convierte en un agente activo para aumentar las opciones, elecciones y posibilidades de los demás» (Kelly, 2010).

Esta idea parece descansar sobre el supuesto de que hay una búsqueda del bien, una especie de sustrato de buenas intenciones. Pero sabemos que hay consecuencias no deseadas y responsabilidades que se encuentran diluidas. Sabemos que enfrentamos el cambio climático, y que, salvo por la aceptación en un mercado, no tenemos instrumentos para decidir sobre las tecnologías que se están desarrollando hoy mismo y que comenzarán a formar parte de nuestro entorno vital en un futuro.

Kelly muestra esta tensión asegurando que nuestro papel como humanos es persuadir a la tecnología a lo largo de los caminos que naturalmente quiere seguir (Kelly, 2010).

Es decir, que aun asumiendo que esa «inercia» por seguir una trayectoria determinada es potente, debemos «persuadir» a la tecnología. Esta «persuasión» se diferencia de otras ideas más críticas, que van desde la condescendencia hasta la radicalización total en contra de estas trayectorias. Lo cierto es que no parece pragmáticamente posible refundar el entramado del desarrollo tecnológico. Parece más sensato intentar colocarlo dentro de la arena de la decisión política amplia y participativa, dentro de una época que *de facto* es compleja.

Allenby (2005) advierte que este sistema de gobernanza internacional se ha vuelto mucho más complejo, que la dominancia del Estado-nación se trasladó a un lugar dentro del conjunto de muchas instituciones involucradas en la gobernanza internacional, como las empresas privadas, las ONG y comunidades de diferentes tipos.

Reforzando la idea de gobernanza, Innerarity sostiene que es necesario renunciar a cualquier instancia central de ordenamiento de

las distintas lógicas que intervienen en la sociedad, porque ya no sería compatible con la complejidad. En la complejidad existe un mecanismo de autoorganización, que no permite su control. Y describe las limitaciones de las tendencias ideológicas actuales: «En este punto [autoorganización] tienen razón los liberales, pero no consideran la otra cara de la realidad, las ineficiencias de la autoregulación o los resultados indeseados de la agregación. El socialismo es más ambicioso en su intervención, pero frecuentemente menos consciente de sus límites. La política de la complejidad apunta a una combinación de ambos enfoques, en la medida en que acepta la complejidad del sistema, pero al mismo tiempo sabe que sus intervenciones tendrán una influencia en la realidad emergente de las sociedades» (Innerarity, 2020).

Si volvemos a las tecnologías ya desarrolladas, podemos considerar que muchas de ellas podrían entrar en el campo de la gobernanza. Pero buena parte de este capítulo se refiere también a cómo pensar las que vendrán, dado que cambiarán formas de vida. En ese sentido, puede pensarse en el concepto de «gobernanza intertemporal», que para Innerarity consiste en «… una cultura política y un diseño institucional que estimula la decisión motivada en el largo plazo, protege los intereses futuros, mejora los instrumentos de previsión y promueve la solidaridad intergeneracional».

Una «gobernanza anticipatoria» parece deseable en todos los campos, pero dado que nos encontramos con la tensión de la inercia de las trayectorias tecnológicas, la anticipación en las tecnologías que se están desarrollando y las que desarrollaremos es fundamental. La complejidad implica riesgo e incertidumbre, pero eso no significa que no existan esfuerzos anticipatorios. Las instituciones públicas tienen, en consecuencia, una importancia fundamental en esta anticipación, tal como también advirtió Oscar Oszlak: «Tal vez se requiera repensar totalmente los enfoques con que se enfrenta la tarea regulatoria,

imaginando formas de intervención temprana antes de que su adopción adquiera gran escala, aunque sin disuadir el cambio tecnológico» (Oszlak, 2019).

La anticipación y los estudios del futuro pueden ser una forma de regulación temprana, como también la evaluación de riesgos y la adopción inteligente del principio de incertidumbre. «Se trata de una tarea que comienza con la reflexión acerca de las implicaciones futuras de las actuales decisiones, sobre las tendencias, que requiere diferenciar las señales críticas del ruido que nos distrae, detectar los problemas latentes, identificar los riesgos y las oportunidades» (Innerarity, 2020).

Una evaluación más democrática que legitime lo aceptable y lo deseable en cuanto a tecnologías futuras (entres sus opciones) es también desarrollo de capacidades, en el sentido de Amartya Sen. Por otra parte, los esquemas de gobernanza (como los que propone Innerarity, asociados a la democracia compleja) parecen un buen marco para la gestión de tecnologías críticas por sus funciones o por su escala, y por su aporte decisivo a la complejidad de la realidad.

11. Particularidades del Estado

Es cierto que una infraestructura puede considerarse como un servicio, y que los problemas tecnológicos en estos casos no parecen ser los mismos que las tecnologías para la administración pública. Hemos visto que muchas tecnologías que son parte del espacio público funcionan como forma de orden, por lo que deben legitimarse en términos de valores e intereses de la ciudadanía. Este espacio público puede ser físico, pero también puede ser el «ciberespacio público», que debería contar con las mismas condiciones de propiedad y acceso que el espacio físico. Estas tecnologías de la información de carácter público deberían contar con los mismos mecanismos de legitimación

y procurar conciliarlas no solamente con el interés por el servicio (en la relación Estado-ciudadano), sino también con los intereses relacionados con su diseño.

Cuando hablamos del Estado, entonces, debemos enfocarnos no ya en dos actores (los que hacen y los que usan), sino también en el tercer actor «Estado» que decide sobre las tecnologías que usaremos, y sobre las tecnologías que usará para su funcionamiento. Esto implica que en la relación Estado-diseño no deben existir las barreras que desvinculan los intereses del desarrollo tecnológico con respecto a los del Estado, y el Estado debe procurar que las tecnologías que llegan a los ciudadanos también minimicen estas barreras.

Si parte de la ética asociada a tecnologías en entornos complejos se orienta a esta simetría entre actores, no parece adecuada la adopción de tecnologías «enlatadas» que sean «cajas negras» por parte del Estado. Tampoco parece adecuado que la adopción se realice a espaldas de la ciudadanía, al menos en términos culturales y representacionales. Este triángulo implica transparencia en sus tres relaciones: Estado-diseño, Estado-ciudadanos, diseño-ciudadanos.

Por otra parte, el Estado cuenta con infinidad de procedimientos relacionados con su estructura y finalidades, muchas veces apoyados en tecnologías que los pueden hacer más eficaces y eficientes; y, eventualmente, redundar en mejores servicios al ciudadano. Esto implica tecnologías ajustadas a la lógica de la administración. Pero también hay una influencia inversa: hay tecnologías que abren posibilidades y permiten cuestionar el modo de organización, como ocurre con las TIC y el flujo de información. Tal vez por ello se las identifica como una oportunidad de «modernización», idea que en su significado encierra mejoras en la administración y en los servicios al ciudadano. En el caso particular de las tecnologías de la información, los Estados se vieron obligados a tomar acciones frente a la posibilidad de que la

información pueda gestionarse de un modo más eficiente, y el Estado abierto es resultante de la tensión entre los procesos burocráticos y la posibilidad de ser observados por la ciudadanía (Oszlak y Kaufman, 2014).

No analizaremos si los procesos actuales son adecuados, pero recordaremos que esa triple relación entre Estado, ciudadanos y diseñadores requiere más condiciones que la relación entre Estado y ciudadanos; y que no puede reducirse a la idea de contratación de proveedores de plataformas de un modo estrictamente instrumental. El caso del voto electrónico, que operativamente resulta atractivo, puede ser un buen ejemplo. No se trata de la «máquina», sino del acceso público a su funcionamiento, de manera de auditar, desde el Estado y también por parte de la ciudadanía, el propio diseño de la máquina, de modo que sea posible conocer cada uno de sus procedimientos y que el proceso de sufragio cuente con todas las garantías. En los casos locales, esto ha tenido muchas dificultades.

Así como las TIC forzaron alguna reacción por parte del Estado, es de esperar que esto siga ocurriendo, dadas las trayectorias tecnológicas actuales. Como esto se produce dentro de un contexto complejo y en escalas mayores a las del alcance estatal, las instituciones de gobierno se encuentran con otra tensión, derivada de la lógica actual con respecto a las tendencias. En este punto cobra importancia la gobernanza tecnológica, como acción conjunta para influir sobre las trayectorias en beneficio del rol del Estado. Esta gobernanza implica también la voluntad por la eliminación de barreras sobre determinadas tecnologías que bajo un esquema de gobernanza pueden considerarse *commons* y que entonces no podrían ser apropiadas por un Estado particular y tampoco por privados.

El flujo de información sobre las TIC está cada vez más asociado al territorio. Ha quedado atrás la época en la que los flujos en el

ciberespacio no tenían referencias físicas. Los servicios de geolocalización, discusión sobre privacidad mediante, intervienen en la internet de las cosas, en la automatización de máquinas en el espacio público y en los conceptos de *smart cities*. Aun sin utilizar GPS, la triangulación entre antenas celulares permite crear análisis de red sobre los movimientos de las personas, insumo para tareas valiosas como la dinámica del tránsito, pero también para tareas de inteligencia. La trayectoria tecnológica de la inteligencia artificial abre cada vez más posibilidades para las bases de datos biométricos y para que un arma automatizada ejecute enemigos humanos en un conflicto.

Esta pequeñísima lista muestra que los Estados no solo tienen un rol central en la gobernanza sobre tecnologías asociadas a su administración, sino también sobre tecnologías asociadas a derechos fundamentales. Los Estados son actores principales en la anticipación de emergentes dentro de los sistemas complejos y poderosos que las tecnologías crean. Por ello, la advertencia de Jonas sobre la responsabilidad proporcional al poder, la responsabilidad intergeneracional de Innerarity, y tratar de garantizar la revinculación entre Estado, ciudadanos y diseñadores juega hoy un papel fundamental para intervenir en el sentido de las trayectorias tecnológicas.

Reflexiones finales

Marc Augé advirtió que ya no teníamos la experiencia del viajero, sino que el turismo había ocupado ese lugar con estereotipos que se transformaron en productos que establecen recorridos y estadías, convirtiendo a unos en espectadores y a otros en espectáculo. Aprender nuevamente a viajar consiste en descubrir nuevos paisajes y nuevos hombres, que pueden abrirnos el espacio de nuevos encuentros.

Esta apreciación, tomada como metáfora sobre nuestro camino hacia el futuro, implica actores involucrados, en todas las escalas, ciudadanos, Estados y esquemas de gobernanza. La administración pública es demandante de tecnologías que son diseñadas y utilizadas. No es posible que se encuentre desvinculado de la pregunta por el problema por solucionar: no debería aceptarse una rueda sin necesitarla. Pero además, debe procurar que no se produzcan desvinculaciones entre los intereses que motivan la creación de las tecnologías con respecto a los intereses en su gestión y los intereses de los usuarios. Esto implica consensos a través de esquemas de gobernanza y mecanismos de participación. Menos barreras generan tecnologías más transparentes. El interés por estudiar y gestionar la trazabilidad de contagios en una pandemia no puede generar tecnologías que lesionen derechos individuales a la privacidad que el Estado debe garantizar, además de auditar el proceso de diseño y gestión de dicha tecnología.

Los Estados son entidades que se encuentran en la escala intermedia de esta problemática, son parte de una red más compleja asociada a las trayectorias tecnológicas y a bienes naturales y culturales que no puede gestionar en forma aislada. El intento por evitar la ruina de estos bienes globales requiere de consensos, también globales.

Ninguna administración, entonces, puede, desde el punto de vista ético, desentenderse de las capacidades en determinar las formas de vida que elijan sus ciudadanos, como tampoco de los aspectos que la conectan con aquello que no puede ser apropiado por el bien de la humanidad. El Estado es una institución crítica en la modulación entre estas escalas. La nueva ética que exigen las tecnologías actuales debe ser un imperativo, o al menos una guía para esta modulación. De ese modo aseguraría tecnologías socialmente más legítimas.

Referencias bibliográficas

Allenby, B. (2005). *Reconstructing Earth: Technology and environment in the age of humans.* Washington: Island Press.

Benkler, Y. (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven and London: Yale University ress.

Broncano, F. (2008). «In media res: cultura material y artefactos». *Revista ArtefacTos*, *1*(1), 18-32.

Carr, N. (2011). *¿Qué está haciendo Internet con nuestra mente?* Madrid: Taurus.

Goldin, I., & Mariathasan, M. (2014). *The Butterly Defect. How globalization creates systemic risks, and what to do about it*. Princeton: Princeton University Press.

Hardin, G. (1968). «The tragedy of the commons. Managing the Commons», Science, v. 162 (1968), pp. 1243-1248.

Innerarity, D. (2020). *Una teoría de la democracia compleja. Gobernar en el siglo XXI*. Barcelona: Galaxia Gutenberg SL.

Jonas, H. (1995). *El principio de responsabilidad. Ensayo de una ética para la civilización tecnológica.* Barcelona: Editorial Herder.

Kelly, K. (2010). *What technology wants*. New York: Viking - Penguin Group.

Lafuente, A. (2007). «Los cuatro entornos del procomún». *Cuadernos de Crítica de La Cultura*, (77-78), 15-22.

Lash, S. (2005). «Formas tecnológicas de vida». En *Crítica de la información* (pp. 39-58). Buenos Aires, Amorrortu Editores.

Mazzucato, M. (2019). *The value of everything. Making and taking in the Global Economy*. New York: Penguin Books.

McLuhan, M., & Fiore, Q. (1967). *El medio es el masaje*. Buenos Aires: Paidós Studio.

Morozov, E. (2015). *La locura del solucionismo tecnológico*. Madrid: Katz.

Nussbaum, M. C. (1997). «Capabilities and Human Rights». *Fordham Law Review*, *66*(2), 273-300. https://doi.org/10.1017/CBO9781107415324.004

Ortega y Gasset, J. (1939). *Meditación de la técnica y otros ensayos*. Revista de Occidente, 1977.

Oszlak, O. (2019). «La gestión pública, ante los desafíos de la cuarta revolución industrial». *La Nación,* https://www.lanacion.com.ar/opinion/columnistas/la-gestion-publica-ante-los-desafios-de-la-cuarta-revolucion-industrial-nid2228330

Oszlak, O., & Kaufman, E. (2014). *Teoría y práctica del gobierno abierto: lecciones de la experiencia internacional*. IDRC - OEA. https://redinpae.org/recursos/kaufman-oszlak.pdf

Parselis, M. (2016). *Las tecnologías entrañables como marco para la evaluación tecnológica*. Salamanca: Universidad de Salamanca.

Parselis, M. (2018). *Dar sentido a la técnica: ¿pueden ser honestas las tecnologías?* Los libros de la catarata/Organización de Estados Iberoamericanos. https://www.oei.es/historico/divulgacioncientifica/?Dar-sentido-a-la-tecnica-Pueden-ser-honestas-las-tecnologias

Quintanilla, M. (2017). *Tecnologías Entrañables.* Editorial Catarata. Madrid.

Quintanilla, M. (2020). *Filosofía Ciudadana*, Editorial Trotta. Madrid.

Schwab, K. (2016). *La cuarta revolución industrial*. Barcelona: Debate.

Sen, A. (2000). *Development as Freedom*. New York: Anchor Books.

Zamagni, S. (2014). *Economía del Don. Perspectivas para Latinoamérica.* (O. Groppa & C. Hoevel, Eds.). Buenos Aires: Ciudad Nueva.

MARTÍN PARSELIS. Observador del fenómeno tecnológico desde una perspectiva interdisciplinar, con foco en la legitimación social del desarrollo tecnológico y en el cuidado del procomún, con especial interés por los fenómenos socio-técnicos asociados a las nuevas tecnologías y sus escenarios futuros, y en la filosofía de la tecnología como marco analítico para el estudio de sus aspectos éticos y políticos.

Investigador y profesor titular en carreras de ingeniería y de humanidades. Autor de *Dar sentido a la técnica* y *Tecnologías entrañables como marco para la evaluación tecnológica*, además de participar en diversos libros y artículos académicos. Experiencia en gestión privada, ámbito público y cooperación internacional.

Doctor en Estudios Sociales de la Tecnología por la Universidad de Salamanca, Magíster en Administración de Empresas por la UCA. Ingeniero electrónico por el ITBA, y con estudios en Comunicación por la UCA.

Esta publicación se inspira en un trabajo de reflexión previo, que involucró a varios de sus autores. En 2019, la Fundación Konrad Adenauer impulsó el *Foro Multisectorial sobre Cooperación Digital* junto con la Secretaría de Gobierno de Modernización de la Nación. Participaron en él representantes del sector público (miembros del Poder Ejecutivo Nacional y representantes del Programa País Digital), del sector privado, del tercer sector y de la academia. Las acciones preparatorias del Foro se desarrollaron en mesas de debate sectoriales. Tanto en estas mesas como en el Foro mismo, se discutieron las propuestas del alto panel del secretario general de la ONU sobre cooperación digital, con el objetivo de aportar una mirada argentina en el marco del *Internet Governance Forum* desarrollado ese año en Berlín.

Debido al rico intercambio de ideas y debate, y ante la escasez de publicaciones sobre esta temática, nos pareció útil poder contribuir al debate público con un trabajo académico que tuviera en cuenta la perspectiva regional.

El libro recorre los principales ejes que deben considerarse en un proceso de transformación digital de la administración pública, tanto en el nivel del *front-desk* como en el del *back office*. Sacarán especial provecho de su lectura los funcionarios públicos de distintas dependencias y niveles, así como legisladores, formadores de opinión y estudiantes de disciplinas directa o indirectamente vinculadas con la administración pública.

KONRAD ADENAUER STIFTUNG