

**Título:** ¿Quién “manda” en el espacio virtual en México? Soberanía, Democracia y Gobernanza Digital.

*Pablo Calderón Martínez, Ph. d.*

*Erick Gonzalo Palomares Rodríguez, Ph. d.*

## **1. Introducción**

El estudio de la soberanía domina la disciplina de la ciencia política y todas sus variables. La democracia, por ejemplo, no puede existir sin el “pleno” ejercicio de la soberanía. A pesar de la creciente tendencia a separar la democracia – definida como un conjunto de instituciones que determinan quién gobierna – y la buena gobernanza – entendida como "el ejercicio de la autoridad política y autoridad administrativa en todos los niveles para gestionar los asuntos de un país" (PNUD, 2012: 3) – no se puede negar que la soberanía es un *sine qua non* de la democracia. La democracia en la forma de “igualdad política en el lado del *input* debe complementarse con imparcialidad en el lado de los resultados del sistema político (*output*), es decir, en el ejercicio de la autoridad pública” (Rothstein y Teorell, 2008: 170). A pesar de la tendencia a enfatizar la promoción de "características deseables" como "participación, rendición de cuentas, inclusión y transparencia" en la formación de una "gobernanza democrática" (Carothers y de Gramont, 2013: 90-91), no cabe duda que una democracia sólida requiere de buenas políticas públicas y de la capacidad para implementarlas. La distinción entre el proceso democrático como *input* y la buena gobernanza como *output*, por lo tanto, parece irrelevante. La idea de que lo que define una democracia es la igualdad en el acceso al poder, y que la imparcialidad en la ejecución/aplicación de políticas es lo que define el buen gobierno (Rothstein y Teorell, 2008: 170), aunque interesante, simplemente busca distanciar a la democracia de la soberanía.

El caso de México en particular – con sus distintivas deficiencias democráticas – y en términos generales el intento por “gobernar” el espacio digital, nos demuestra que una democracia plena requiere no solamente de buenas y bien intencionadas políticas públicas, sino también de una capacidad para ejercer dichas políticas. En el caso de la gobernanza digital, México se encuentra en una situación incierta en ambos sentidos. Por una parte, México corre el riesgo de decantarse a

favor del modelo de gobernanza digital soberanista con tintes iliberales y antidemocráticos (al menos en su interpretación actual). Al mismo tiempo, México, como muchos otros países en la región, tiene que lidiar con el relativo atraso tecnológico que le pudiera impedir ejercer cualquier modelo de gobernanza digital que eventualmente elija.

## **2. Efectividad y legitimidad en el marco teórico de la gobernanza digital**

Distinta de la racionalidad política que exige la legitimidad del soberano, la efectividad de las relaciones causales (es decir, de las políticas públicas) exige datos y conocimientos probados. Debido a esto podemos observar que las causas de la ineffectividad gubernamental se deben no solo a la “ilegitimidad”, sino también a la “impotencia”, la “incompetencia”, la “ineficiencia” y la “insuficiencia” del gobierno (Aguilar, 2022:74-75). Es necesario entonces preguntarnos cómo la creciente relevancia del espacio digital afecta el problema de la ineffectividad gubernamental. En otras palabras, ¿cómo podemos implementar las decisiones, y garantizar la efectividad de estas, en un contexto donde se carecen de las herramientas, así como de la experiencia que garantice la relación causal del gobierno digital?

La problematización de la gobernanza digital pasa en primer lugar por su “facticidad”: ¿cómo garantizar que “efectivamente” sucedan las previsiones con las que se elaboran las políticas públicas orientadas a la gobernanza digital? Aparecen por tanto las necesidades no sólo en términos del marco legal que regulen las acciones, sino también en los instrumentos estatales que garanticen su eficacia: un aparato estatal, con conocimientos probados, y por ende con funcionarios capacitados en todos los niveles, para la implementación y observancia de ese marco legal. No hay soberanía democrática del espacio digital sin instrumentos que pueden ser utilizados para ello.

Lo que es más, si bien la esfera digital no produce los bienes públicos tradicionales que se consagran en las constituciones estatales (derechos básicos), sí se ha ido convirtiendo en un canal y herramienta para la satisfacción de muchos de ellos. La “incertidumbre” sobre la efectividad de las posibles acciones directivas impulsadas para conseguir los objetivos sociales es un desafío que se agrava ante la novedad del fenómeno digital, caracterizado por un lenguaje y unas plataformas que se alejan del interés público y de dominio estatal, sobre todo por la ausencia de información

probada, datos necesarios, así como buenas prácticas que guíen la toma de decisiones. Todo esto resulta acuciante en contextos como el latinoamericano, con su trayectoria estatal caracterizada por una conformación del aparato burocrático que responde a clientelismo, favoritismos y compromisos ideológicos y electorales, que no obedecen a una profesionalización.

Los debates sobre la legitimidad de la soberanía estatal en el espacio virtual están atravesados por cuestiones de fondo que determinan los diferentes argumentos: definiciones sobre la idea de comunidad política o la obediencia a la autoridad estatal conforman el trasfondo de las diferentes posturas que se pueden asumir. Preguntarse, por ejemplo, si hablamos de una comunidad digital, qué sería, en términos de comunidad política, lo que los miembros de esa comunidad se supone que comparten en común y qué preocupaciones o lealtades se espera que tengan los unos con los otros (Shorten, 2016).

De la mano con la pregunta sobre la comunidad política está la cuestión misma sobre el Estado y su ejercicio de autoridad. La pregunta esencial sobre la existencia del estado y su justificación se renueva ante la pregunta sobre su posible intervención soberana en el espacio virtual, y exige revisitar la larga tradición filosófico-política sobre la definición del Estado, desde Locke señalando que el objeto central del poder político es el derecho a hacer leyes y castigar a quienes desobedezcan, a Weber que agrega el monopolio legítimo de la violencia, pasando por la tradición anarquista y marxista que ven en el Estado instrumentos de opresión y control de parte de la clase dominante (Rosen & Wolff, 2012).

Si las características esenciales del ejercicio de la autoridad de los Estados consisten en reclamar de forma exclusiva esa autoridad sobre sus ciudadanos, sin limitaciones en el contenido, distinguiendo la autoridad del simple ejercicio coercitivo de poder al contar con la conformidad de los ciudadanos sin que necesariamente se esté de acuerdo con el juicio y las razones detrás de sus decisiones (Bird, 2006: 155-157), esto se debería traducir necesariamente en un intento de ejercer la autoridad del Estado sobre el espacio virtual que plantea dudas no solo en su posibilidad práctica, que puede ser entendida como la eficacia de la gobernanza planteada antes, sino, y sobre todo, en términos de su legitimidad y aceptación: ¿cómo se percibe por parte de los ciudadanos esa legitimidad de las decisiones estatales sobre el espacio virtual?

Todos los estados modernos, en términos puramente weberianos, necesitan cumplir con ciertas características como la monopolización de la violencia (que sólo puede ocurrir después de que se haya ganado cierta legitimidad), la integridad territorial, un mínimo de administración central eficiente y nuevos canales de lealtad individual que le permiten influir de manera sustancial en aspectos de la vida individual y social (Spruyt, 2007: 212-214). Esta última característica podría describirse como el aspecto “afectivo” o “integrador de masas” del estado moderno, que contrasta marcadamente con la dimensión puramente “represiva” de los regímenes políticos anteriores. Por tanto, el estado moderno es único porque “siempre opera a través de medios extra-burocráticos y extralegales” (Görg y Hirsch, 1998: 585). En términos generales, esta capacidad de acción sólo se logra mediante la formación de una identidad nacional, basada principalmente en sentimientos afectivos. El estado soberano, por lo tanto, no puede existir sin los tres elementos: instituciones, territorio y una dimensión ideológica/afectiva que lo sostenga. Son estas dos últimas dimensiones las que el espacio digital está transformando de manera acelerada.

### **3. México, democracia y ciberespacio**

Eventos recientes alrededor del mundo parecen respaldar el argumento de que “ni siquiera la democracia en las ‘sociedades desarrolladas’ es inevitable o irreversible” (Merkel, 1998: 42), y definitivamente México no es la excepción. No es ningún secreto que la democracia en México ha sufrido de deficiencias marcadas que nos impiden definir a México como una democracia consolidada o plena. Aunque es relativamente prematuro, se ha dicho que el dominio político y electoral del que disfruta MORENA en México, aunado a los intentos del presidente López Obrador por transformar unilateralmente las instituciones electorales, reflejan un paso hacia el autoritarismo competitivo de antaño en vez de un paso hacia la democracia plena (Incháustegui y Olaiz, 2020; Agren, 2022). Independientemente de la influencia positiva o negativa del *obradorismo* en la calidad de la democracia en México, es difícil argumentar que la “transición votada” ha logrado algo más que un éxito parcial. Aunque a partir de 1997 las elecciones en México son libres, justas y supervisadas por un árbitro relativamente independiente, las instituciones establecidas por el Partido Revolucionario Institucional (PRI) nunca fueron sustancialmente transformadas. Además de estas carencias institucionales, podríamos ir más allá

e inclusive hablar de una democracia fallida considerando los escandalosos niveles de corrupción e impunidad, un sistema judicial colapsado, una crisis de seguridad interminable, la persistencia de los cacicazgos y el regreso de la vieja guardia política a la presidencia. Finalmente, también hay preocupaciones claras de que en México existe una fuerte correlación –y que no es tan fácil de explicar – entre su pasado autoritario y sus perspectivas democráticas (Middlebrook, 2004: 28). Ya sea por la falta de una reforma estatal integral, un sistema judicial defectuoso, el legado de un gobierno autoritario o el dominio casi absoluto de Morena y el obradorismo en el panorama político/electoral, es difícil no estar de acuerdo con la idea de que la democracia mexicana es imperfecta.

El desarrollo de una estrategia para lidiar con la creciente influencia del espacio digital, por lo tanto, podría haber llegado en un mejor momento para México. En términos generales, México enfrenta retos similares a otros países de América Latina. El aumento acelerado de conectividad, la creciente dependencia de los sistemas de información del país en tecnología extranjera, su condición de economía de nivel medio profundamente incierta en las dinámicas comerciales globales, y la corrupción generalizada que impregna todos los niveles de la vida pública son todas características que definen a muchos de los países latinoamericanos (Rodríguez-Hernández y Velásquez, 2021: 486). De manera más específica, la actual guerra contra el narcotráfico en México presenta riesgos particulares para la seguridad y las instituciones democráticas debido a la presencia trascendental del crimen organizado. Aunque parece evidente, hay que destacar que la gobernanza digital, a pesar de las características distintivas del ciberespacio, forma parte de la amplia gama de políticas públicas que son la responsabilidad del estado. Por lo tanto, la calidad de la democracia, libertades civiles, el estado de derecho y la participación popular dan forma a la estrategia digital de cualquier país. Un país como México, con alta concentración de poder en el ejecutivo, débiles mecanismos horizontales de control y vigilancia entre las distintas ramas del gobierno (sobre todo aquellas que tienen que ver con el aparato de seguridad e inteligencia) (Solar, 2023: 43), desarrollará por ende una estrategia de gobernanza digital acorde a dichas características. Al mismo tiempo, el fuerte programa anti-corrupción de López Obrador, combinado con la fuerte crisis de seguridad, se ha traducido en un creciente involucramiento y relevancia de las fuerzas armadas. No sorprende, por lo tanto, que México parece decantarse en

algunos sentidos por una estrategia militarizada basada en la idea de la “soberanía digital” para lidiar con los retos presentados por la expansión del espacio digital.

A pesar, por ejemplo, de que la Estrategia Nacional De Ciberseguridad (ENC) concebida en el 2017 por el Gobierno de Enrique Peña Nieto reconocía a la cuestión económica como su componente central (OEA, 2022: 64), lo cierto es que la ENC no ha llevado a la creación de nuevos programas (como la creación del Subcomité de Ciberseguridad dentro de la Secretaría de Gobernación que la ENC proponía), ni se han creado los mecanismos adecuados para ejercer la estrategia (Lopátegui Torres, 2020: 103). Sigue siendo difícil identificar un presupuesto concreto asignado al tema de la ciberseguridad por parte del Gobierno Federal y la ENC parece haber sido abandonada por completo por el gobierno actual. Aunque existe una iniciativa de Ley Federal de Ciberseguridad que propone crear la Agencia Nacional de Ciberseguridad que dependería directamente del Ejecutivo, la realidad es que la ciberseguridad en México sigue siendo la prerrogativa de la Guardia Nacional (Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica) y la Policía Federal (Unidad de Ciberseguridad), militarizando así *de facto* la soberanía del estado sobre el espacio digital.

Además de la Policía Federal y la Guardia Nacional, la Secretaría de Comunicaciones y Transportes se encarga de publicar la Guía de Ciberseguridad a nivel nacional y existen Policías Cibernéticas en cada estado del país. Estas fuerzas policiacas estatales son las encargadas de atender reportes y denuncias, desarrollar alertas cibernéticas y ofrecer atención ciudadana sobre el uso seguro y responsable de las herramientas tecnológicas. En gran medida, por lo tanto, la interacción cotidiana que se pueda dar entre ciudadano y el “gobierno” en el espacio digital en México, no es entre el ciudadano y el Gobierno Federal sino entre el ciudadano y los gobiernos estatales. Esto puede beneficiar la administración pública pero no deja de tener posibles consecuencias negativas. En México, como en otros países de la región, la descentralización ha creado “soberanías locales” que pueden entrar en conflicto con la soberanía nacional. La coordinación entre los diferentes niveles administrativos forma parte de este modo de las necesidades de gobernanza digital, y por ende de la resolución de posibles conflictos políticos, exacerbados por los intereses electorales y la manipulación emocional de las campañas electorales.

Ejemplo emblemático de la descentralización de la gobernanza digital por su vanguardia es el marco legal promovido por la Ciudad de México, quienes, han promovido, por un lado, leyes para reconocer el espacio digital como un espacio legítimo de interlocución entre los ciudadanos y la autoridad soberana estatal, reemplazando las leyes locales de Gobierno Electrónico y Firma Electrónica, por una la Ley de Ciudadanía Digital de la CDMX, así como una Ley de Operación e Innovación Digital para la Ciudad de México, que crea la Agencia Digital de Innovación Pública de la Ciudad de México para diseñar y coordinar las políticas públicas encargadas de la gestión de datos, la gobernanza tecnológica y la conectividad, así como la implementación de soluciones tecnológicas laboratorios de innovación. En este caso, el hecho de que ambos gobiernos, estatal y nacional, sean del mismo partido, MORENA, ha favorecido a la coordinación y coherencia entre leyes y soberanías a los diferentes niveles de gobierno.

#### **4. Modelos de gobernanza digital y la posición de México**

El desarrollo económico de Latinoamérica requiere de una infraestructura digital estable y de la implementación de políticas públicas en el ámbito que permitan desatar el potencial económico del comercio digital en la región. Aún más importante, sin embargo, es considerar el impacto político del espacio digital en las democracias emergentes de la región. Nos queda claro que “un internet seguro es crucial si las democracias emergentes quieren construir instituciones sólidas y abordar problemas graves de desarrollo” (Solar, 2020: 401). El incremento en interconectividad en América Latina no ha sido acompañado por un proceso institucional que permita la regulación del nuevo espacio digital. Lo que es peor aún es que en un momento crucial en el desarrollo de la región, en el que un internet libre y seguro parece fundamental para desarrollar industrias clave en el comercio digital (actividades principalmente desarrolladas por intereses y actores privados), las tendencias soberanas de los estados latinoamericanos, incitadas por consideraciones tradicionales de seguridad nacional, parecen dominar el debate. Aunque México no sufre una historia similar a la de otros países de la región en cuanto a injerencia de las fuerzas armadas en la vida pública del país, sería un error minimizar la tendencia a militarizar el espacio digital en México. Las fuerzas armadas mexicanas, como las de muchos de los otros países en la región, tienden a respetar el control civil sobre las mismas, pero eso no significa que sea una institución que pueda o deba de

interactuar con actores civiles en el desarrollo de estructuras claves para las nuevas democracias y economías digitales.

Existe, por lo tanto, una aparente paradoja en la manera en la que México busca “gobernar” el espacio digital. Por un lado, la tendencia hacia la securitización, militarización y la implementación de la soberanía en el espacio digital parece irreversible. Por otra parte, hablar de soberanía virtual es en sí mismo una paradoja tanto ideológica como práctica. Desde una perspectiva ideológica, el internet emergió como un espacio libertario donde la responsabilidad individual y la autorregulación eran suficientes para garantizar el funcionamiento del nuevo espacio creado. Aunque la relación entre soberanía y espacio digital era una pregunta que se discutía ya en círculos académicos, se daba casi por hecho que la soberanía tal y como la conocemos no podría existir en el espacio virtual; “El ciberespacio se propuso como un espacio radical con su propia soberanía emergente, más allá de la autoridad o control de los estados” (Zeng, Stevens y Chen, 2017: 434). Este modelo libertario de la década de 1990 se desvaneció con el crecimiento del Internet (Flonk, Jachtenfuchs y Obendiek, 2020: 382), dando paso al modelo liberal liderado por Estados Unidos. Este modelo defiende un ethos "libertario y de libre mercado" con una regulación gubernamental mínima, elogiando la disrupción como necesaria para la innovación y el crecimiento económico (Schneider, 2020: 8). Los proponentes de dicho modelo argumentan que la soberanía digital contradice el orden global actual basado en estándares comunes y el libre flujo de información, considerando que los intentos de soberanía son inútiles (Mueller, 2020: 780).

A pesar del dominio liberal en el debate sobre la gobernanza digital, los recientes desafíos de las visiones soberanistas, defendidas en particular por China y sus aliados, están ganando terreno. El discurso de Xi Jinping en 2015 marcó la formalización de la postura de China sobre la "soberanía digital", aspirando a una gobernanza del ciberespacio alineada con los principios de las relaciones internacionales (Zeng, Stevens y Chen, 2017: 434). Sin embargo, esta aspiración, que se ha desarrollado a lo largo de una década, carece de un modelo ideológico coherente o de una propuesta técnica viable. La noción de replicar los modelos de soberanía estatal en el espacio digital con marcos regulatorios sólidos, leyes de localización de datos y parámetros fronterizos tradicionales existe en teoría, pero significa una desviación significativa de la configuración actual



del Internet. Si bien la idea de espacios digitales regionales o múltiples "internets" es teóricamente posible, no se alinea con las tendencias actuales (Mueller, 2020: 788) ni con las intenciones soberanistas.

Las ideologías soberanistas, a pesar de las cuestiones teóricas o técnicas, no dejan de ser relevantes. Incluso Estados Unidos, el defensor inquebrantable del modelo liberal, pretende frenar el poder del *Big Tech*; La Comisión Federal de Comercio, por ejemplo, busca dividir Facebook, se encuentra investigando a Amazon y ha presentado demandas antimonopolio contra Google, mientras que el Departamento de Justicia también está investigando la tienda de aplicaciones de Apple (Chander y Sun, 2022: 285-286). Si bien el espacio digital parece no tener fronteras, existe geográficamente, especialmente en el ámbito de la seguridad. Los ciberataques a gran escala se dirigen a ubicaciones específicas; "Las redes penetradas, los datos robados y la importancia de los datos pertenecen a entidades dentro del territorio soberano de un Estado" (Arcos, 2021: 13). El desarrollo de reglas para el espacio digital puede parecer poco probable, pero Joseph Nye (2022) señala que la falta de un marco claro no garantiza la anarquía perpetua. Las normas internacionales (como cualquier otro tipo de normativa "social"), tardan décadas en ser desarrolladas, internalizadas, aceptadas y eventualmente respetadas por los distintos actores. El lento desarrollo de las normas internacionales no implica necesariamente la expansión de la soberanía estatal en el ciberespacio. Sin embargo, señala la necesidad del modelo liberal de evolucionar, reconociendo que el espacio digital plantea un nuevo desafío de seguridad, particularmente para las economías emergentes de América Latina.

A pesar de la aparente necesidad de lidiar con este nuevo panorama, alrededor del 50% de las naciones del mundo siguen sin tener una estrategia de ciberseguridad formal. Esto no significa que la mayoría de los países del mundo, entre ellos la gran mayoría de los estados latinoamericanos, no han comenzado a tomar en serio los retos que representa el espacio digital. Pero tampoco han desarrollado todavía estrategias claras y coherentes o respuestas institucionalizadas a estos riesgos (Romaniuk y Manjikian, 2021: 6). México es uno de estos países. Por una parte, la política exterior mexicana ha sido caracterizada, desde los gobiernos del PRI, por un pragmatismo fundamentado en el apoyo al multilateralismo. A partir de la firma de múltiples tratados comerciales (iniciando con tratado de libre comercio con los Estados Unidos y Canadá en 1994), la economía mexicana

ha atravesado un periodo de rápida internacionalización. Su estrategia y posición en cuanto al comercio digital, la lucha contra el cibercrimen y las tecnologías financieras (Fintech) están en gran medida ligadas a esta internacionalización y, por lo tanto, apegadas al multilateralismo (*multistakeholderism*) preferido por el modelo liberal (Rodríguez-Hernández y Velásquez, 2021: 489-490). El capítulo 19 sobre Comercio Digital en la última versión del tratado comercial en América del Norte, el T-Mec, consolida la posición de México dentro del modelo liberal en muchos sentidos, pero paradójicamente también parece atrapar a México dentro de un marco regulatorio específico que puede contribuir a la creciente división del espacio digital (Ciuriak y Fay, 2021: 61). Debido a este aparente alineamiento, la normativa legal en materia digital en México parece adecuada y suficientemente actualizada en lo que atañe a estos aspectos (Fintech, cibercrimen, PI y comercio digital), aunque cabe recalcar que más allá de las leyes formales “el panorama de la ciberseguridad en México está caracterizado por desafíos, vacíos y contradicciones críticas” (Rodríguez-Hernández y Velásquez, 2021: 488).

Por eso es importante recalcar que el modelo promovido tan fuertemente por Rusia y China principalmente (se ha proclamado al Gran *Firewall* como la principal exportación china para el mundo (Gravett, 2020: 129)) no deja de ser relevante para México. Podemos encontrar versiones de este modelo en países importantes del sur global tanto democráticos como autoritarios incluyendo a Sudáfrica, Brasil e Irán. A pesar de ser un país esencialmente democrático, en el espacio virtual el estado sigue siendo, paradójicamente, la principal amenaza para la mayoría de los ciudadanos en México. Existe suficiente evidencia que indica que órganos cercanos al estado mexicano (incluyendo agencias de seguridad) han utilizado herramientas de vigilancia digital para espiar, acosar e inclusive localizar con el objetivo de asesinar a un buen número de activistas, periodistas y miembros del gobierno (Rodríguez-Hernández y Velásquez, 2021: 487).

Las tendencias autoritarias dentro del estado mexicano no dejan de ver a un modelo promovido por China - el país que ha tenido más éxito explotando el espacio digital con fines autoritarios (Miller, 2022: 244) - como una propuesta atractiva. México, recordemos, apenas inicia a desarrollar su agenda digital en un contexto de fragilidad democrática. López Obrador, como ya se mencionó, ha hecho de la lucha contra la corrupción su principal prioridad, y su gobierno ha mostrado interés y conocimiento de las amenazas que la transformación digital representa para su

democracia (Schneider, 2020: 15-16). Pero al mismo tiempo, el desarrollo de una estrategia digital coherente y concreta basada en un entendimiento liberal de un internet libre y abierto sigue pendiente; las pocas leyes existentes en México, por ejemplo, en la materia de protección de información, datos y privacidad enfrentan riesgos importantes. En particular existe una falta de conocimiento a nivel de los ciudadanos, una cultura débil en lo referente a protección de información privada y las autoridades tienden a darle poca relevancia a violaciones de leyes sobre manejo de datos (*idem*: 17). México, por lo tanto, se encuentra entre ambos modelos. A nivel internacional México parece adoptar una posición multilateral regida por sus intereses comerciales, pero a nivel doméstico el estado mexicano no puede ignorar las ventajas que el modelo soberanista ofrece a regímenes no completamente democráticos.

### **5. Una teoría de gobernanza digital en México: indicadores y desafíos.**

Para poder pensar en la gobernanza digital en México, considerando los desafíos ya planteados respecto a la eficacia y la legitimidad democrática, particularmente la dimensión ideológico-afectiva de esta última, sugerimos una serie de indicadores a partir de una reinterpretación crítica de las cuatro unidades causales propuestas por Aguilar Villanueva (2022) para una teoría del gobierno. La abstracción de la teoría se vuelve de suma utilidad, al permitir el análisis empírico del contexto mexicano, dejando espacio para una variación que se adapte a las particularidades de la gobernanza del espacio digital. Las cuatro unidades causales que deberían integrar una teoría de la gobernanza digital en México, parten de tres supuestos sobre la gobernanza en México (Aguilar, 2022:137-138): a) la gobernanza es una “acción normada”, es decir, que se delimita por un ordenamiento jurídico-legal, leyes que establecen el marco de acción; b) la gobernanza es una “acción racional”, es decir, que sus acciones están sustentadas en un sistema de conocimientos que se sustentan en datos y relaciones causales probadas, que permiten elegir opciones de acción costo-eficientes, que considera los costos de oportunidad y respeta el equilibrio fiscal con alta probabilidad de llegar al cumplimiento de los objetivos planteados; c) la gobernanza es una “acción política”, que mediante la interlocución y concertación de los actores sociales se consigue definir y alcanzar los objetivos de valor público. Para estas tres acciones se establecen cuatro unidades causales que serán analizadas de manera individual.

*A) Variables causales del ordenamiento normativo del estado:*

La primera unidad causal por considerar en la gobernanza digital en México es el marco regulatorio. Determinar las variables y analizar el contexto del marco normativo mexicano es el primer paso para pensar una gobernanza digital en México. Y lo primero que salta a la vista son los “frecuentes defectos de calidad regulatoria de las leyes” en México (Aguilar, 2022:158). Si bien es cierto que el poder judicial en México es de los pocos aparatos del estado que cuenta con un proceso de evaluación y selección para ser parte de él, aun así la asignación de jueces y de los altos cargos del poder judicial está atravesada por la negociación partidista. La designación de los jueces de la suprema corte, y del resto de instancias, se ve frecuentemente politizada y obedece a lealtades político-partidistas.

La actual reforma del poder judicial está ligada a las dinámicas dentro de los poderes legislativo y ejecutivo, ambos controlados por MORENA. La relación y vínculo entre el partido en el ejecutivo y la mayoría parlamentaria ofrece ventajas y desventajas. Por el lado de las ventajas, permite que se puedan llevar adelante reformas de gran calado, que empujen la reforma de leyes, en este caso de gobernanza digital si así se quisiera, en sintonía con la implementación de las decisiones. Sin embargo, la ausencia de contrapesos entre los diferentes poderes del aparato estatal impide contraposiciones de argumentos y posibles mejoras que consideren distintos puntos de vista, particularmente aquellos representados por los partidos políticos en la oposición. Es necesario, por lo tanto, prestar particular atención (a falta de contrapesos importantes) a los posibles conflictos de interés que puedan devenir de la protección de derechos de los ciudadanos, frente al legítimo interés de enriquecimiento y búsqueda de la ganancia de las entidades privadas. Particularmente cuando estas últimas sean actores privados internacionales, cuya obediencia al estado debe reflejar una correlación de fuerzas que permita el equilibrio entre derechos ciudadanos e intereses privados.

Junto a las decisiones del poder ejecutivo, se requiere también de un marco legal que permita que organismos públicos y consejos de deliberación público-privados, puedan ir resolviendo la gobernanza digital según vayan apareciendo los problemas y la propia administración vaya aprendiendo sobre los desafíos y necesidades de gestión. Al ser la gobernanza digital una nueva

esfera de acción estatal quedan abiertas las puertas para la experimentación en cuanto a la forma que deba tener la administración pública en este ámbito. El principal desafío de la gobernanza digital en México, sin embargo, radica en la posible contradicción y conflicto entre los derechos y libertades ciudadanas, por un lado, y el interés privado de búsqueda de la ganancia de las empresas privadas, muchas de ellas transnacionales sobre las cuales se tiene menor influencia respecto a la soberanía estatal. La coacción del estado encuentra límites respecto a la jurisdicción internacional, sumado a la voluntad popular de aceptar la renuncia a ciertos derechos y libertades (como el derecho a la privacidad, o aceptar que se usen sus datos personales con fines comerciales) a cambio de poder hacer uso de las redes, plataformas y servicios digitales.

Actualmente, el estado mexicano, como muchos otros, se encuentra en una situación de desventaja frente a las *big tech* (GAFAM y otras). A diferencia de la Unión Europea con su modelo de RGPD, por ejemplo, México simplemente no tiene la importancia como mercado para poder imponer sus condiciones a las grandes empresas tecnológicas en cuanto a manejo de datos. Pero eso no significa que no pueda desarrollar un marco legal que le provea de herramientas y parámetros de acción dentro del respeto a las libertades individuales y empresariales. México podría introducir cláusulas de ubicación de mercado como las incluye el RGPD; GAFAM y otras grandes empresas tecnológicas ya operan bajo dichos principios debido a la regulación europea y al alto costo de realizar sus operaciones utilizando marcos regulatorios distintos. México podría así beneficiarse aún más del “efecto Bruselas” (Schneider, 2020: 13). Paradójicamente, el régimen regulatorio regional de Norteamérica en el que opera México parece el principal impedimento para dichas reformas. Las nuevas regulaciones sobre localización de datos introducidas en el capítulo sobre comercio digital del T-MEC prohíben el uso de instalaciones locales de almacenamiento de datos como condición para hacer negocios en el país (Ciuriak y Fay, 2020: 55). De nuevo, México parece estar atrapado entre distintos modelos de gobernanza digital.

#### *b) Variables causales del Sistema de Conocimiento de la Sociedad*

El sistema de conocimiento del espacio digital en México tiene serias limitaciones que afectan la posibilidad de la gobernanza digital. Existen al menos tres condiciones limitantes que podemos encontrar en el sistema de conocimiento mexicano, las cuales son determinantes respecto a las

posibilidad para la gobernanza digital: 1) la temporalidad de la causalidad, que se refiere al desconocimiento del tiempo requerido para el desarrollo del capital intelectual necesario para la gobernanza digital, así como los distintos acontecimientos que van determinando la agenda política sin que puedan ser determinados con anterioridad; 2) la racionalidad limitada, que conlleva una ineludible incertidumbre sobre las probabilidades de que se pueda llevar a cabo la decisión, y sobre todo las consecuencias y efectos socialmente deseados de dicha decisión, debido a la naturaleza imprevisible de los fenómenos sociales y el imprevisible comportamiento humano; 3) la pluralidad valorativa de los sujetos sociales, que conlleva que “los efectos producidos, aunque son hechos objetivamente evidentes, son también valoraciones subjetivas de los sujetos sociales que pueden concluir calificándolos como malos, regulares o satisfactorios.” (Aguilar, 2022: 165)

El primer indicador por considerar respecto a la sociedad del conocimiento necesaria para la gobernanza digital se refiere al conocimiento disponible para el análisis, valoración, contraste y toma de decisiones. Sin información, no se puede decidir. De ahí que el primer esfuerzo al que debe orientar su energía el poder estatal se refiere a la captación de información en sus posibles diferentes formatos. El gobierno mexicano debe comenzar con una política de investigación y obtención de datos, ya que sin ella es imposible dar los siguientes pasos. Esto necesariamente contribuiría al desarrollo de un marco regulatorio y de capacidades tecnológicas que le permitan al estado mexicano utilizar los datos e información generada por sus ciudadanos, empresas y organizaciones. Como se dijo con antelación, el derecho y la capacidad de analizar la información generada (lo que Shoshana Zuboff (2019) definió como el “*behavioral surplus*”) es el recurso más importante de la futura economía digital basada en algoritmos predictivos.

Aun cuando se cuente con información y bases de datos, así como con herramientas y dispositivos tecnológicos que permitan la gestión de la información, la gobernanza digital exige personal cualificado en instituciones públicas y privadas que cuenten con el capital intelectual suficiente para el manejo, creación, gestión y mejoramiento de las herramientas digitales. En el proceso de las políticas públicas, tras la definición del problema y la formulación de la política, queda la difícil tarea de la implementación que no puede ser valorada sin que le acompañe necesariamente un proceso de evaluación de sus resultados: la forma en que se expresa la implementación, sus aciertos y errores, se la da necesariamente el proceso de evaluación que la acompaña. Con lo cual es

indispensable incluir en las variables necesarias para la gobernanza digital, una sistematización del proceso de evaluación de las medidas, sean legales, administrativas o coercitivas, sobre la esfera digital.

*c) Variables causales de las Relaciones Políticas*

La actuación del estado es necesaria, pero no suficiente para atender los problemas del espacio digital. La gobernanza digital requiere la participación de los distintos actores interesados e involucrados en el espacio digital, y para ello es indispensable el diálogo, acuerdo y negociación para que los intereses, visiones y valores en conflicto encuentren un consenso que permita que la política pública sea eficiente y legítima. Nos referimos entonces a una versión del *multi-stakeholderism* “de abajo hacia arriba” suscrito y promovido por los Estados Unidos y otros países occidentales que propone que el sector privado y la sociedad civil deben de ser actores clave en la gobernanza del internet (Chander y Sun, 2022: 295). La gobernanza digital requiere del involucramiento de dichos actores no solamente para garantizar su eficacia, sino para ganar su aprobación; la legitimidad de la actuación estatal depende de la forma en que se relacione, incluya y discuta con los distintos actores sociales.

Es indispensable, a nuestro entender, que se co-gubierne no solamente con un constante diálogo sino también con el estado abierto a la participación ciudadana. La larga transición hacia la democracia en México, aunque acentúa los problemas ya mencionados, al menos ha ido creando condiciones institucionales para garantizar dicha participación. Consejos consultivos, organismos públicos descentralizados, foros de diálogo puntuales o permanentes son pasos decisivos que se han acompañado de una consolidación de los actores privados y de la sociedad civil en México. Consideramos el involucramiento de dichos organismos de vital importancia para el desarrollo de la gobernanza digital en México sobre todo por la oportunidad que representa para los sectores más marginados de la población. El denominado “*last billion*” describe al sector de la población mundial que aún no tiene acceso al espacio digital (Arora, 2019), y parte de esta población se encuentra en las partes rurales más pobres de México. El involucramiento de dichos sectores marginalizados en el desarrollo de la estrategia digital en México les permitiría desarrollar su propia versión de “soberanía de red local” sobre el aprendizaje, uso y operación de los nuevos

sistemas de manera que apoyen las culturas y ontologías locales (Parks, Srinivasan y Cerna Aragón, 2022: 2141). Tomemos como ejemplo al proyecto de Telecomunicaciones Indígenas Comunitarias en el estado de Oaxaca, que ha construido la red celular comunitaria más grande del mundo con casi 20 torres de telefonía celular establecidas y manejadas por la misma comunidad local (ídem: 2143). Este proyecto ha sido en su mayoría apoyado por el estado mexicano a pesar de promover una versión autónoma (es decir independiente de intervención directa gubernamental o de los grandes conglomerados de la telecomunicación en México) en lo que se refiere al acceso al espacio digital. Vemos esto como un paso positivo en la creación de una estrategia de gobernanza digital inclusiva en México.

Para que esto se pueda dar es necesario reconocer a los actores civiles como legítimos participantes, pero también es necesario poder reconocer al gobierno como el interlocutor válido y legítimo. En la democracia se requiere de una representación reconocida en lo interno y en lo externo. Por un lado un reconocimiento a la representación en lo interno del colectivo o grupo social que se dice representado, es decir que exista la sensación por parte de los representados de que el representante efectivamente les representa. Y en lo externo, es decir que aquellos interlocutores que tratan con el representante reconozca que efectivamente representa a aquellos que dice representar. Este doble reconocimiento a la representación, tanto interna como externa, es indispensable no solo para el gobierno, sino también para el resto de actores sociales, lo cual hace de esto el gran problema de la democracia y la gobernanza digital: “El *problema* crítico de las relaciones políticas de la democracia es el de *la representatividad política* del agente gubernamental y también, cada vez más, la representatividad de los ciudadanos que son aceptados por el gobierno como interlocutores y socios en su decisión.” (Aguilar, 2022: 168)

*d) Variables causales de la decisión del agente gubernamental.*

En la teoría sobre la gobernanza digital, la decisión “del gobernante” es la unidad central, entendido “no solo como la persona que ocupa legítimamente la posición de autoridad de la sociedad, sino como el dirigente de la agencia directiva de la sociedad, que llamamos “Gobierno”, y que está conformada por el conjunto de las organizaciones administrativas y coactivas especializadas a través de las cuales gobierna a la sociedad.” (ídem: 169)



La decisión “, sea personal u organizacional, está compuesta por dos juicios que concluyen en dos elecciones: el *juicio de valor* que el decisor hace de ciertas situaciones y hechos de su vida y que por su valía los elige como el fin o el objetivo de su acción, y el *juicio de hecho* que hace de las opciones de acción y elige la que puede realizar el objetivo con los menores costos. El juicio de valor se sustenta en el sistema personal o social de valores (ético, jurídico, afectivo) del sujeto decisor y el juicio de hecho en su sistema personal o social de conocimientos.” (ídem, 170)

Es la variable sobre el juicio de valor, en la que el sistema de creencias efectivo-ideológicas afecta, no solo en la percepción de los ciudadanos que hemos discutido párrafos antes en relación con la legitimidad, sino también, y de especial importancia, en la toma de decisión del gobernante, quien decide no únicamente en base al sistema de conocimiento causalmente probado con el que cuenta para valorar la mejor decisión, sino a partir de sus emociones y afectos, de sus valores y creencias, que poco (o nada) tiene que ver con un análisis causal, técnico y racional sobre la mejor decisión de interés público.

Al ser la decisión del gobernante la que aglutina las otras tres unidades causales, debemos entender que las variables que conforman la decisión sobre la gobernanza digital, y que dan un sentido de coherencia a la teoría propuesta, consiste en la revisión de cada una de las unidades (1. ordenamiento normativo del Estado, 2. Sistema de Conocimiento, y 3. Relaciones Políticas), para con ello ser capaces de (4) tomar las decisiones de gobernanza y (5) comunicarlas a la ciudadanía para conseguir la legitimidad de la decisión soberana en gobernanza.

## **Conclusiones**

Como hemos podido observar, México ha hecho realizados avances en relación al marco legal que regule, y legitime, su intervención soberana en el espacio digital. Sin embargo, tal y como sugerimos en nuestra teorización sobre gobernanza digital, el marco legal es solo una de las unidades causales de la gobernanza democrática. Y si bien hay esfuerzos por crear organismos que gestionen la sociedad del conocimiento digital, como la Agencia Nacional de Ciberseguridad, las comisiones parlamentarias, o la Agencia Digital de Innovación Pública de la Ciudad de México,

aún queda mucho por hacer en relación a la gestión eficaz de los datos, el gran desafío sigue siendo en México la unidad causal de las relaciones políticas. El actual gobierno mexicano ha ejercido el poder a través de un autoritarismo jerárquico basado en la voz y el carisma de el presidente, que es así mismo líder absoluto del partido político que él mismo creó, MORENA; y que además controla al poder legislativo y tiene mayoría en los tribunales supremos del poder judicial; y esto parece que seguirá siendo así si, a fecha en que se escribe este texto, se cumplen las expectativas de que sea la candidata de MORENA y ex jefa de la ciudad de México, Claudia Sheinbaum, la próxima presidenta de México y continuadora, como ella misma dice, del modelo y programa política, lo que ellos llaman “la Cuarta Transformación” del país. La polarización que genera esta forma de gobierno, con la exacerbación de los sentimientos de rechazo basado en la manipulación de argumentos, pidiendo militancia frente al opositor más que una comprensión crítica de sus ideas, conlleva la implementación de un autoritarismo digital basado en el apoyo emocional y solidario de sus votantes, a quienes las razones para apoyar al gobierno no son suficientes: por encima de ello está el compromiso moral y político de apoyar una versión, frente a opositores que nunca tienen la razón.

## Referencias:

1. Agren, D. (2022). Mexico’s Congress approves López Obrador’s cuts to electoral authority, *Financial Times*, 14/12/2022. <https://www.ft.com/content/50688532-94d0-4eaf-8227-2c37a230e649>
2. Aguayo Quezada, S. (2010). *La Vuelta en U: Guía para Entender y Reactivar la Democracia Estancada*. Ciudad de México: Taurus.
3. Aguilar Villanueva, L. F. (2022) *Acerca del Gobierno. Propuesta de teoría*. Ciudad de México: Tirant Lo Blanch. El Colegio de Jalisco.
4. Arcos, R. (2021), Securing the Kingdom’s Cyberspace: Cybersecurity and cyber intelligence in Spain, en S. N. Romaniuk y M. Manjikian (eds). *Routledge companion to global-cyber security strategy* (11-25). Londres: Routledge.
5. Arora, P. (2019). *The next billion users: Digital life beyond the west*. Cambridge, Massachusetts: Harvard University Press.

6. Bird, C. (2006). *An introduction to political philosophy*. Cambridge: Cambridge University Press.
7. Carothers, T. and de Gramont, D. (2013). *Development Aid Confronts Politics: the Almost Revolution*. Washington, D.C.: Carnegie Endowment for International Peace.
8. Chander, A., & Sun, H. (2022). Sovereignty 2.0. *Vanderbilt Journal of Transnational Law*, 55(2), 283-324.  
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/vantl55&div=12&id=&page=>
0. Ciuriak, D., & Fay, R. (2021). The USMCA and Mexico's Prospects under the New North American Trade Regime, en Aliza Chelminsky, Bernadette G. Vega Sánchez and Jorge O. Armijo de la Garza (eds). *Implementing the USMCA: A Test for North America*. Ciudad de México: Senado de la República, 45-66.
1. Estrategia Nacional de Ciberseguridad del Gobierno de México (2017). [https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria\\_y\\_Recomendaciones\\_ENCS.pdf](https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf)
0. Flonk, D., Jachtenfuchs, M., y Obendiek, A. S. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists?. *Global Constitutionalism*, 9 (2), 364-386.  
<https://www.cambridge.org/core/services/aop-cambridge-core/content/view/E1035680DF6CAE90CD45A1EEFC1F97/S2045381720000167a.pdf/authority-conflicts-in-internet-governance-liberals-vs-sovereigntists.pdf>
0. Görg. C. y Hirsch, J. (1998). "Is International Democracy Possible?," *Review of International Political Economy*, 5 (4), 585-615.
0. Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, 20(1), 125-146.  
<http://www.scielo.org.za/pdf/ahrlj/v20n1/06.pdf>
0. Hendrik S. (2007) "War, Trade and State Formation". C. Boix and S. C. Stokes (Eds.), *The Oxford Handbook of Comparative Politics* (211-235). Oxford, England: Oxford University Press.
1. Incháustegui, S. y Olaiz, J. (2020) ;El presidente AMLO y la Constitución: cuando la regresión se disfraza de transformación', *Nexos*, 18/8/2020.  
<https://eljuegodelacorte.nexos.com.mx/el-presidente-amlo-y-la-constitucion-cuando-la-regresion-se-disfraza-de-transformacion/>

0. Torres, M. A. L. (2020). Towards a Cybersecurity Zone in North America: Exploring the Creation of a Regional Cybersecurity Complex Under the USMCA. *Stosunki Międzynarodowe*, 56(1), 91-113.
1. Merkel, W. (1998). 'The Consolidation of Post-autocratic democracies: A Multi-level Model'. *Democratization*, 5 (3), 33-67.
0. Merino, M. (2003). *La Transición Votada: Crítica a la Interpretación del Cambio Político en México*. Ciudad de México: Fondo de Cultura Económica.
0. Middlebrook, K. J. 2004. 'Mexico's Democratic Transitions: Dynamics and Prospects', en K.J. Middlebrook (ed.), *Dilemmas of Political Change in Mexico*. London: Institute of Latin American Studies.
0. Miller, C. (2022). *Chip War: the fight for the world's most critical technology*, Londres: Simon and Schuster.
0. Mueller, M. L. (2020). Against Sovereignty in Cyberspace, *International Studies Review*, 22, 779-801.
0. Nye, JS. (2022). The end of cyber-anarchy? How to build a new digital order, *Foreign Affairs*, Enero-Febrero, <https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy>
1. Organización de Estados Americanos (2022), *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions*. <https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=667&lang=1>
0. Parks, L. Srinivasan, R. y Cerna Aragon, D. (2022). Digital empowerment for whom? An analysis of 'Network sovereignty' in low-income, rural communities in Mexico and Tanzania, *Information, Communication & Society*, 25 (14), 2140-2161, <https://doi.org/10.1080/1369118X.2021.1928264>
0. PNUD – Programa de las Naciones Unidas para el Desarrollo (2012), 'UNESCO (2012) Governance and Development'. *Thematic Think Piece, UN System Task Force on the Post-2015 UN Development Agenda*.  
[http://www.un.org/millenniumgoals/pdf/Think%20Pieces/7\\_governance.pdf](http://www.un.org/millenniumgoals/pdf/Think%20Pieces/7_governance.pdf)
0. .

0. Rodríguez-Hernández, S.M. y Velásquez, N. (2021) Mexico and Cybersecurity: Policies, challenges, and concerns. En S. N. Romaniuk y M. Manjikian (eds). *Routledge companion to global-cyber security strategy* (484-490). Londres: Routledge.
0. S. N. Romaniuk, S.N. y Manjikian, M. (eds) (2021), *Routledge companion to global-cyber security strategy*, Londres: Routledge
0. Rosen, M. y Wolff, J. 2012. *Political Thought*. Oxford: Oxford University Press.
0. Rothstein, B. y Teorell, J. (2008). 'What is Quality of Government? A Theory of Impartial Government Institutions'. *Governance*, 21 (2), 165-190.
0. Schneider, I. (2020). Democratic governance of digital platforms and Artificial Intelligence? Exploring governance models in China, the US, the EU and Mexico', *The eJournal of eDemocracy and Open Government*, 12 (1), 1-24.
0. Shorten, Andrew (2016) *Contemporary political theory*. UK: Palgrave Macmillan.
0. Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, 2 (3), 392-401.
0. Solar, C. (2023). *Cybersecurity governance in Latin America*. Albany: SUNY University Press.
0. Zeng, J., Stevens, T., y Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "internet sovereignty", *Politics & Policy*, 45(3), 432-464. <https://onlinelibrary.wiley.com/doi/abs/10.1111/polp.12202>
0. Zuboff, S. (2019) *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. Nueva York: Public Affairs.