Soberanía digital en el siglo XXI: consideraciones brasileñas a partir del nuevo concepto de ciberespacio

Luiz Fernando Horta
Postdoctorado, University of Denver (DU), Denver, Colorado, Estados Unidos.
Profesor, Universidad de Brasília (UnB), Brasília, Brasil.
http://lattes.cnpq.br/0589727185579085
moonbladers@gmail.com

Andre Ricardo Nogueira
Doctorado en Ciencia Política, Universidade de São Paulo (USP), São Paulo, Brasil.
Professor, Universidade Federal do Espírito Santo (UFES), Vitória, Espírito Santo, Brasil.
http://lattes.cnpq.br/0589727185579085
andrericardonogueira@gmail.com

Enviado el: 30/08/2023. Aprobado el: 04/02/2025. Publicado en: dd/mm/yyyy.

RESUMEN

Las transformaciones digitales son características propias del siglo XXI. La velocidad de los cambios que provocan las nuevas tecnologías acaba dejando atrás la capacidad de transformación del propio Estado. Crear leyes, pensar en sistemas de protección de la democracia, los ciudadanos y los bienes públicos es un proceso más lento que las inversiones en ciencia y tecnología de diversas empresas. El resultado es un intento de respuesta rápida por parte del Estado que ha sido globalmente insuficiente tanto para garantizar los derechos como para contener los procesos de explotación. Una de las alternativas más utilizadas para reducir la diferencia entre las transformaciones y los espacios de control del Estado ha sido la analogía entre lo material y lo digital. Así, toda la legislación que durante siglos se ha ido perfeccionando para contener los abusos de los agentes económicos sobre el tejido social se convierte del mundo material al mundo digital. Sin embargo, esta conversión ha demostrado ser errónea e insuficiente. El artículo analiza los efectos de la analogía digital del concepto de “soberanía” y compara las propuestas estadounidenses y brasileñas en algunas áreas clave del desarrollo de la legislación sobre el mundo digital. La conclusión es que Brasil no solo está atrasado en el desarrollo de estas tecnologías, sino también en la forma en que el Estado intenta afirmar los derechos de sus ciudadanos y proteger los bienes públicos. En el fondo, lo digital es más complejo de lo que sugiere la analogía con lo material.

Palabras clave: soberanía digital; ciberespacio; transformaciones digitales; inteligencia artificial; control estatal.

LA IDEA DE SOBERANÍA

La soberanía es un concepto fundamental para la contemporaneidad. Es una condición esencial para la existencia de un país el hecho de que este tenga “soberanía”. El término proviene del latín “superanus” y se refiere a aquel que tiene el poder supremo. Ejercer “soberanía” sobre un territorio es definir su rumbo “en última instancia”. El concepto

de soberanía ha sido objeto de ataques desde finales del siglo XX. La geopolítica, con la aparición de diversos actores internacionales, la consolidación de instituciones internacionales y la cristalización de una serie de derechos humanos, ha hecho que el término "soberanía" sea, como mínimo, poroso. En esencia, se ha convertido en algo relativo a las capacidades reales de ejercicio de los poderes de un Estado. En este texto, abordaré el significado de la soberanía digital y cómo se relaciona con el concepto de espacio digital en el siglo XXI. Jean Bodin (2009) define la soberanía como "*[…] the right to impose laws generally on all subjects regardless of their consent*" (Bodin, 2009, p. 33)[1]. Reconoce además que la soberanía no se confunde únicamente con las "leyes", en la medida en que el francés aún pensaba a partir de las claves del siglo XVII para interpretar el mundo. Según Bodin, los hombres están sometidos en primer lugar a la "ley de Dios" y es de ella de donde emana toda la idea de soberanía.

En este sentido, Bodin afirma que la soberanía humana no es absoluta, sino que tiene su origen en la "verdadera" religión, capaz de interpretar la voluntad de Dios.

> If we insist however that absolute power means exemption from all law whatsoever, there is no prince in the world who can be regarded as sovereign, since all the princess of the earth are subject to the laws of God and of nature, and even to certain human laws common to all nations (Bodin, 2009, p. 27-28).

Mientras que para Bodino la soberanía es algo que emana de lo divino hacia el soberano, es Hobbes quien la establece como humana y circunscrita a un territorio. Un territorio en el que, según el autor, opera un contrato social que otorga a un poder central la posibilidad de regular el comportamiento humano. En "Leviatán", Hobbes define la soberanía como "absoluta"[2] y indivisa. Debe ser plena para poder superar el estado de naturaleza, y solo estará limitada por las fronteras del territorio al que está vinculada.

Kant, en "La paz perpetua", sigue la línea de flexibilización del concepto. Si con Bodin es plena y divina, y con Hobbes es fruto de un contrato cuya consecución no depende de la voluntad de los contratantes en todo momento (funcionando como un pacto tácito), con Kant la soberanía dependía fundamentalmente de la racionalidad de los ciudadanos que comprendían la voluntad de cooperación para la organización de un Estado. Los límites de la idea de soberanía en Kant ya no se encuentran solo en la delimitación geográfica (frontera), sino también en el respeto a los derechos y en la promoción de la autonomía de la moral individual. El sentido de soberanía ya no funcionaba como un pacto tácito, sino como una

1 Traducción: "[…] el derecho a imponer leyes de manera general a todos los súbditos, independientemente de su consentimiento" (Bodin, 2009, p. 33, Traducción editorial).

2 Na argumentação de Hobbes, já que não faz sentido pensar em soberania submetida a algum outro poder que lhe é entendido como superior. O poder divino, que fazia parte da conceituação de Bodin, deixa de existir. Hobbes muda a natureza e a fonte da soberania de Bodin. Ao entendê-la como humana, a fonte da soberania deveria vir do povo que buscava proteção e segurança.

"For by art is created that great Leviathan called a Commonwealth, or State (in Latin, *Civitas*), which is but an artificial man, though of greater stature and strength than the natural, for whose protection and defence it was intended; and in which the sovereignty is an artificial soul, as giving life and motion to the whole body; the magistrates and other officers of judicature and execution, artificial joints; reward and punishment […]" (Hobbes, 1651, p. 7).

Traducción: "Porque por el arte se crea ese gran Leviatán llamado Commonwealth, o Estado (en latín, Civitas), que no es más que un hombre artificial, aunque de mayor estatura y fuerza que el natural, para cuya protección y defensa fue concebido; y en el que la soberanía es un alma artificial, que da vida y movimiento a todo el cuerpo; los magistrados y otros funcionarios de la judicatura y la ejecución, articulaciones artificiales; la recompensa y el castigo […]" (Hobbes, 1651, p. 7, traducción editorial).

acción conjunta condicional, que obedecía tanto a la racionalidad de los sujetos como a sus proyectos morales, y sería tanto más atractiva para los pactantes cuanto más demostrara respeto por las limitaciones impuestas por la cognición de cada individuo.

El camino que recorre el concepto de soberanía, desde el siglo XVI hasta hoy, refleja una doble adecuación. En primer lugar, la soberanía pasa de ser una característica divina interpretada por un individuo (el soberano) a formar parte de la institucionalidad del Estado. Está a disposición del individuo solo por la conexión que este tiene con el Estado, y no como forma divina o tácita originaria. La formación de estos Estados modernos, en términos de Anderson (1995), acaba impersonalizando la noción de soberanía que, hacia el siglo XVIII, ya estaba completamente sometida al concepto de Estado. La soberanía ya no era ejercida por alguien, sino de forma institucional, estaba sumergida en las capacidades y necesidades de la propia idea de Estado.

Por otro lado, la idea de soberanía tuvo que adaptarse a la relación económico-productiva de la contemporaneidad. Si entre los siglos XVI y XVIII la soberanía estaba restringida por las fronteras del Estado que la ejercía, el capitalismo de los siglos XIX y XX construyó una noción de soberanía que se desprende del espacio físico ocupado por los Estados, circunscrita a sus fronteras físicas. Los bienes, el capital, las personas, entre otros recursos económicos, llevan un signo distintivo de su origen que señala su sumisión a una autoridad estatal primordial, independientemente del territorio en el que se encuentren eventualmente estos recursos. La noción de “propiedad privada” trasciende el sentido de soberanía y, si bien no se puede afirmar que la soberanía sea siempre plena sobre las propiedades privadas, tampoco se puede asumir que la propiedad privada esté libre de disputas de soberanía.

De aquí surgen leyes, principios, normas y dispositivos jurídicos, consensuados o no, que buscan resolver los conflictos entre la soberanía y la propiedad privada. La soberanía deja de estar restringida a las fronteras físicas de un Estado determinado y se reconoce como parte integral de un poder difuso sobre las cosas en el mundo. El capital, por ejemplo, adquiere el derecho a la “libre circulación” y deja de estar subordinado a su ubicación original. Las mercancías adquieren derecho a la protección de su integridad material y también de su privacidad.

En el siglo XX, el término soberanía (y su aplicabilidad práctica) se vuelve complejo, ya que ya no existe una soberanía plena o absoluta. Por otro lado, si es compartida, según Bodin y Hobbes, parece que no hay soberanía posible sin alguna contradicción lógica.

Para resolver tales contradicciones, el Derecho suele separar la soberanía en áreas de ejercicio. Establece la soberanía sobre algo como el conjunto de normas, costumbres y acciones políticas que emanan de un Estado que tiene cuatro ámbitos de acción: (1) administrar Justicia, (2) proteger las fronteras (territorio, cuerpo o valor), (3) organizar la producción económica (reglas, condiciones y prohibiciones), y (4) recaudar impuestos (de formación, de transacción o de tránsito).

Actualmente, un Estado se considera soberano si tiene la capacidad legal (soberanía de iure) y la posibilidad efectiva (soberanía de facto) de llevar a cabo estas cuatro tareas sobre un espacio físico, capital, mercancía o persona en cuestión. La soberanía, por lo tanto, implica el ejercicio monopolístico de las decisiones finales sobre estas cuatro áreas político-económicas, y se admite su existencia parcial, en relación con el tiempo o el espacio[3].

De un significado restringido al territorio físico (soberanía en Bodin y Hobbes), el término ha adquirido la flexibilidad necesaria para satisfacer los intereses del capitalismo contemporáneo. De la noción encerrada en el referente físico (Estado y fronteras), el significado se desplaza hacia una soberanía de origen, determinada por la propiedad en el momento de la creación de la mercancía, del capital o del nacimiento del individuo (como acto formativo del pacto social), sujeta a los intereses de un Estado[4].

> Now, the contemporary crisis of the concept of sovereignty relies precisely on the progressive dissolution of its seemingly pacific relationship with borders. As a matter of fact, such a crisis is determined by factors such as the globalization of the flows of goods and information; it is actively produced by the mobility rights achieved by men and women, and yet contrasted, filtered, slowed down or accelerated by both formal and informal devices of global governance (Chignola, 2021, p. 2)[5].

La soberanía digital en el siglo XXI

El siglo XXI se caracteriza por el surgimiento de un espacio no físico en el que los intereses humanos, estatales y del capital operan a velocidades y valores cada vez mayores

3 Estas referencias surgen de la lectura de la obra de Carl Schmidt. Schmidt asume que la soberanía está indiscutiblemente vinculada a la noción de "frontera" y que, en la práctica, el concepto es relevante. "[...] ao interesse público, ou ao interesse de Estado, à segurança pública e ordem" (Schmidt, 2005, p. 5, tradução nossa).
Original: "[...] the public interest or interest of the state, public safety and order, le salut public, and so on" (Schmidt, 2005, p. 5).
Traducción: "[...] el interés público o el interés del Estado, la seguridad y el orden públicos, la seguridad pública, etc" (Schmidt, 2005, p. 5, traducción editorial).
"[...] ou ao governo controlado pelo espírito do comercialismo[...]" (Schmidt, 2005, p. 10, tradução nossa).
Original: "[...] a self-governing body controlled by the spirit of commercialism [...]" (Schmidt, 2005, p. 10).
Traducción: "[...] un organismo autónomo controlado por el espíritu del comercialismo [...]" (Schmidt, 2005, p. 10).

4 Parte de la naturaleza problemática del debate sobre la soberanía en el siglo XXI surge de las diferencias de significado entre los términos "dominium" e "imperium". Mientras que el primero implica posesión y se organiza con base en los sentidos del mundo material, el segundo establece autoridad y está mucho más relacionado con las condiciones del mundo inmaterial.
Original: "In the years preceding its Hobbesian theoretical definition, then, the concept of sovereignty appears to be deeply influenced by global perspectives, tensions and problems. The Empire and the State constantly mirror each other on a juridical threshold that represents the trigger of the modern conceptual device. This happens precisely through a continuous exchange between the logic of 'imperium' and the logic of 'dominium' that resignifies legal practices and lexicons as well as the categories and exempla taken from ancient historiography" (Chignola, 2021, p. 9-10).
Traducción: "En los años previos a su definición teórica hobbesiana, el concepto de soberanía parece estar profundamente influenciado por perspectivas, tensiones y problemas globales. El Imperio y el Estado se reflejan constantemente el uno al otro en un umbral jurídico que representa el detonante del dispositivo conceptual moderno. Esto ocurre precisamente a través de un intercambio continuo entre la lógica del "imperium" y la lógica del "dominium", que resignifica las prácticas y los léxicos jurídicos, así como las categorías y los exempla tomados de la historiografía antigua" (Chignola, 2021, p. 9-10, traducción editorial).

5 Traducción: "Ahora bien, la crisis contemporánea del concepto de soberanía se basa precisamente en la disolución progresiva de su relación aparentemente pacífica con las fronteras. De hecho, dicha crisis está determinada por factores como la globalización de los flujos de mercancías e información; es producida activamente por los derechos de movilidad conseguidos por hombres y mujeres, y sin embargo contrastada, filtrada, ralentizada o acelerada por dispositivos tanto formales como informales de gobernanza global (Chignola, 2021, p. 2, traducción editorial).

(Bratton, 2016). El mundo digital surge como una paradoja: es un espacio inmaterial constituido por no-materialidades (información, nociones, ideas, significados), codificado en forma binaria en algún lugar, y que modifica sustancialmente toda la materialidad del planeta.

> Convinced by the demise of the Cold War and the magic of a new technology, people accepted the view that history as we once knew it was ending and that, along with the end of politics as we once knew it, there would be an end to the laws propagated by that most dismal of sciences, economics. Constraints once imposed by scarcities of resources, labor, and capital would end, or at least loosen significantly, and a new economics of cyberspace (a "network economics") would make it easier for societies to grow and, especially, to grow rich (Mosco, 2004, p. 16)[6].

El mismo camino de acomodación epistemológica que siguió el concepto de soberanía (de la noción rígida de espacio a la noción más sutil de tiempo y propiedad) con el objetivo de ser utilizado como condición definitoria de un Estado, puede percibirse cuando se comprende la trayectoria histórica del concepto de "espacio digital" (ciberespacio[7]).

El término "digital" se refiere al mundo construido en lenguaje de máquina, donde la información se creaba, manipulaba, controlaba o modificaba alterando tan solo dos dígitos (0 y 1, en el sistema binario, utilizado como base de la programación). Inicialmente incomprensible para todos, el mundo digital adquirió significado para la mayoría de la población a través de una analogía con el espacio físico.

Así, de la misma manera que existía un espacio físico en el que vivíamos e interactuábamos (controlado por los sentidos del tacto, el olfato, el oído, etc.), el mundo digital se percibía como un "espacio" inmaterial que existía a partir de un código o referencia digital[8]. Se estableció una percepción inicial de que el ciberespacio sólo existía gracias a un conjunto específico de información que requería una conexión al dispositivo físico (servidor de almacenamiento).

Esta analogía ha cumplido un doble propósito desde 1960. Por un lado, ha permitido comprender qué es este "mundo digital", de tal manera que los seres humanos, que se dejan llevar por sus experiencias sensoriales y las consideran determinantes de la realidad, puedan comprenderlo[9], pudieron comprender (construir, reflexionar, debatir y comunicar) el mundo digital mediante analogías con sus referencias y experiencias físicas. Por otro lado,

---

6 Traducción: "Convencidos por el fin de la Guerra Fría y la magia de una nueva tecnología, la gente aceptó la idea de que la historia tal y como la conocíamos estaba llegando a su fin y que, junto con el fin de la política tal y como la conocíamos, también llegaría el fin de las leyes propagadas por la más sombría de las ciencias, la economía. Las restricciones que antes imponían la escasez de recursos, mano de obra y capital desaparecerían, o al menos se relajarían significativamente, y una nueva economía del ciberespacio (una "economía de red") facilitaría el crecimiento de las sociedades y, sobre todo, su enriquecimiento" (Mosco, 2004, p. 16, traducción editorial).

7 El primer uso de la palabra "ciberespacio" aparece en la novela de William Gibson de 1984
Traducción: "Neuromancer". "Los japoneses ya habían olvidado más neurocirugía de la que los chinos jamás habían aprendido. Las clínicas clandestinas de Chiba eran de vanguardia, escuelas enteras de conocimientos técnicos que se superaban mes a mes, y aun así no lograron reparar el daño que había sufrido en aquel hotel de Memphis. Un año allí y aún soñaba con el ciberespacio, con la esperanza muriendo un poco cada noche. Todo el speed que tomó, todas las vueltas que dio y las esquinas de Night City por las que pasó, y aún así veía la matriz en sus sueños, brillantes rejillas de lógica desplegándose sobre ese vacío sin color [...]" (Gibson, 1984, p. 15, traducción editorial).

8 He decidido no usar la dicotomía entre el mundo digital y el mundo real porque entiendo que lo digital también es real. A lo largo del artículo, se usará la dicotomía entre el mundo físico y el mundo digital.

9 Es cierto que la humanidad siempre se ha enfrentado a un mundo "ideal" que operaba principalmente al margen de la materialidad. Sin embargo, la primacía de la materialidad sobre la filosofía a partir del siglo XIX relegó lo inmaterial a un espacio menor del que ya había ocupado en la vida de las personas en siglos anteriores.

definir lo digital como un “espacio físico no material” permitió adaptar a esta nueva realidad toda la reflexión históricamente construida sobre política, legislación y derechos (creados para controlar los espacios materiales). Entender lo digital como un “espacio” (territorial) permitió adaptar las antiguas funciones del Estado al nuevo dominio no material que estaba emergiendo.

En este sentido, el pensamiento liberal ha construido significados respecto al mundo digital, basados en la noción de soberanía. Si un Estado solo es soberano si puede ejercer las cuatro acciones (mencionadas anteriormente en este texto) sobre el territorio, entonces la soberanía digital, tomada de la analogía con el espacio físico, afirma que ser soberano en el mundo digital significa poder (1) penalizar, imputar culpabilidad o determinar la inocencia de los sujetos que operan en el mundo digital, (2) crear, modificar e imponer reglas de acceso, (3) determinar límites y condiciones para la creación y/o distribución del valor económico generado por el espacio digital, y (4) recaudar impuestos para la administración de este nuevo espacio. Obviamente, las mismas instituciones históricas que se impusieron funcionalmente en el espacio material del Estado fueron también las primeras en reivindicar legitimidad para establecer el mismo tipo de relación de dominación con el espacio digital.

El Estado se arrogó el derecho de control sobre este “nuevo mundo”[10], como consecuencia necesaria de la existencia histórica previa de sus derechos y poderes, construidos y organizados para operar en el mundo material. Lo digital, por lo tanto, se consideraba un reflejo del mundo material, y las instituciones y normas ya existentes en este debían aplicarse a este nuevo espacio por analogía.

Así, se produjo una adaptación del conjunto de derechos y deberes existentes en el mundo material al espacio digital, siguiendo, en términos generales, la misma analogía original que explicaba lo digital como un “espacio físico no material”. La percepción liberal arraigada en el pensamiento del siglo XX (liberalismo arraigado) tomó el control del mundo digital basándose en las nociones de privacidad, libertad y generación de valor económico. Esta analogía, que si bien tuvo el mérito histórico de permitir una comprensión funcional del espacio digital (al menos hasta la década de 1980), también provocó una especie de encarcelamiento en la comprensión del ciberespacio y capturó sus potencialidades y especificidades.

En otras palabras, pensar en el espacio digital como una analogía del espacio físico implica transponer las categorías sociohistóricas con las que el Estado controla el espacio físico al control del mundo digital. Y esta operación es más compleja y menos efectiva de lo que el sentido común acepta.

Así, en la interpretación actual, un espacio digital debe estar anclado al espacio geográfico (territorio) para que las herramientas de control del Estado puedan operar con

10 Si bien históricamente es posible afirmar que el Estado es el resultado de disputas políticas entre diversas formas de organización social que se han intentado a lo largo del tiempo, este proceso aún se encuentra en desarrollo en el mundo digital. Los Estados aún no han logrado dominar ni controlar el ámbito digital, y generalmente solo lo logran mediante la correlación entre el castigo y el control sobre quienes supuestamente se benefician económicamente de él. El mundo digital no puede controlarse excepto amenazando con castigos a ciertos individuos (sus posesiones o ganancias) en el mundo material.

una efectividad mínima. El derecho a “ir y venir”, consagrado desde el siglo XVIII como un derecho humano, fue, por analogía, la base de la idea de “libertad” en el mundo digital. El derecho a la privacidad y la inviolabilidad del cuerpo humano experimentaron el mismo movimiento analógico para convertirse en “privacidad digital”, y las nociones de propiedad capitalista (material o intelectual) fueron centrales en los controles fiscales e impositivos establecidos sobre el mundo digital durante las décadas de 1980, 1990 y 2000. No es que hayamos creado un nuevo conjunto normativo adecuado para el mundo físico no material (digital). Se produjo una transición por analogía con los entendimientos previos (sociales, políticos y económicos) y la puesta en práctica de las regulaciones (leyes) establecidas históricamente para el mundo material. Y esto con una dosis de autoritarismo por parte de las naciones que primero pudieron establecer marcos de control y gobernanza sobre el mundo digital (EE. UU. y los países europeos).

La visión liberal del Estado, sus funciones, herramientas y obligaciones fue, en cierto modo, una reducción cognitiva para comprender el mundo digital. Mediante esta analogía imprecisa, los derechos y garantías de los ciudadanos en el mundo físico se transpusieron al espacio digital con poca o ninguna adaptación a la verdadera esencia del nuevo espacio digital. El derecho a la privacidad, por ejemplo, que se configuró a partir del siglo XVIII como una protección del individuo contra los abusos del Estado, se convirtió, en la analogía del mundo digital, en una protección únicamente para los “datos” de quienes operan en espacios digitales. La analogía enfatiza la reducción del individuo a datos para su protección contra el autoritarismo del Estado. Los datos se protegen imaginando (por analogía) que el individuo está siendo protegido.

Sin embargo, esta relación termina generando más problemas de comprensión que soluciones a las cuestiones contemporáneas. No entraré aquí en las distinciones legales entre “secreto” y “confidencialidad”[11], por ejemplo, lo que ya sería un punto a tener en cuenta al tratar con el mundo digital, pero, de forma más sencilla, es posible preguntar: ¿qué exactamente debemos proteger en el ciberespacio?

La respuesta a esta pregunta, hasta ahora, también se obtiene volviendo a la analogía que ayuda a comprender el mundo digital. Los datos que se pretende proteger son aquellos que permiten localizar, identificar o distinguir al usuario en el mundo físico. Por lo tanto, nos referimos a las direcciones de entrada de red (*IP – Internet Protocol*) que se asocian, en la estación servidor, con la información que distingue al usuario en el mundo material. El mundo digital, en este sentido, se percibe únicamente como una existencia/acción accesoria, dependiente y restringida a su contraparte material. Recientemente, aunque sin una codificación legal adecuada, el historial de navegación de los usuarios en las redes se

11 El secreto opera dentro de un orden que establece lo que debe ocultarse del escrutinio público por su propia naturaleza, mientras que la confidencialidad establece el mismo significado con base en circunstancias circunstanciales. Si bien el secreto es una condición para la formación de lo que se protege, la confidencialidad es una relación entre la necesidad y la posibilidad impuesta a ciertos grupos de interés social, político y/o económico.

ha incluido en el conjunto de datos "protegidos"[12]. Sin embargo, todavía existe una enorme brecha en la protección del individuo[13], que, por un lado, es apropiado comercialmente por las "*Big Tech*" y, por otro, sirve como puerta de entrada para atacar a las democracias contemporáneas.

En esta penumbra sobre la comprensión del mundo digital — a partir del siglo XXI —, varias empresas comenzaron a entender al individuo inmerso en el mundo digital no como una persona física que actúa a través de un medio específico (digital), sino como un "ciudadano digital". Existe la percepción consciente de que las analogías anteriores ya no son funcionalmente válidas. Tomar lo digital como un espejo de lo material ya no es sostenible.

En este sentido, también han tenido que actualizarse los conceptos de privacidad y libertad. Mientras el Estado seguía siendo analógico, las empresas tecnológicas comenzaron a operar según la percepción de la existencia de un "ser digital". La protección de los datos de origen del usuario (que era el centro de la legislación hasta finales del siglo XX) carecía de sentido en los modelos de negocio actuales de *Google* y *YouTube* (Zuboff, 2019) que, por ejemplo, pasaron a retener, estudiar y vender los datos del paso del ciudadano por el mundo digital (elecciones, búsquedas, compras, historiales, entre otros). Ya no era una preocupación los datos de origen (los que identifican al usuario en el mundo físico), sino las elecciones, preferencias y manifestaciones recopiladas de forma individual y anónima, y tratadas mediante estadísticas, que componían un "individuo digital tipificado" que era apropiado por modelos digitales y psicológicos para generar conocimiento.

El mundo digital se separaba del mundo físico. A partir de la consolidación del individuo dentro del mundo digital a través de las redes sociales (y no como un mero reflejo del físico), los únicos referentes relevantes para la realización de actividades digitales pasaron a ser los que existían únicamente en el mundo digital. Los "correos electrónicos" sustituyeron a las cartas físicas para casi todas las necesidades de la vida pública y privada. Con la aparición de los documentos electrónicos, el propio Estado se rinde y pasa a utilizar lo digital como identificadores civiles, legales y sociales. Estos datos consolidan al "ciudadano digital".

En este mismo sentido, el consumo, que podría alegarse que es esencialmente físico (comer, vestirse, vivir, calentarse), acaba creando todo un nuevo espacio de generación de valor económico en un mundo digital, como demuestran empresas como *Uber* o *Ifood*. A principios del siglo XXI, fue el mundo material el que se convirtió en accesorio del mundo digital, y hoy en día, básicamente, la única información que el mundo físico necesita proporcionar a la lógica de organización de las sociedades digitales es la dirección de entrega de los artículos de consumo material.

En este nuevo contexto, es necesario reflexionar sobre la democracia. En principio, el conjunto de derechos establecidos a partir del siglo XVIII tenía como propósito proteger

12 A continuación se presentan algunos testimonios reveladores dados por Peiter Zatko sobre *Twitter* ante el Comité Judicial del Senado de Estados Unidos el 13 de septiembre de 2022 (U.S. Senate committee on the judiciary, 2022) y por Eugene Zarashaw sobre cómo y dónde maneja *Facebook* los datos personales de los usuarios (Biddle, 2022).

13 Aquí es importante llamar la atención del lector sobre la diferencia entre la noción de lo digital como reflejo del mundo material, en la que el individuo digital sería una imagen del individuo material, y la noción de lo digital como autónomo, para un individuo digital que existe de manera indiferente, distante o incluso en oposición a la existencia material.

al individuo limitado al mundo material. Su privacidad, su libertad de pensamiento, la inviolabilidad de su cuerpo físico, del espacio de su hogar (entendido como íntimo), tenían la función principal de preservar el núcleo sociológico y filosófico de lo que el individuo es materialmente, tal como lo definió el liberalismo del siglo XVIII. El Estado protegía las funciones biológicas, sociológicas, políticas y filosóficas de la elección individual.

Incluso cuando nos convertimos en una "sociedad de la información"[14] (no final do século XX), esta información estaba controlada y matizada por herramientas estatales e intereses comerciales. El control sobre las señales de radio y televisión y la legislación sobre telecomunicaciones de los años setenta y ochenta son ejemplos de este proceso. En aquel momento, los ciudadanos necesitaban que se garantizaran la libertad y la privacidad para poder funcionar dentro de la democracia. En resumen, la protección positiva del ciudadano en el mundo material (desde sus funciones de privacidad hasta su libertad) es fundamental para el ejercicio contemporáneo de la democracia. ¿La cuestión central es si tales protecciones pueden lograrse y hacerse efectivas mediante el uso análogo de lo que existe en materia de regulación en el mundo material para el nuevo ciudadano digital?

¿Es posible establecer esta analogía como marco conceptual para las regulaciones en el mundo digital? ¿Basta decir que "lo que es un delito en el mundo material es un delito en el espacio digital"? ¿Y, más aún, protegiendo únicamente mediante el reflejo del ciudadano del mundo físico en el mundo digital, se garantiza que en el ámbito digital tendremos una elección política libre y democrática? ¿Protegiendo únicamente la "privacidad digital" es posible garantizar la condición de pensamiento autónomo e individual que la democracia busca asegurar? El problema central para responder a estas preguntas radica en cómo se conceptualiza el ciberespacio.

El concepto de ciberespacio

El punto de partida de esta conceptualización fueron las redes de comunicación analógica (teléfono, radio y televisión) en las décadas de los años 50 y 60. Así, la noción original de ciberespacio se basaba en un conjunto de elementos definidores del "punto de acceso" (I), el "nodo de direccionamiento" (II) y el "punto de llegada" (III) y los "paquetes de información" (datos) (IV). El espacio digital estaba delimitado, por lo tanto, por la relación que se establecía en el proceso de comunicación de datos. (Fang, 2018, p. 28).

Poco a poco, este sentido fue consolidando la imagen de una "red" (*network*) que conectaba digitalmente (y físicamente) puntos de acceso a los lugares accedidos. La conexión digital entre estos puntos creaba la ilusión de un espacio inmaterial, pero real, que se entendía por analogía con el espacio físico y, por lo tanto, susceptible de ser coordinado/

14 Aquí, distingo la Sociedad de la Información de la Sociedad Digital desde el marco de la consolidación del "ciudadano digital". Si bien la convergencia entre lo digital y lo material garantizaba la presencia de lo digital como accesorio, nos encontrábamos en una "sociedad de la información" (siglo XX). En el siglo XXI, el mundo digital se constituye y construye una sociedad digital (Mosco, 2017).

regulado por los Estados. Encontrar a los responsables de las acciones en el mundo digital siempre significaba salir de este mundo y volver al material para poder identificar, procesar, culpar, gravar o compensar.

En 1997, Estados Unidos creó números de registro y asignación digitales, entregando la gestión de estos números de direccionamiento (que individualizan cada acceso a las redes) a una empresa privada llamada ICANN (*Internet Corporation for Assigned Names and Numbers*)[15]. El espacio digital estaba bajo escrutinio, y la concesión o revocación de permisos para su uso recaía en una empresa privada estadounidense. Este fue solo el comienzo de la lucha por la soberanía del ciberespacio (Konkas, 2023).

Hasta este punto, explorar el espacio digital y transformarlo en números de direcciones significaba poseer ese mismo espacio. En este sentido, aparece en el concepto de ciberespacio, propuesto por *National Military Strategy for Cyberspace Operations*[16] del gobierno de los EE.UU., en 2006, como

> […] a domain characterized by the use of eletrocnics and electromagnetic spectrum **to store, modify and exchange information** via networked systems and physical structures (Departament of Defense Washington, 2006, p. 9, nuestro énfasis)[17].

Hasta principios del siglo XXI, para proteger a los ciudadanos, basándose en el principio de analogía entre lo material y lo digital, bastaba que el Estado protegiera los datos de identificación del individuo que accede a la red y la información almacenada intencionadamente por éste[18]. Fue a partir del retraso en la comprensión por parte de los Estados sobre cómo funcionaba el mundo digital que algunas empresas privadas vislumbraron la oportunidad de convertirse en multimillonarias. Si bien los datos de identificación y la información producida y almacenada por los individuos estaban protegidos por el concepto de ciberespacio de la época, la información producida por el **tránsito** del individuo (usuario) en el mundo digital (como compras en línea, visitas, elecciones, "me gusta", manifestaciones, etc.) no lo estaba. Rápidamente, Google y otras empresas se organizarían en el mundo digital para estimular no solo que los individuos se constituyeran en el mundo digital (mediante la creación de perfiles y redes sociales), sino también que navegaran y se mantuvieran activos las veinticuatro horas del día, produciendo información.

Por esta razón, no debería sorprender que el coste de acceso a la red informática global haya disminuido rápidamente en comparación con las décadas de 1980 y 1990, y

15 Hoy en Brasil, ésta es una de las funciones del Comité Gestor de Internet. (CGI.br).

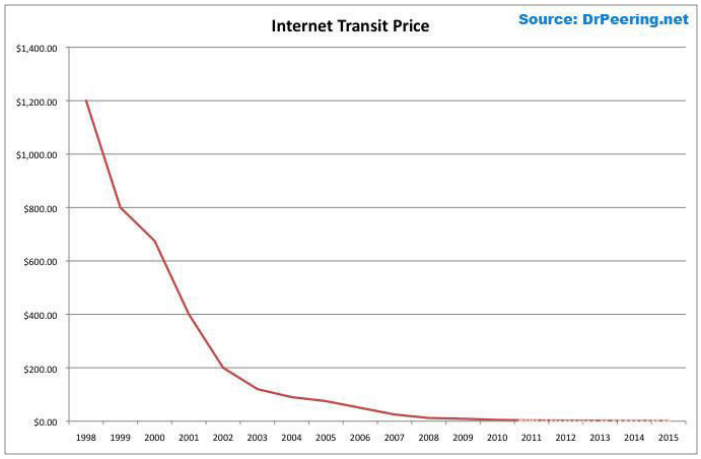
16 DEPARTAMENT OF DEFENSE WASHINGTON. **The national military strategy for cyberspace operations (U)**. Washington: Departament of defense, 2006. 54 p. Disponible en: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf. Consultado en: 25 jul. 2025.

17 Traducción: […] Un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético **para almacenar, modificar e intercambiar información** a través de sistemas en red y estructuras físicas (Departament of Defense Washington, 2006, p. 9, nuestro énfasis, traducción editorial).

18 Cabe destacar la diferencia entre la información depositada deliberadamente en las redes y los datos extraídos por la acción del individuo dentro del mundo digital. Sobre el primer tipo de información, existe un consenso relativamente establecido de que está protegida por analogías con la propiedad intelectual en el mundo material. Sobre el segundo tipo de información (las impresiones de paso y movimiento en las redes), las "*Big Techs*" se aseguran el derecho a ser propietarias de dicha información. La afirmación se basa en la idea de que dicha información no sería posible sin el trabajo de seguimiento que realizan estas empresas. Así, ellas serían las creadoras de estos conjuntos de información que, hoy en día, son inmensamente más valiosos que los primeros.

que la tendencia sea, como mínimo, hacia el acceso gratuito. No se trata de una reducción de los costes de acceso debido a las "nuevas tecnologías", sino de un modelo de negocio que ahora depende de la generación de esta información a medida que las personas se mueven por las redes[19]. Cuanto mayor sea el tiempo de conexión, mayor será la cantidad de información producida y mayor el beneficio para las empresas que operan en este nicho.

Imagen 1 – Precio del tránsito de Internet



Fuente: DrPering.net, c2014.

En el siglo XXI, las empresas denominadas "*Big Tech*" animan a los Estados a convertir el derecho al acceso al mundo digital en un derecho humano y a trabajar (los Estados) para ofrecer a todos la posibilidad de convertirse en "ciudadanos digitales". A partir de ahí, todo ciudadano del mundo digital es un creador incesante de información pasajera[20] en las redes, y esa información genera valor económico. Al igual que ocurrió con el surgimiento de la educación pública en el siglo XIX, la lógica es que los Estados paguen los costes de la inserción digital de todos para que estos ofrezcan materia prima (como ciudadanos digitales) a la iniciativa privada. Ahora, ya no solo dentro de los Estados, sino a escala mundial.

Sin embargo, a diferencia de la información que distingue a los sujetos en el mundo material (su nombre, dirección, números de documentos o sus producciones intelectuales y artísticas específicas dentro de la red), esta nueva lista de información producida por los sujetos NO ES de su propiedad, por lo que puede ser organizada, reorganizada, apropiada y vendida en función de los intereses de empresas privadas. **La mercantilización de los sujetos digitales implica la alienación de estos sujetos sobre la información que producen.** Y aquí, convenientemente, cesaron las analogías capitalistas entre la propiedad privada del mundo material en el siglo XX y la propiedad del mundo digital del siglo XXI.

19 Los datos agregados son un promedio. Al estratificarlos, se observa que en zonas periféricas con bajos niveles de consumo, los valores se mantuvieron estables o experimentaron reducciones marginales (como en América Latina) e incluso aumentaron, como en algunos casos en el continente africano (Kazeem, 2019).

20 La información que identifica a un individuo y permite ubicarlo en el mundo material está protegida, ya que se entiende que la posee. Sin embargo, el resto de la información generada en el mundo digital se entiende como ajena a cualquier persona. Cada acceso a un sitio web de compras, las páginas visitadas, el tiempo dedicado a cada sitio o pantalla, los "me gusta" u otras señales de aprobación o desaprobación generan una enorme cantidad de información que los modelos de negocio digitales del siglo XXI han aprovechado para generar valor.

La generación de valor generada por la apropiación de información de diversos sujetos que transitan por el mundo digital ha sido tan grande que las empresas ya no se preocupan por establecer vínculos entre lo digital y lo material. Se crean perfiles falsos en todas las redes sociales sin ninguna preocupación ni control, lo que demuestra que la información que distingue a los individuos (el foco de toda la legislación y la seguridad del Estado en el siglo XX) ha perdido importancia.

Las grandes empresas digitales ya no quieren saber quién eres ni dónde estás. Esta información ya no es necesaria para generar valor en el mundo digital. Necesitan tu perfil digital. Al mapear las elecciones, preferencias o antipatías de cualquier sujeto (real, parodias, oculto, anónimo, etc.), incluso si no se identifica ni se distingue en el mundo material, se obtiene información comercial relevante que las empresas digitales se apropian y venden como si fuera de su propiedad. Para la construcción de perfiles digitales psicográficos que puedan utilizarse para estrategias de marketing o políticas, la identificación de ciudadanos materiales en el mundo digital es totalmente innecesaria hoy en día. En otras palabras, el conjunto de información que el perfil del "gatito azul" produce en las redes sociales tiene el mismo valor que el perfil de "Antônio Silva", siendo este último plenamente identificado y distinguido en el mundo material.

Si bien no puede controlar eficazmente esta información, el valor generado por la apropiación de información en tránsito no ha pasado desapercibido para el Estado en los últimos años. Y, aunque aún no existe una forma específica de tributación para este tipo de producción y apropiación de la **creación humana en el mundo digital**, el concepto de ciberespacio se ha modificado gradualmente no solo para "proteger" a los usuarios, sino también para permitir al Estado un mayor control (soberanía) sobre el mundo digital.

En 2003, en un documento titulado "*The National Strategy to Secure Cyberspace*" (Estrategia Nacional para Proteger el Ciberespacio), la Casa Blanca definía el "ciberespacio" como

> […] composed of hundreds of thousands of interconnected computers, servers routers, switches, and fiber optic cables that allow our critical infrastructures to work[21] (United States, 2003, p. vii)[22].

Aunque está claro que el concepto es muy poco funcional, ya amplía el significado de ciberespacio en comparación con el del siglo XX. Antes, solo los servidores y otros espacios de almacenamiento de información formaban parte de dicha definición. Las estaciones de contacto y producción (los ordenadores personales de los usuarios) no formaban parte del ciberespacio, al igual que tampoco lo eran los routers o los puntos intermedios de redireccionamiento.

21 UNITED STATES. **The National Estrategy to secure cyberspace**. Washington: The White House, 2003. Disponible en: https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf. Consultado en: 30 ago. 2023.

22 Traducción: "[…] compuesto por cientos de miles de ordenadores, servidores, routers, conmutadores y cables de fibra óptica interconectados que permiten el funcionamiento de nuestras infraestructuras críticas." (United States, 2003, p. vii, traducción editorial).

El concepto utilizado en 2022 por la NICCS (*National Initiative for Cibersecurity careers and studies*) de la CISA (*Cybersecurity and Infrastructure Security Agency*) de los Estados Unidos para comprender el mundo digital ya no es “ciberespacio”, sino “ciberecosistema”, y la agencia lo define como:

> The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions (NICCS, 2025, *online*)[23].

La diferencia es significativa. La analogía que guió a las sociedades a lo largo del siglo XX, del espacio digital como un “espacio real inmaterial”, se está desvaneciendo. En 2022, el núcleo del concepto ya no reside en la noción de “espacio” en sí, sino en las relaciones o “sistemas” de interconexión. En 2022, el foco de la protección que el Estado busca lograr ya no son los datos de identificación ni sus ubicaciones de almacenamiento, sino los individuos digitales, sus decisiones, su entorno y sus condiciones de interacción.

A partir de esta nueva comprensión de lo que sería lo “digital”, la analogía con el espacio físico (que orientó las primeras acciones del Estado en el mundo digital) comienza a descartarse y se hace necesario un nuevo esfuerzo de conceptualización. La protección y el control del Estado (que caracterizan la idea de soberanía) ya no pueden establecerse únicamente en los puntos materiales en los que el mundo digital se encuentra con el mundo material (servidores, *switches*, cables, etc.). También es necesario un esfuerzo para pensar, en el momento actual, en formas de proteger el “medio digital” en sí mismo, las “interacciones” de los usuarios y los efectos o consecuencias de estas acciones en la vida material.

El tejido digital se aleja de la noción analógica de “espacio” y se acerca al sentido contemporáneo de “tiempo”. Este movimiento, dicho sea de paso, forma parte de la transformación epistemológica característica del siglo XXI[24]. La ilusión del espacio digital se desvanece, y su transformación en un “espacio-tiempo” continuo es lo que permite la enorme generación de valor económico que ofrece el mundo digital. Sin embargo, esta misma transformación también acaba amenazando a las democracias contemporáneas.

23 Traducción: “La infraestructura de información interconectada de las interacciones entre personas, procesos, datos y tecnologías de la información y la comunicación, junto con el entorno y las condiciones que influyen en dichas interacciones.” (NICCS, 2025, *online*, traducción editorial).

24 Entre todas as novidades que estão em estudo ou já de alguma forma assentadas, a epistemologia do século XXI passou a não assumir o objetivo e o subjetivo como separados, emulando a impossibilidade de separar o tempo do espaço predito pela Teoria da Relatividade (Wendt, 2015).

Protegiendo la democracia

Uno de los problemas contemporáneos más urgentes que hay que resolver es la cuestión de la influencia del mundo digital en la democracia[25]. Transformaciones recientes[26] (como las experiencias de *Brexit*, o incluso las elecciones brasileñas de 2018 y 2022) estos métodos han demostrado ser un desafío muy complejo para las antiguas herramientas de control del siglo XX, e incluso para algunos intentos desarrollados a principios del siglo XXI. Tanto el control y la apropiación de los datos de los usuarios como la educación digital de los individuos se han instrumentalizado políticamente mediante técnicas de microsegmentación (Eisenberg; Cepik, 2002)[27].

La proliferación de nuevos canales y plataformas de comunicación hace prácticamente imposible controlar y responsabilizar civil o penalmente a las personas, basándose en la anticuada analogía del mundo digital como un "espacio" que refleja el mundo material. Una mujer tranquila y jubilada de 65 años en el mundo real puede ser una neonazi activa en el mundo digital, operando en redes sociales desde un teléfono celular las 24 horas del día. Incluso la información generada por los usuarios en el mundo digital no es propiedad de esos usuarios (porque estas son las fuentes de generación de valor por *Big Tech*), luego

25 "A revolução digital, em particular o forte desenvolvimento das redes sociais, alterou radicalmente o funcionamento da nossa democracia. Oferece inúmeras novas possibilidades de comunicação e de acesso a uma quantidade infinita de informações. Mas a Internet também deteriorou a qualidade que tradicionalmente estava assegurada na informação, reduziu o nível dos debates e inundou o espaço público de slogans simplistas, notícias falsas e polarização. Substituiu as comunidades reais, que uniam pessoas reais, solidárias entre si, por bolhas virtuais, que não proporcionam aos seus membros ligações genuínas" (Council of Europe, 2022, p. 3, traducción editorial). Original: "The digital revolution, in particular the strong development of social media, has radically changed the functioning of our democracy. It offers a myriad of new possibilities to communicate with each other and to access infinite information. But the internet has also undermined the traditional quality assurance of information, lowered the standard of debate and filled the public space with a deluge of simplistic slogans, fake news and polarisation. It has replaced the real communities that bound real people together, caring for each other, with virtual bubbles that do not give their members a rooting in anything real" (Council of Europe, 2022, p. 3).
Traducción: "La revolución digital, en particular el fuerte desarrollo de las redes sociales, ha cambiado radicalmente el funcionamiento de nuestra democracia. Ofrece un sinfín de nuevas posibilidades para comunicarnos entre nosotros y acceder a una información infinita. Pero Internet también ha socavado la garantía tradicional de la calidad de la información, ha rebajado el nivel del debate y ha inundado el espacio público con una avalancha de eslóganes simplistas, noticias falsas y polarización. Ha sustituido a las comunidades reales que unían a personas reales, que se cuidaban unas a otras, por burbujas virtuales que no proporcionan a sus miembros ningún arraigo en la realidad" (Council of Europe, 2022, p. 3, traducción editorial).

26 "Cyberspace is not just the space in which myths are enacted; it also contributes to mythic thinking today, because it embodies the sense of betwixt and between (or, more formally, what cultural theorists call liminality). Myths are fed by the sense that we are leaving one era, the Industrial Age, and entering a new one, with a host of names, most of which, like "Information Age" and "Digital Age," have to do with computers. The "then" and "now" markers change depending on whether one accentuates the technological, the economic, the political, the social, or the cultural (e.g., are we moving from the factory to the office? From modernism to postmodernism?). They also change depending on how one feels about (e.g.) the difference between the Information Age and the Surveillance Society" (Mosco, 2004, p. 32).
Traducción: "El ciberespacio no es solo el espacio en el que se representan los mitos, sino que también contribuye al pensamiento mítico actual, ya que encarna la sensación de estar entre dos mundos (o, más formalmente, lo que los teóricos culturales denominan "liminalidad"). Los mitos se alimentan de la sensación de que estamos dejando atrás una era, la era industrial, y entrando en una nueva, con una gran cantidad de nombres, la mayoría de los cuales, como "era de la información" y "era digital", tienen que ver con los ordenadores. Los marcadores "antes" y "ahora" cambian dependiendo de si se acentúa lo tecnológico, lo económico, lo político, lo social o lo cultural (por ejemplo, ¿estamos pasando de la fábrica a la oficina? ¿Del modernismo al posmodernismo?). También cambian dependiendo de cómo se perciba (por ejemplo) la diferencia entre la era de la información y la sociedad de la vigilancia" (Mosco, 2004, p. 32, traducción editorial).

27 Un método o proceso de uso de grandes bases de datos en redes digitales para mapear patrones de comunicación y abordar estilos de comunicación únicos para grupos específicos, con el objetivo de aumentar la adherencia, confiabilidad y legitimidad del mensaje transmitido, a menudo independientemente de si el contenido es verdadero o no.

los crímenes cometidos en el mundo digitall (como las "*fake news*") parecen poseer una condición ontológica de no tener autoría, quedando fuera de las capacidades de control (soberanía) del Estado[28].

Comprender el mundo digital como un "espacio físico" reflejado para aplicar, por analogía, las herramientas de control desarrolladas históricamente para el Estado Moderno ha resultado insuficiente para la protección de la democracia misma. La computación en la nube, por ejemplo, ha hecho que tal analogía sea casi imposible de sostener, ya que los "servidores" ya no pueden utilizarse como puntos de acceso físicos únicos e individuales, sujetos a sanciones y control respecto a la información que circulan. En esta brecha, muchas amenazas se han mantenido activas. Las empresas venden información a partidos o grupos políticos, y estos grupos actúan de forma criminal y agresiva contra las instituciones democráticas, sin ninguna oposición mínimamente funcional por parte de los poderes del Estado.

En el mundo físico, se han desarrollado la policía, las fronteras, la vigilancia con cámaras, la denuncia anónima y una serie de otras herramientas estatales para controlar el espacio y hacer valer la soberanía estatal. Esto se debe, en gran medida, a que, en el mundo físico, la materia no se reproduce (ni desaparece) a un ritmo mayor que el que los medios de control y prueba pueden apropiarse (o percatarse) de su existencia. Si consideramos, por ejemplo, las formas en que el Estado controla actividades como la expansión del nazismo o la imposición de impuestos a los bienes manufacturados, veremos la importancia de la materialidad física. La condición de la existencia física de la materia es la base de todas las construcciones institucionales que el Estado ha construido para ejercer su soberanía. Esta ha dejado de existir en los últimos veinte años en el mundo digital[29].

Todos los intentos de controlar físicamente el mundo digital han fracasado. Se han intentado códigos rastreables, programas de duplicación, mantenimiento de datos digitales y todo tipo de personalización de la información. Tecnología NFT[30] es exactamente eso. Esfuerzos desesperados por mantener la analogía entre los mundos digital y físico y por reproducir en el mundo digital la escasez característica del mundo material. El arma de un delito que se pretende castigar, o el producto del trabajo humano que se pretende gravar,

28 Hasta el cierre de este artículo, esperé el texto final del proyecto de ley 2630 propuesto por el Gobierno brasileño para regular las "*Big Tech"* y "acabar con las noticias falsas". Por los mismos problemas señalados en este artículo, el intento brasileño también es inútil. Adolece de problemas de diseño de la ley, falta de capacidad técnica del Estado y un profundo desconocimiento de la escala de producción de información que existe hoy en día en el mundo digital. Incluso la DSA (*Digital Services Act*), la regulación propuesta por la UE, no entrará en vigor hasta 2024 y, en la práctica, todavía no tenemos ejemplos efectivos de protección estatal.

29 En el mundo real, dos cuerpos no pueden ocupar el mismo espacio al mismo tiempo, y la materia no puede replicarse sin una enorme cantidad de energía y tiempo. En el mundo digital, en cambio, todo es replicable, consumible y desaparece casi sin dejar rastro.

30 NFT significa literalmente "*non fungible token*" o pieza no consumible, en el sentido de que no desaparecerá ni se replicará en su esencia. Es un intento del mundo digital por recrear la escasez del mundo material y otorgar valor a ciertos objetos digitales. Una obra de arte producida en el mundo digital puede copiarse infinitamente y no hay posibilidad de escasez. En la percepción económica tradicional, su valor siempre sería el mismo y tendería a cero. Con la creación de los "NFT", el capitalismo digital intenta romper con esta característica del mundo digital y, así, aplicar la lógica conocida del valor a través de la escasez en el mundo.

no se multiplica (ni desaparece) en el mundo material como sí puede hacerlo en el mundo digital[31]. Esta característica del mundo digital ha demostrado ser un desafío complejo para que el Estado ejerza efectivamente su soberanía sobre el mundo digital.

Una parte importante de este problema reside en la analogía del mundo digital como un "espacio" que requiere una materialidad única (o al menos una construida a partir de datos) para ser comprendido por los seres humanos. ¿De dónde (base física) se originan los ciberataques a un país? ¿Dónde está el punto de acceso del usuario que amenaza la democracia? El punto de referencia espacial para estas preguntas es esencial para que las herramientas estatales actuales operen en control o contención precisamente por analogía. La existencia digital sin una referencia material sigue siendo difícil de comprender, especialmente para las sociedades históricamente analógicas.

La experiencia americana

La velocidad de la transformación digital es algo a lo que los países y sociedades de todo el mundo aún no se han adaptado. Si bien es cierto que Estados Unidos fue el país que controló el mundo digital durante el siglo XX, creando empresas para indexar, controlar y explotar dicho mundo, también es cierto que, aun así, Estados Unidos parece no estar preparado para las transformaciones más recientes, tanto en la economía digital como en las transformaciones sociales resultantes.

El sociólogo Vincent Mosco (Mosco, 2004) sostiene que existía un mundo digital antes de las "*Big Techs"*[32] y otro, completamente diferente, después de las transformaciones que estas empresas han generado en el mundo digital. El siglo XXI ha sido testigo de cambios cada vez más rápidos y profundos en la forma en que las sociedades viven en el mundo digital. Si bien todo el proceso de creación de la World Wide Web estuvo controlado por Estados Unidos durante el siglo XX[33], dada la escala de la producción de información que se practica en el siglo XXI, el Estado estadounidense no ha podido mantener el control y el escrutinio de Internet.

Las repercusiones de esta transformación fueron múltiples, desde la percepción de una pérdida de control estatal, que derivó en investigaciones sobre las fallas de seguridad que finalmente permitieron los atentados contra el WTC en 2001, hasta investigaciones sobre delitos sexuales y el contrabando de armas químicas. La sociedad estadounidense comenzó a exigir un control sobre el mundo digital que Estados Unidos, como Estado, ya no podía imponer.

---

31 Una de las iniciativas más exitosas para evitar el borrado y la modificación de datos es la tecnología "*blockchain*", que está permitiendo la consolidación de las monedas digitales, según la profesora Gláucia Campregher (2022).

32 "*Big Tech"* Es el término utilizado para referirse al conjunto de empresas que controlan y operan en el mundo digital. *Google* se creó en septiembre de 1998, *Facebook* en febrero de 2004 y *Uber*, por ejemplo, en marzo de 2009. Cada uno de estos servicios tiene una empresa detrás, como, por ejemplo, *Alphabet Inc*., matriz de *Google*, *YouTube*, etc.

33 Desde la década de 1960 hasta 1997, el Departamento de Comercio de EE. UU. controlaba todos los permisos e incluso la indexación de direcciones en la red. En 1997, el gobierno estadounidense transfirió esta responsabilidad (y el monopolio de la asignación de nombres y números de registro) a la empresa ICANN (*Internet Corporation for Assigned Names and Numbers*), que aún hoy conserva sus responsabilidades (ICANN, 2021).

En este escenario, las "*Big Tech*" se afirman. No sólo ha habido un cambio en la forma en que se extrae valor del mundo digital. La creación de las llamadas "redes sociales" (como *Facebook, Twitter* y *YouTube*) ha dado lugar efectivamente a individuos digitales. Antes de las redes sociales, la presencia de las personas en ellas era efímera. Internet se utilizaba como medio de comunicación, repositorio de datos o plataforma de intercambio. **Las redes sociales generan vida digital (existencia).** Al crear un "perfil", el usuario se constituye en el mundo digital. Sus gustos, intereses, posturas políticas, preferencias sociales e incluso la forma en que construye su discurso han sido apropiados (explotados) por plataformas que han mercantilizado esta "información transitoria". El nombre real del usuario, su dirección o cualquier otra información que el mundo material exige e impone como "secreto" ya no importaba. Las redes se benefician más de los perfiles falsos (ya que también reducen los costos legales de mantenerlos) y ni siquiera necesitan saber quién está realmente detrás del perfil, dónde está ni con qué propósito. Todo el marco de gobernanza digital creado en el siglo XX ha quedado completamente obsoleto.

Constituidos como individuos digitales, los seres humanos han llegado a vivir en redes. Consumir, aprender, colaborar, explorar, trabajar, robar, amenazar, secuestrar y prácticamente todas las acciones que se realizan en el mundo material se han llevado a cabo en el mundo digital. Hoy en día, las redes sociales prescinden de nombres a cambio de información sobre comportamiento político, social y comercial, preferiblemente generada las 24 horas del día. Todas las luchas de los marcos de gobernanza del siglo XX contra la entrega de "información confidencial" sobre individuos se han vuelto anacrónicas. El modelo actual de extracción de valor prescinde de cualquier información que conecte lo real con lo digital. Con la excepción de la dirección de entrega de los bienes adquiridos, las plataformas no necesitan mantener nada más.

A medida que estos seres digitales se mueven a través de las redes, imprimen patrones de comunicación, conducta política, preferencias comerciales y comportamiento[34]. En el siglo XXI, el mundo digital extrae valor precisamente de esta información que, en el siglo XX, se consideraba insignificante (basura, en inglés). Que dicha información se genere mediante un perfil social con nombre real y fotos, o mediante un perfil falso con la foto de un peluche y un nombre completamente extraño, da igual para las plataformas actuales. El peluche del perfil consumirá, compartirá, producirá, etc., de la misma manera que el perfil "real", y para el mundo digital, su individualización ya no necesita reflejar el mundo material. De ahí la pregunta: ¿qué debe proteger realmente el Estado?

En el siglo XX, eran las direcciones reales, los números de documentos y todo tipo de información lo que, por analogía con el mundo material, el Estado consideraba importante. Este cambio de importancia no ha sido bien comprendido por los Estados incluso hoy en día, ni siquiera por el estadounidense. Se han generado billones de dólares a partir del desperdicio de información digital (información que nadie quería en el siglo XX), y los controles

34 A toda esta información la llamo aquí "información de tránsito" porque se genera a partir del tiempo que los ciudadanos pasan (conectados) en el ciberespacio..

estatales han sido ineficaces[35]. Tanto para proteger a la sociedad como para la tributación y la recaudación de impuestos. En la práctica, las "*Big Tech"* tecnológicas han vivido los últimos 10 o 12 años en un paraíso capitalista sin ley. Las empresas digitales dedicadas a las apuestas, los juegos de azar y la venta de prácticamente cualquier cosa imaginable (bienes y servicios legales e ilegales) se han amontonado en las redes, convirtiéndose en multimillonarias y dejando al Estado cada vez más indefenso, según la analogía fundamental de comprensión que citamos en este artículo. Relacionar lo digital con lo material ya no permitía una comprensión de lo digital como se intentaba antes.

El momento en que el Estado comprendió la necesidad de reinterpretar el mundo digital, ahora desde nuevas perspectivas, fue la aparición de *Cambridge Analytica* y la manipulación que este comenzó a ejercer sobre los significados políticos de una sociedad. El referéndum del 23 de junio de 2016, en el que Inglaterra decidió abandonar la Unión Europea, reveló este nuevo mundo digital para el cual todas las herramientas de control anteriores (que ya eran prácticamente inútiles) quedaron obsoletas.

Estados Unidos, Europa y prácticamente todo el mundo se habían dado cuenta de que lo que necesitaba protección no era la información estática en cualquier servidor sobre el origen y las características materiales de algún usuario. **Lo que necesitaba protección era la condición humana de la toma de decisiones individual, bien informada y crítica.** El mundo digital capturó la esencia de nuestras construcciones políticas y la unidad básica de nuestras democracias: **las condiciones para formarse juicios sobre el mundo.**

La comercialización de este nuevo "producto", secuestrado por las grandes tecnológicas, ha devuelto el fascismo a la sociedad. La extrema derecha, con el fuerte apoyo de multimillonarios, ha logrado superar las características únicas de algunos políticos de masas, como la capacidad de comunicación, el carisma, la empatía y la representatividad, utilizando mecanismos y herramientas de comunicación digital. Hoy, en la política digital, se pueden crear Martin Luther King y Mandelas de la nada con una estrategia de comunicación digital. Esto le ha dado a la extrema derecha todo el éxito electoral que necesitaba para atacar la idea misma de la democracia.

Lo más interesante de esto es que las "*Big Tech"* comercializan esta información, extrayendo valor financiero y político de todo lo que sucede en las redes, pero al mismo tiempo se declaran neutrales e irresponsables de lo que se produce a través de sus herramientas en el mundo digital. Esta doble conducta, la de una presencia para reclamar beneficios y propiedad, y la de una ausencia para asumir responsabilidades, es el tema central hoy en día en todos los estudios sobre gobernanza digital.[36].

35 El ejemplo más preocupante fue Cambridge Analytica, que compró miles de millones de datos de Facebook (a un precio de 2 o 3 dólares por perfil) que en ese momento no estaban protegidos porque estaban "desidentificados". Facebook (Meta) modificó sus términos de privacidad para obligarse a proteger únicamente la información que identifica a las personas en el mundo material y no los datos de tránsito. Estos datos fueron vendidos a Cambridge Analytica (Mccallum, 2022).

36 El simple acceso a los informes de investigación elaborados por la Unión Europea en 2021 y 2022 da una idea de la importancia de este problema para la política del Viejo Continente. Por un lado, existe una dificultad para gravar y regular, y por otro, también existe una dificultad para exigir responsabilidades a los ciudadanos digitales e incluso protegerlos (ver, por exemplo, o "Relatório do grupo de alto nível para a democracia europeia" de 31 de enero de 2022).

En este sentido, la Corte Suprema de Estados Unidos comenzará a analizar la cuestión en abril de 2022, a partir del caso "Reynaldo Gonzalez *et al*. vs. *Google*"[37]. Básicamente, los defensores de la acción argumentan que indexar y ofrecer la información no puede considerarse una acción neutral:

> Mere posting on bulletin boards and in chat rooms was the prevalent practice when section 230[38] was originally enacted. But over the last two decades, many interactive computer services have in a variety of ways sought to recommend to users that they view particular other-party materials, such as written matter or videos. Those recommendations are implemented through automated algorithms, which select the specific material to be recommended to a particular user based on information about that user that is known to the interactive computer service. The public has only recently begun to understand the enormous prevalence and increasing sophistication of these algorithm-based recommendation practices (United States, 2021, *online*)[39].

El caso en cuestión aborda precisamente la pregunta: "¿Qué debe protegerse en el mundo digital?". El argumento de los peticionarios es que la indexación y la oferta de cualquier contenido no se realiza mediante un algoritmo "neutral" y, si permite obtener beneficios de la compra de espacio publicitario y preferencias de indexación, también debe rendir cuentas por el daño que la información allí presentada pueda causar.

> That financial structure has given rise to the now widespread practice of recommending (for want of any agreed upon better term) material to website users, in the hope of inducing them to look at yet more material and thus to remain ever longer on that website. Many of those recommendations are based on algorithms, which review all the information an interactive service provider has about each particular user, and selects for recommendation the material in which that user is most likely to be interested. "[A]lgorithms [are] devised by these companies to keep eyes focused on their websites.... '[T]hey have been designed to keep you online [...] (United States, 2021, *online*)[40].

Al momento de redactar este artículo, el Tribunal Supremo aún no había emitido un fallo, pero la cuestión es clara y exige un cambio de paradigma completo. Lo que debe protegerse, mediante la legislación estatal, ya no es el "espacio" digital, entendido de forma

37 UNITED STATES. Court of appeals for the Ninth Circuit. Petition for a writ of certiorari filed. **No. 21-1333**. Julgado em: 22/06/2021. Disponible en: https://www.supremecourt.gov/docket/docketfiles/html/public/21-1333.html. Consultado en: 25 jul. 2025.

38 Sección 230 del Título 47 de "Telecommunications Act", de 1996, dice que "No provider or user of an interactive computer service shall be treated as the publisher of or speaker of information provided by another information content provider" (One hundred fourth congress of the United States of america, 1996, p. 101). Este dispositivo constituye la base de la protección que las *Big Tech* tecnológicas se proporcionan a sí mismas cuando se les imponen responsabilidades civiles o penales..

Traducción: "No provider or user of an interactive computer service shall be treated as the publisher of or speaker of information provided by another information content provider" (One hundred fourth congress of the United States of america, 1996, p. 101, traducción editorial).

39 Traducción: "Cuando se promulgó inicialmente la sección 230, la práctica habitual consistía simplemente en publicar mensajes en tablones de anuncios y salas de chat. Sin embargo, durante las últimas dos décadas, muchos servicios informáticos interactivos han intentado, de diversas maneras, recomendar a los usuarios que vean determinados materiales de terceros, como textos escritos o vídeos. Estas recomendaciones se implementan mediante algoritmos automatizados, que seleccionan el material específico que se va a recomendar a un usuario concreto basándose en la información sobre ese usuario que conoce el servicio informático interactivo. El público solo ha empezado a comprender recientemente la enorme prevalencia y la creciente sofisticación de estas prácticas de recomendación basadas en algoritmos" (United States, 2021, *online*, traducción editorial).

40 Traducción: "Esa estructura financiera ha dado lugar a la práctica, ahora muy extendida, de recomendar (a falta de un término mejor acordado) material a los usuarios de sitios web, con la esperanza de inducirlos a ver aún más material y, por lo tanto, a permanecer más tiempo en ese sitio web. Muchas de esas recomendaciones se basan en algoritmos, que revisan toda la información que un proveedor de servicios interactivos tiene sobre cada usuario en particular y seleccionan para recomendar el material que más probablemente le interese a ese usuario. "[E]stos algoritmos [han] sido diseñados por estas empresas para mantener la atención centrada en sus sitios web... [H]an sido diseñados para mantenerte conectado" [...]" (United States, 2021, *online*, traducción editorial).

análoga al mundo material a través de la información que permite el reconocimiento y la individualización de los ciudadanos reales. La información estática, alojada en uno o más servidores, tampoco requiere necesariamente protección estatal en el mundo digital del siglo XXI. El objetivo es proteger el "tiempo" que un individuo pasa en el mundo digital. Cambiar el concepto de ciberespacio por una interpretación del tiempo dentro de las redes permite proteger la capacidad de cada ciudadano para comprender el mundo individualmente, mediante la responsabilidad de indexar y presentar la información al ciudadano digital.

No está claro si este cambio de paradigma será suficiente para proteger a los ciudadanos (y, en consecuencia, a la política y la democracia) en el mundo digital. Sin embargo, es evidente que el camino seguido por Estados Unidos parece más fructífero para resolver el problema que, por ejemplo, las iniciativas brasileñas. Estas iniciativas son las que analizaremos a continuación.

El camino de Brasil

La analogía entre el mundo digital y el físico ya surgió en Brasil con la LGPD (Ley General de Protección de Datos) de 2018[41]. Existe una gran dificultad para hacer referencia al alcance de la Ley precisamente por la cuestión de la analogía. En el artículo 3, por ejemplo, la ley establece que

> aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados (Brasil, 2018, *online*)[42]

A continuación, se incluyen tres cláusulas que buscan dotar de mayor precisión geográfica a la disposición, haciendo hincapié en el elemento de "territorio nacional". Obviamente, esto implica la aplicación del concepto de soberanía y, por lo tanto, legislar únicamente sobre asuntos "nacionales", pero también recurre a la desafortunada noción analógica de "territorio", que, como hemos demostrado, se ha abandonado a nivel mundial en materia de gobernanza digital[43].

En el artículo 5 de la misma ley se intenta definir qué es lo que realmente abarca la ley, enumerando un total de 19 cláusulas para intentar dar cuenta de la definición de los cuatro

41 BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei n.º 13.853, de 2019). Brasília: Presidência da República, 2018.

42 Traducción: "Esto se aplica a cualquier operación de tratamiento realizada por una persona física o jurídica, de derecho público o privado, independientemente del medio, del país de su sede o del país donde se encuentren los datos" (Brasil, 2018, *online*, traducción editorial).

43 La DSA (*Digital Services Act*) y la DMA (*Digital Markets Act*) europeas ya tratan de no limitarse al territorio europeo como sede de "servidores" que almacenan información estacionaria y pretenden la soberanía sobre todo lo que acceden los ciudadanos europeos: "A fim de assegurar a eficácia das regras estabelecidas no presente regulamento e condições de concorrência equitativas no mercado interno, essas regras deverão aplicar-se aos prestadores de serviços intermediários, independentemente do seu local de estabelecimento ou da sua localização, desde que ofereçam serviços na União, tal como comprovado por uma ligação substancial à União" (União Europeia, 2022, *online*).

Traducción: "Para garantizar la eficacia de las normas establecidas en el presente Reglamento y la igualdad de condiciones en el mercado interior, dichas normas se aplicarán a los prestadores de servicios intermediarios, independientemente de su lugar de establecimiento o ubicación, siempre que ofrezcan servicios en la Unión, como lo demuestra un vínculo sustancial con la Unión" (União Europeia, 2022, *online*, traducción editorial).

elementos que componen el mundo digital, a saber: emisor, receptor, medio y mensaje[44]. El intento de definir con precisión los términos de la ley y de fundamentar lo mejor posible los elementos en que se basa la legislación fracasa precisamente por mantener la analogía con el mundo material (Nemer, 2022). Esta falla crea enormes lagunas que permiten eludir la ley en su capacidad reguladora central: la protección del ciudadano y del Estado brasileño.

En ningún lugar del texto de la ley se hace referencia a los términos "ciberespacio", "ecosistema digital" ni a ningún otro que se utilice en los documentos de gobernanza digital. El término "medios digitales" solo se utiliza en un lugar (al principio del primer artículo) y no aparece en ningún otro lugar. Por lo tanto, la ley se centra únicamente en los "datos" estáticos y su referencia geográfica (nacional). Al estar completamente obsoleta e incapaz incluso de definir —según la usabilidad contemporánea— los términos que aborda, la ley de 2018 fracasa estrepitosamente.

La gobernanza digital brasileña funciona con base en dos leyes (14129 de 29/03/2021 e Lei complementar 182 de 01/06/2021[45]), 8 decretos (10996, 10782, 10332, 10278, 9756, 9854, 9637, 9319, lançados entre 2018 e 2022 apenas), además de cinco ordenanzas y una resolución adicionales para el trienio 2013-2015, el documento principal, la Ley 14129, no contiene términos similares a los mencionados anteriormente, indicando en el inciso XI del artículo 4 que se utilizarán todos los conceptos de la LGPD de 2018.[46]. Esto conduce a un error teórico y epistemológico continuo al no lograr adaptarse a los significados del mundo digital en línea con lo que se produce a nivel mundial.

Lo curioso de esta ley es que, a pesar de utilizar un marco teórico insuficiente y deficiente para definir el mundo digital, se propone ser contemporánea en cuanto a la construcción de un "ciudadano digital", rompiendo con la cultura de la duplicación entre los mundos digital y material. En su Capítulo V, el Artículo 42 establece que "los órganos y entidades a que se refiere el Artículo 2 de esta Ley, a elección del usuario, podrán realizar todas las comunicaciones, notificaciones y citaciones por medios electrónicos". El peligro de este enfoque reside en que, sin un marco sólido para comprender y definir qué es el espacio digital en el siglo XXI, la ley da un paso más allá, haciendo innecesarios los procesos históricos en el mundo material (citaciones y notificaciones, por ejemplo) y sustituyéndolos por analogías en el mundo digital. No es necesario volver a discutir la incongruencia de esta analogía, pero es importante entender que el problemático camino de "modernizar" la legislación, al intentar "saltear" etapas importantes de regulación, comprensión y teorización, termina creando espacios de "no legislación" en el mundo digital que pueden usarse en detrimento de las mejores prácticas jurídicas[47]. Las iniciativas del gobierno de Bolsonaro se

44 BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei n.º 13.853, de 2019). Brasília: Presidência da República, 2018. Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Consultado en: 25 jul. 2025.

45 Apenas aqui mencionada por regular "startups" que comumente são formas de inovação digital no século XXI.

46 Até o fechamento deste artigo, o conteúdo da PL 2630 ainda não tinha sido votado na Câmara Federal.

47 Las dificultades para notificar citaciones para iniciar procesos judiciales son comunes en Brasil, llegando el propio Supremo Tribunal Federal a recurrir al cierre total de los servicios como forma de obligar a los titulares de las solicitudes a comparecer ante las autoridades judiciales brasileñas (Sant'Ana; Falcão; Vivas, 2022).
Este tipo de acción es inconsistente, ya que hay varias formas de burlar la prohibición, desde las populares VPNs (*Virtual Private Network*), hasta extensiones en navegadores que no pueden rastrearse, como *Thor*, que opera desde la *deep web*.

vuelven aún más preocupantes cuando se lee en el Decreto 10332 de 2020, en su anexo, el objetivo de "transformar el cien por cien de los servicios públicos en digitalizables para 2023". Sin resolver la cuestión central de qué es el ciberespacio y cómo se conceptualiza funcionalmente, parece que estamos construyendo una casa sobre la nada.

El "Plano Nacional da Internet das Coisas" (Decreto 9.854 de 25 de julho de 2019) es aún más deficiente e ineficaz para proteger a los ciudadanos brasileños y al Estado en el ámbito digital del siglo XXI. Por ejemplo, define IoT (*Internet of Things*) como

> [...] a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação [...] (artigo 2º, inciso I) (Brasil, 2019, *online*)[48].

En otras palabras, una vez más, no se hace referencia al sustrato conceptual-epistemológico necesario que constituye la representación de lo digital en nuestra época y sociedad. Se opera con una analogía paralela que contribuye a la incapacidad regulatoria, estableciendo el IoT como una "prestación de servicios" en un intento vago de conectar con los marcos regulatorios ya existentes y vigentes para el mundo material (Pani; Pandey, 2022).

La última referencia brasileña a cuestiones como "seguridad cibernética" y "defensa cibernética" data de 2018, con el decreto 9.637 de diciembre de 2018, firmado aún por Michel Temer. En este caso, preocupa la redacción del artículo 12 (modificado por el decreto 10641 de 2021), que otorga al GSI (Gabinete de Seguridad Institucional de la Presidencia de la República) la competencia sobre los temas de "seguridad de la información", dejando fuera a otros órganos e instancias de los procesos de toma de decisiones sobre el tema. A modo de énfasis, el artículo 13 de la misma ley afirma que el Ministerio de Defensa (instancia civil superior) debe "APOYAR" al GSI en lo que respecta a la ciberseguridad (Puyvelde; Brasntly, 2019). No es necesario argumentar a favor de la inversión de los sentidos de la participación política en estas decisiones, ya que el Gobierno de Bolsonaro siempre ha optado por la disminución y nunca por el aumento de la participación.

Si los marcos de gobernanza digital vigentes en Brasil son insuficientes y deficientes, y los ajustes implementados durante el período 2018-2022 bajo el gobierno de Bolsonaro son imprudentes, los intentos de avanzar en temas aún más contemporáneos rayan en el desastre total. En el tema de la inteligencia artificial, por ejemplo, tenemos las iniciativas de los proyectos de ley 5051/2019, 21/2020 y 872/2021[49]. Estos proyectos, que ni siquiera se han sometido a votación, no abordan en absoluto las cuestiones centrales sobre la inteligencia artificial que se estudian en la actualidad[50]. El proyecto 5051/2019 vuelve a exigir "la garantía de la privacidad y los datos personales" (SIC) y aboga por la sumisión decisoria

48 Traducción: "[...] La infraestructura que integra la provisión de servicios de valor agregado con las capacidades de conexión física o virtual de cosas con dispositivos basados en tecnologías de la información [...]" (artigo 2º, inciso I) (Brasil, 2019, *online*, traducción editorial).

49 Proyectos iniciados por el senador Styvenson Valentim (PODEMOS/RN), el diputado federal Eduardo Bismarck (PDT/CE) y el senador Vital do Rêgo (MDB/PB), respectivamente.

50 Los tres debates principales aquí giran en torno a la autonomía, la opacidad y la responsabilidad con respecto a la inteligencia artificial (Chesterman, 2021).

de la Inteligencia Artificial a la "supervisión humana". Esta postura es descabellada, ya que resulta imposible de ejecutar. Los microprocesos gestionados por la inteligencia artificial son demasiado numerosos como para siquiera pensar en cualquier sometimiento en *stricto sensu*, y la legislación es ineficaz incluso en *lato sensu*, ya que ni siquiera logra conceptualizar lo que sería la Inteligencia Artificial.

El Proyecto 21/2020, aunque algo más elaborado, pretende definir la Inteligencia Artificial como artículo 2

> [...] o sistema baseado em processo computacional que, a partir de um conjunto de objetivos definidos por humanos, pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo predições, recomendações, classificações ou decisões [...][51] (Brasil, 2020, *online*)[52].

En esta definición, se incluye incluso la programación terminal en las antiguas calculadoras científicas o las rutinas en aplicaciones populares como *Excel,* que ya es capaz de reconocer patrones externos y "predecir" y "recomendar" acciones. Ya en 1950, Alan Turing ofrecía una reflexión más precisa sobre el problema central de la inteligencia artificial, que es su relación (y no su sumisión) con el componente humano A PARTIR de sus concepciones históricas, políticas y sociales, preguntándose si tales reglas de mediación podrían considerarse "invariables en el tiempo" y, por lo tanto, inhumanas

> The idea of a learning machine may appear paradoxical to some readers. How can the rules of operation of the machine change? They should describe completely how the machine will react whatever its history might be, whatever changes it might undergo. The rules are thus quite time-invariant (Turing, 1950, p. 21)[53].

Cuestiones contemporáneas como la IA fuerte frente a la IA débil, la aplicabilidad de estas entidades y el debate sobre los límites y las diferencias entre el *Deep Learning* y *Machine Learning* ni siquiera parecen haberse planteado, y cuestiones completamente imposibles como la "búsqueda de la neutralidad" (art. 5, apartado 4) se describen allí como "principios" operativos.

La discrepancia entre lo que se debate a nivel internacional (que, en cierto modo, representa una mayor adecuación al estado actual del debate) y lo que Brasil aún está en

---

51 La definición es una copia casi textual del artículo 3 de un documento de la Unión Europea (*Proposal for a Regulation of the European Parliament and of the council Laying down Harmonised Rules on Artificial Intelligence and amending certain Union legislative acts*) Es necesario entender que este documento es el resultado de 38 páginas de discusión previa y se refiere a un Anexo (como recurso definitorio) que se refiere objetivamente a "*Machine Learning*", "*Deep Learning*", "Sistemas de máquinas deductivos e inductivos" y "enfoques estadísticos". El autor del proyecto ignoró una parte esencial del documento e hizo una "copia", cuyo resultado es la imposibilidad de cualquier avance hacia una buena regulación.

52 Traducción: "[...] un sistema basado en un proceso computacional que, a partir de un conjunto de objetivos definidos por el ser humano, puede, mediante el procesamiento de datos e información, aprender a percibir e interpretar el entorno externo, así como interactuar con él, realizando predicciones, recomendaciones, clasificaciones o decisiones [...]" (Brasil, 2020, *online*, traducción editorial).

53 Traducción: "La idea de una máquina que aprende puede parecer paradójica para algunos lectores. ¿Cómo pueden cambiar las reglas de funcionamiento de la máquina? Deben describir completamente cómo reaccionará la máquina, sea cual sea su historial, sean cuales sean los cambios que pueda sufrir. Por lo tanto, las reglas son bastante invariables en el tiempo" (Turing, 1950, p. 21 traducción editorial).

proceso de debate legislativo se aprecia claramente al comparar lo que el Proyecto de Ley 872 de 2021 (también sobre inteligencia artificial) pretende regular con la iniciativa de la Unión Europea sobre el mismo tema. En Brasil, la redacción del Artículo 2 del mencionado proyecto de ley es (Brasil, 2021, *online*)[54]:

> A disciplina do uso da Inteligência Artificial tem como fundamento:
>
> I. O respeito à ética, aos direitos humanos, aos valores democráticos e à diversidade;
> II. A proteção da privacidade e dos dados pessoais;
> III. A transparência, a confiabilidade e a segurança dos sistemas;
> IV. A garantia da intervenção humana, sempre que necessária.

El documento elaborado por la Unión Europea[55] Tiene más de 108 páginas y además hace referencia a otros anexos como forma de representar el pensamiento legislativo del momento, y señala que el objetivo del reglamento es:

> e) (a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;
>
> f) (a) prohibitions of certain artificial intelligence practices;
>
> g) (b) specific requirements for high-risk AI systems and obligations for operators of such systems;
>
> h) (c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;
>
> i) (d) rules on market monitoring and surveillance (European Commission, 2021, p. 38)[56]

Mientras que la legislación brasileña aún se centra en los "datos" y enumera valores que, si bien son esenciales, están definidos de forma vaga e ineficaz (como "ética", "derechos humanos" y "diversidad"), su contraparte europea ya trabaja en una lista definitiva de prohibiciones para el uso de sistemas de IA, obligaciones para los operadores y normas de transparencia con requisitos específicos para la evaluación de riesgos en el uso de dichas tecnologías. La comparación que se hace aquí puede parecer incorrecta si se considera la idea de que la Unión Europea opera con la burocracia de una organización supranacional compuesta en gran medida por los resultados de las burocracias de 27 países, mientras que

---

54 Traducción: La disciplina de utilización de la Inteligencia Artificial se basa en:
I. Respeto a la ética, los derechos humanos, los valores democráticos y la diversidad;
II. La protección de la privacidad y de los datos personales;
III. La transparencia, confiabilidad y seguridad de los sistemas;
IV. La garantía de la intervención humana, siempre que sea necessária (Brasil, 2021, *online,* traducción editorial).

55 EUROPEAN COMMISSION. **2021/0106 (COD)**. Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence act) and amending certain union legislative acts. Brussels: European Commission, 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Consultado en: 28 jul. 2025.

56 Traducción editorial: "a) normas armonizadas para la comercialización, la puesta en servicio y el uso de sistemas de inteligencia artificial («sistemas de IA») en la Unión;
a) prohibiciones de determinadas prácticas de inteligencia artificial;
b) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;
c) normas armonizadas de transparencia para los sistemas de IA destinados a interactuar con personas físicas, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica, y los sistemas de IA utilizados para generar o manipular contenidos de imagen, audio o vídeo;
d) normas sobre seguimiento y vigilancia del mercado" (European Commission, 2021, p. 38, traducción editorial).

el esfuerzo brasileño se limita a un solo país. Sin embargo, el argumento aquí no se centra en comparar los recursos financieros ni el número de personas involucradas en el diseño de los proyectos, sino en los propios conceptos. La distancia entre el debate brasileño y el conocimiento establecido, así como las premisas para debatir el tema y la necesidad de protección regulatoria, es evidente.

El proyecto brasileño ignora los avances actuales en la materia y carece de una conceptualización mínimamente operativa, además de proponer regulaciones sobre puntos imposibles (como “garantizar la intervención humana”) o irrelevantes (como la “protección de datos personales”). Al mismo tiempo, el proyecto —que, cabe destacar, ni siquiera ha sido votado en el Parlamento— ya es insuficiente e incapaz de responder a las necesidades sociales actuales en relación con el mundo digital (Silva, 2021).

CONCLUSIÓN

La soberanía digital es un término completamente diferente de la “soberanía” tal como se entendía en el siglo XX, derivada del proceso de resignificación histórica desde Jean Bodin. Mientras que el antiguo concepto de soberanía se refería a la vigilancia, el control, el castigo y la tributación, y en última instancia a la capacidad de controlar el destino de cuerpos y bienes dentro de ciertas fronteras, la soberanía digital no permite la presencia de tales referencias.

Si la analogía con el “espacio” material, que, como he demostrado, guió la comprensión humana de lo “digital”, no es suficiente para comprender las funcionalidades, los límites y las posibilidades del mundo digital, necesitamos buscar una nueva forma de comprender y generar significado, capaz de ordenar nuestros sentidos para que podamos comprender y construir sociedades basadas en las transformaciones del siglo XXI.

Este artículo propone un cambio en el significado de la comprensión del mundo digital: de la antigua analogía con un “espacio” que ahora es digital, a una analogía con el “tiempo”. Los recientes intentos de cambiar la conceptualización del mundo digital, observados en todo el mundo, muestran no solo la incomodidad con la analogía de lo digital con el “espacio” físico, sino también esfuerzos epistemológicos por transformar esta comprensión. El consenso actual es el término “ecosistema digital”. El significado de ecosistema incorpora la idea de movimiento, así como correlaciones y sinergias que no se entienden únicamente a través de su sentido utilitario. En un ecosistema, toda existencia es a la vez causa y consecuencia de las existencias con las que comparte tiempo y espacio.

Entender el mundo digital desde la perspectiva del tiempo significa replantearse las formas de soberanía. Implica pensar en nuevos objetos que deben ser protegidos por el Estado. Este camino ya ha sido recorrido por las llamadas “*Big Tech”*. Mientras los Estados siguen legislando (guiados por analogías disfuncionales) con el fin de proteger, por ejemplo, la privacidad de los usuarios y la propiedad intelectual de los grandes constructos digitales, los modelos de negocio digitales actuales se preocupan poco o nada por estos marcos. En realidad, ni *Meta*, ni *Alphabet*, ni siquiera la empresa matriz de *Twitter* tienen hoy en día ningún interés en conocer (retener, conservar o divulgar) los datos que identifican al usuario en el mundo material (nombre, números de documentos, etc.). Esa información no es importante para el modelo actual. El enfoque de la rentabilidad y, por lo tanto, el objetivo de la apropiación que las grandes empresas tecnológicas llevan a cabo hoy en día es el de los datos “de paso”. Desidentificada, la brutal cantidad de datos que se pueden recopilar en 24 horas dentro del territorio brasileño es el verdadero sentido de la acumulación capitalista de los negocios del mundo digital actual. Estos datos permiten producir potentes modelos estadísticos de comportamiento y consumo, y sirven para comprender los patrones de aprendizaje humano, los sentidos de la toma de decisiones políticas, los conjuntos de referentes lingüísticos que se utilizarán sobre un tema determinado y, en última instancia, todo ello acaba siendo materia prima para el desarrollo de algoritmos e inteligencia artificial.

Lo que se desprende del artículo es que ninguna de estas funciones está siendo objeto de protección estatal. Ni desde una perspectiva educativa y social (como forma de proteger a la sociedad de las transformaciones digitales), ni siquiera desde una perspectiva de mercado, ya que estos datos se siguen utilizando como si no fueran producidos por nadie y su propiedad se transfiere a quienes los recopilan (las plataformas) sin compensación alguna para el Estado ni la sociedad.

En la transición del siglo XX al XXI, los Estados, incapaces de comprender a fondo el mundo digital (en gran medida debido al uso de la desafortunada analogía con el mundo material), no percibieron el surgimiento de las *"Big Tech"*. Empresas capitalistas que dominan, explotan, controlan y manipulan el mundo digital, ejerciendo de facto un poder político y económico. Los efectos del ejercicio de estos poderes se extienden no solo al tejido digital, sino también al mundo material, que, a lo largo del siglo XXI, se ha convertido cada vez más en un cómplice del mundo digital. Esta novedad ha dejado a los Estados indefensos ante los cambios y transformaciones en curso. Particularmente en lo que se refiere al ejercicio de las instituciones políticas y jurídicas.

Reflexionar sobre la soberanía digital se convierte, por lo tanto, en una de las mayores necesidades del siglo XXI. Pensar en el mundo digital desde sus propios conceptos y funcionalidades es, hoy en día, la mayor necesidad de un Estado. Sin embargo, pocos Estados están ya en condiciones de llevar a cabo estas acciones. Este artículo analizó algunos de los intentos de Estados Unidos y Brasil, y ni siquiera los estadounidenses, referentes sociales, políticos y económicos a lo largo del siglo XX, están hoy a la vanguardia del proceso de comprensión y dominio del mundo digital.

El análisis de las trayectorias legislativas de Brasil y Estados Unidos plantea numerosas inquietudes, ya que ambos siguen operando con base en la analogía digital-material, que ya ha demostrado ser insuficiente. Sin embargo, mientras que en Estados Unidos ya se observa al menos una transformación conceptual en los marcos de comprensión y legislación del mundo digital, en Brasil estamos muy por detrás de lo que hoy se considera el estado del arte para conocer, operar y regular el mundo digital. El análisis de los proyectos de ley en trámite en el Congreso Nacional pone de manifiesto esta preocupación. La conclusión del análisis sugiere que deberíamos empezar a pensar en cambiar la analogía básica para comprender el mundo digital. Ya no se trata de un "espacio" digital donde debemos defender sus puntos de contacto con el mundo físico (información de identificación del usuario, documentos, direcciones, etc.), sino que debemos entender lo digital como TIEMPO. El tiempo que una persona pasa conectada a la red digital debe ser objeto de protección social, política y económica. Cada vez más, las personas están conectadas al mundo digital y durante periodos cada vez más largos, generando más valor sin recibir nada a cambio.

Pensar en cambiar la analogía implica repensar todos los marcos legales de protección, tributación, acción y prohibición. La Unión Europea, por ejemplo, está considerando la creación de un impuesto anual que las empresas que operan en el mundo digital pagarían por el uso

del tiempo social de la población bajo su protección[57]. Al igual que ocurrió con los espectros y bandas electromagnéticas, el tiempo de los ciudadanos digitales es ahora un espacio de imposición.

De igual manera, las protecciones que el Estado debe ofrecer deben pasar de una referencia espacial a una temporal. Ya no es apropiado preguntar dónde se ubica esta o aquella empresa que opera en el mundo digital. El enfoque debe centrarse en el período en el que opera en la vida de los ciudadanos. Dado que el mundo digital ha dejado de ser una red externa para convertirse en una parte integral de nuestras vidas (mediante el uso incesante de computadoras, tabletas, teléfonos celulares, etc.), es imposible limitarse a analogías del siglo XXI.

Dado que el concepto de "tiempo" es intangible comparado con el de "espacio", los Estados quedan atrapados en el problema de definir el mundo digital y cómo ser funcionales en la protección de los derechos que históricamente han estado obligados a proteger. El avance de las tecnologías es tan rápido y eficaz en la transformación de las relaciones sociales y económicas que el mismo tiempo del que dispone el Estado democrático para abordar las cuestiones planteadas ya lo vuelve inerte para resolverlas.

Debido a este problema, varios países están pasando de los intentos de crear leyes a las llamadas regulaciones "soft", con la formación de consejos y comités de gestión, a la vez que buscan capacitar y educar a su población para el nuevo mundo digital (alfabetización digital). Cualquier intento actual del Estado por operar en el mundo digital que no se centre esencialmente en el concepto de tiempo, la idea de la existencia de ciudadanos digitales y un amplio esfuerzo en educación digital ya se está volviendo obsoleto debido a la velocidad del desarrollo tecnológico.

En lugar de proteger direcciones, nombres y documentos, necesitamos salvaguardar todo el tiempo que un ciudadano está conectado al mundo digital. Dado que esto es imposible sin el compromiso de las empresas que operan en el mundo digital, es más viable trabajar en el otro extremo: la educación del ciudadano digital. Este cambio es tan drástico que podría decirse que la "soberanía digital" hoy en día se logra mediante la educación, la investigación y la tecnología, no mediante la legislación, el control y el castigo. Y dado que las transformaciones digitales están causando daños significativos al mundo material (violencia urbana, terrorismo digital, violencia sexual, fascismo, destrucción de democracias) y creando una nueva forma de colonialismo, el Estado debe encontrar la manera de garantizar que las ganancias de estas empresas financien todo el proceso de reeducación y la adaptación de las poblaciones analógicas al mundo digital.

Lo preocupante es que Brasil está muy rezagado en este cambio, e incluso en la comprensión de lo que es el mundo digital. Esto implica que entramos al siglo XXI como una nación subyugada, no soberana. Como ciudadanos inconscientes de los peligros del

57 Véase el considerando número 101 de la Ley de Servicios Digitales (DSA) de la Unión Europea. En principio, se cobrarán tasas (denominadas "tasas de supervisión") para subvencionar los costes que supone para los Estados mantener las estructuras de supervisión y reparación de daños derivados de las actividades de explotación del mundo digital europeo. Sin embargo, ya se está estudiando la posibilidad de convertir esto en una nueva forma de tributación (véase el considerando 112).

mundo digital, incapaces de disfrutar o transformar el mundo que se transforma en el siglo XXI. Dado que estas transformaciones no se pueden bloquear ni retrasar, se necesita un esfuerzo urgente para *"catching up"* y no quedarnos en una posición medieval cuando el mundo entero ya está altamente industrializado. Esta es solo una analogía que podría explicar la situación actual en Brasil.

REFERENCIAS

ANDERSON, P. **Linhagens do estado absolutista**. 3. ed. São Paulo: Brasiliense, 1995.

BIDDLE, S. The Intercept. **Facebook engineers**: we have no idea where we keep all your personal data. 7 Sept. 2022. Disponible en: https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/. Consultado en: 24 jul. 2025.

BODIN, J. **Six books of the commonwealth**. Oxford: Liberty Library of Constittional classics, 2009.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília: Presidência da República, 2020.

BRASIL. **Decreto nº 10.641, de 2 de março de 2021**. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília: Presidência da República, 2021.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília: Presidência da República, 2018.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Brasília: Presidência da República, 2019.

BRASIL. **Lei complementar nº 182, de 1º de junho de 2021**. Institui o marco legal das startups e do empreendedorismo inovador; e altera a Lei nº 6.404, de 15 de dezembro de 1976, e a Lei Complementar nº 123, de 14 de dezembro de 2006. Brasília: Congresso Nacional, 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Consultado en: 24 jul. 2025.

BRASIL. **Lei nº 14.129, de 29 de março de 2021.** Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília: Presidência da República, 2021.

BRASIL. **Projeto de Lei n° 21, de 2020.** Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2020.

BRASIL. **Projeto de lei n° 2630, de 2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: Congresso Nacional, 2020.

BRASIL. **Projeto de lei nº 5051/2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília: Senado Federal, 2019.

BRASIL. **Projeto de lei nº 872/2021**. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2021.

BRATTON, B. H. **The stack**: on software and sovereignty. Londres: MIT Press, 2016.

CAMPREGHER, G. A terra é redonda: eppur si muove. **Moedas digitais** – que dinheiro é esse? 30 jun. 2025. Disponible en: https://aterraeredonda.com.br/moedas-digitais-que-dinheiro-e-esse/. Consultado en: 25 jul. 2025.

CHESTERMAN, S. **We, the robots?** regulating artificial intelligence and the limits of the law. Cambridge: Cambridge University Press, 2021.

CHIGNOLA, S. Homo homini trigris: Thomas Hobbes and the global images of sovereignty. **Philosophy and Social Criticism**, [*s. l.*], v. 48, n. 5, p. 726-754, 2021.

COMITE DAS REGIÕES EUROPEU. **Relatório do grupo de alto nível para a democracia europeia**. Bruxelas: União Europeia, 2022. Disponible en: https://cor.europa.eu/en/news/Pages/Report-of-the-High-Level-Group-on-European-Democracy.aspx. Consultado en: 17 ago. 2025.

EISENBERG, J.; CEPIK, M. (org.). **Internet e política:** teoria e prática da democracia eletrônica. Belo Horizonte: Editora UFMG, 2002.

EUROPEAN COMMISSION. **2021/0106 (COD)**. Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence act) and amending certain union legislative acts. Brussels: European Commission, 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Consultado en: 28 jul. 2025.

EUROPEAN UNION. **EUR-Lex**. 27 Oct. 2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014. Consultado en: 24 jul. 2025.

FANG, B. **Cyberespace sovereignty:** reflections on building a community of common future in cyberspace. Pequim: Springer, 2018.

GIBSON, W. **Neuromancer**. São Paulo: Aleph, 1984.

HOBBES, T. **Leviathan**. London: Green Dragon, 1651.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. ICANN. **Policy development**: how domain name system policy is developed, and how you can get invoved. [*S. l.*]: ICANN, 2021. Disponible en: https://www.icann.org/en/system/files/files/icann-policy-development-report-16jun21-en.pdf. Consultado en: 24 jul. 2025.

KANT, I. **À paz perpétua:** um projeto filosófico. 2. ed. Petrópolis: Vozes, 2020.

KAZEEM, Y. **The cost of internet access dropped everywhere in the world last year**—except in Africa. 21 Mar. 2019. Disponible en: https://finance.yahoo.com/news/cost-internet-access-dropped-everywhere-112424571.html. Consultado en: 24 jul. 2025.

KOKAS, A. **Trafficking data:** how China is winning the battler for digital sovereignty. Nova Iorque: Oxford University Press, 2023.

MCCALLUM, S. Meta settles Cambridge Analytica scandal case for $725m. **BBC**. 23 Dec. 2022. Disponible en: https://www.bbc.com/news/technology-64075067. Consultado en: 24 jul. 2025.

MOSCO, V. **Becoming digital**: toward a post-internet society. Londres: Emerald Publishing Limited, 2017.

MOSCO, V. **Digital sublime**: myth, power and cyberspace. Londres: MIT Press, 2004.

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES. NICCS. Cybersecurity and career resources. **Vocabulary**. c2025. Disponible en: https://niccs.cisa.gov/cybersecurity-career-resources/glossary#C. Consultado en: 24 jul. 2025.

NEMER, D. **Tecnologia do oprimido:** desigualdade o mundano digital nas favelas do Brasil. Vitória: Editora Milfontes, 2022.

NORTON, W. B. DrPeering international. **Internet transit prices** - historical and projected. c2014. Disponible en: https://drpeering.net/white-papers/Internet-Transit-Pricing-Historical-And-Projected.php. Consultado en: 25 jul. 2025.

ONE HUNDRED FOURTH CONGRESS OF THE UNITED STATES OF AMERICA. **Telecommunication services**. Begun and held at the City of Washington on Wednesday, the third day of January, one thousand nine hundred and ninety-six An Act To promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies. Washington: Congress, 1996. Disponible en: https://transition.fcc.gov/Reports/tcom1996.pdf. Consultado en: 25 jul. 2025.

PANI, S. K.; PANDEY, M. (ed.). **Internet of things:** enabling technologias, security and social implications. Singapura: Springer, 2022.

PUYVELDE, D.; BRANTLY, A. **Cybersecurity:** politics, governance and conflict in cyberspace. Medford: Polity Press, 2019.

SANT'ANA, J.; FALCÃO, M.; VIVAS, F. **G1**. **Politíca**. Moraes determina bloqueio do aplicativo de mensagens Telegram em todo o Brasil. 18 mar. 2022. Disponible en: https://g1.globo.com/politica/noticia/2022/03/18/moraes-determina-bloqueio-do-aplicativo-de-mensagens-telegram-em-todo-o-brasil.ghtml. Consultado en: 24 jul. 2025.

SCHMIDT, C. **Political theology:** four chapters on the concept of sovereignty. Chicago: Chicago University Press, 2005.

SILVA, T. **Racismo algoritmico:** inteligência artificial e discriminação nas redes digitais. São Paulo: Edições SESC, 2021.

TURING, A. Computing machinery and intelligence. **Mind**, [*s. l.*], v. 49, n. 236, p. 433-460, 1950.

U. S. SENATE COMMITTEE ON THE JUDICIARY. **Senate judiciary committee releases testimony of twitter whistleblower peiter "Mudge" Zatko**. 13 Sept. 2002. Disponible en: https://www.judiciary.senate.gov/press/dem/releases/senate-judiciary-committee-releases-testimony-of-twitter-whistleblower-peiter-mudge-zatko. Consultado en: 24 jul. 2025.

UNIÃO EUROPEIA. Parlamento Europeu. Conselho da União Europeia. Regulamento (UE) 2022/2065, de 19 de outubro de 2022. Relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). **Jornal Oficial da União Europeia**, L 277, p. 1–102, 27 out. 2022. Disponible en: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065. Consultado en: 24 jul. 2025.

UNITED STATES. Court of appeals for the Ninth Circuit. Petition for a writ of certiorari filed. **No. 21-1333**. Julgado em: 22/06/2021. Disponible en: https://www.supremecourt.gov/docket/docketfiles/html/public/21-1333.html. Consultado en: 25 jul. 2025.

UNITED STATES. **The National Estrategy to secure cyberspace**. Washington: The White House, 2003. Disponible en: https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf. Consultado en: 24 jul. 2025.

WENDT, A. **Quantum mind and social science:** unifying physical and social ontology. Cambridge: Cambridge University Press, 2015.

ZUBOFF, S. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Nova Iorque: Perseus Books, 2019.