Rev. secr. Trib. perm. revis. 2026, Año 14, Nº 23, e568.
ISSN 2304-7887 (en línea) - ISSN 2307-5163 (impreso)
DOI: 10.16890/rstpr.a14.n23.e568
Artículo original/Artigo original/ Original article/Article original

La paradoja de seguridad y libertad en la era digital: un análisis crítico desde perspectivas biopolíticas y filosóficas

O paradoxo da segurança e da liberdade na era digital: uma análise crítica a partir de perspetivas biopolíticas e filosóficas

The Paradox of Security and Freedom in the Digital Age: A Critical Analysis from Biopolitical and Philosophical Perspectives

Le paradoxe de la sécurité et de la liberté à l'ère numérique : une analyse critique sous l'angle biopolitique et philosophique

Fernando Ramos-Zaga *

Universidad César Vallejo, Lima, Perú.

Resumen: La tensión entre seguridad y libertad constituye uno de los dilemas fundamentales de las sociedades contemporáneas, intensificado exponencialmente por el advenimiento de tecnologías digitales de vigilancia masiva. Este trabajo examina críticamente esta paradoja desde marcos teóricos biopolíticos y filosóficos, argumentando que las arquitecturas digitales contemporáneas no simplemente equilibran seguridad y libertad, sino que reconfiguran radicalmente las modalidades mismas del poder gubernamental y la subjetividad individual. A través de un análisis que integra los conceptos foucaultianos de biopolítica y gubernamentalidad con perspectivas contemporáneas sobre vigilancia digital, se sostiene que el paradigma securitario actual opera mediante mecanismos de control preventivo que trascienden las formas disciplinarias tradicionales. La investigación explora

E-mail:fernandozaga@gmail.com

Recibido: 30/09/2025. Aceptado: 18/02/2026.

Editor responsable: Natasha Suñé . Secretaría del Tribunal Permanente de Revisión, Asunción, Paraguay.

cómo algoritmos predictivos, sistemas de reconocimiento facial y plataformas de datificación masiva construyen regímenes de visibilidad donde la libertad es simultáneamente proclamada y erosionada. Se argumenta que esta paradoja no representa una contradicción accidental sino una característica estructural del capitalismo de vigilancia, donde la extracción de datos biométricos y comportamentales constituye tanto el medio de control como el fundamento económico de plataformas digitales. Las conclusiones sugieren que resolver esta tensión requiere repensar fundamentalmente las categorías políticas heredadas de la modernidad temprana, desarrollando marcos normativos capaces de proteger la autonomía individual sin sucumbir a ilusiones de transparencia total o seguridad absoluta.

Resumo: A tensão entre segurança e liberdade constitui um dos dilemas fundamentais das sociedades contemporâneas, intensificado exponencialmente pelo advento das tecnologias digitais de vigilância em massa. Este trabalho examina criticamente esse paradoxo a partir de marcos teóricos biopolíticos e filosóficos, argumentando que as arquiteturas digitais contemporâneas não apenas equilibram segurança e liberdade, mas reconfiguram radicalmente as próprias modalidades do poder governamental e da subjetividade individual. Através de uma análise que integra os conceitos foucaultianos de biopolítica e governamentalidade com perspetivas contemporâneas sobre vigilância digital, sustenta-se que o paradigma securitário atual opera por meio de mecanismos de control preventivo que transcendem as formas disciplinares tradicionais. A pesquisa explora como algoritmos preditivos, sistemas de reconhecimento facial e plataformas de datificação em massa constroem regimes de visibilidade onde a liberdade é simultaneamente proclamada e corroída. Argumenta-se que este paradoxo não representa uma contradição acidental, mas sim uma característica estrutural do capitalismo de vigilância, onde a extração de dados biométricos e comportamentais constitui tanto o meio de control como também o fundamento económico das plataformas digitais. As conclusões sugerem que resolver essa tensão requer repensar fundamentalmente as categorias políticas herdadas da modernidade inicial, desenvolvendo marcos normativos capazes de proteger a autonomia individual sem sucumbir a ilusões de transparência total ou segurança absoluta.

Abstract: The tension between security and freedom constitutes one of the fundamental dilemmas of contemporary societies, exponentially intensified by the advent of mass digital surveillance technologies. This work critically examines this paradox from biopolitical and philosophical theoretical frameworks, arguing that contemporary digital architectures do not simply balance security and freedom but radically reconfigure the very modalities of governmental power and individual subjectivity. Through an analysis that integrates Foucauldian concepts of biopolitics and governmentality

with contemporary perspectives on digital surveillance, it is argued that the current security paradigm operates through preventive control mechanisms that transcend traditional disciplinary forms. The research explores how predictive algorithms, facial recognition systems, and mass datification platforms construct visibility regimes where freedom is simultaneously proclaimed and eroded. It is argued that this paradox represents not an accidental contradiction but a structural feature of surveillance capitalism, where the extraction of biometric and behavioral data constitutes both the means of control and the economic foundation of digital platforms. The conclusions suggest that resolving this tension requires fundamentally rethinking the political categories inherited from early modernity, developing normative frameworks capable of protecting individual autonomy without succumbing to illusions of total transparency or absolute security.

Résumé : La tension entre sécurité et liberté constitue l'un des dilemmes fondamentaux des sociétés contemporaines, intensifié de manière exponentielle par l'avènement des technologies numériques de surveillance de masse. Cet article examine de manière critique ce paradoxe à partir de cadres théoriques biopolitiques et philosophiques, en soutenant que les architectures numériques contemporaines ne se contentent pas d'équilibrer sécurité et liberté, mais qu'elles reconfigurent radicalement les modalités mêmes du pouvoir gouvernemental et de la subjectivité individuelle. À travers une analyse qui intègre les concepts foucaldiens de biopolitique et de gouvernementalité avec des perspectives contemporaines sur la surveillance numérique, il est soutenu que le paradigme sécuritaire actuel fonctionne grâce à des mécanismes de contrôle préventif qui transcendent les formes disciplinaires traditionnelles. La recherche explore comment les algorithmes prédictifs, les systèmes de reconnaissance faciale et les plateformes de datification massive construisent des régimes de visibilité où la liberté est simultanément proclamée et érodée. Il est avancé que ce paradoxe ne représente pas une contradiction accidentelle, mais une caractéristique structurelle du capitalisme de surveillance, où l'extraction de données biométriques et comportementales constitue à la fois le moyen de contrôle et le fondement économique des plateformes numériques. Les conclusions suggèrent que pour résoudre cette tension, il faut repenser fondamentalement les catégories politiques héritées du début de la modernité, en développant des cadres normatifs capables de protéger l'autonomie individuelle sans succomber aux illusions d'une transparence totale ou d'une sécurité absolue.

Palabras clave: Biopolítica, Vigilancia digital, Gubernamentalidad, Libertad, Seguridad, Capitalismo de vigilancia.

Palavras-chave: Biopolítica, Vigilância digital, Governamentalidade, Liberdade, Segurança, Capitalismo de vigilância.

Keywords: Biopolitics, Digital surveillance, Governmentality, Freedom, Security, Surveillance capitalism.

Mots clés : Biopolitique, Surveillance numérique, Gouvernementalité, Liberté, Sécurité, Capitalisme de surveillance.

1. INTRODUCCIÓN

Las sociedades contemporáneas enfrentan una paradoja fundamental que define el carácter de la existencia política en el siglo XXI. Por un lado, el discurso dominante proclama la expansión sin precedentes de libertades individuales, autonomía personal y derechos humanos universales. Por otro, estas mismas sociedades han construido infraestructuras de vigilancia de alcance, sofisticación y penetración inimaginables para cualquier régimen autoritario del pasado. Esta contradicción aparente no constituye simplemente un efecto secundario no deseado del progreso tecnológico, sino que representa una característica estructural de las formas contemporáneas de gubernamentalidad que demanda examen crítico riguroso[1].

La promesa de seguridad absoluta se ha convertido en el imperativo categórico que justifica la erosión sistemática de espacios de privacidad, anonimato y autonomía previamente considerados inviolables. Desde los ataques terroristas de inicios del milenio hasta las crisis sanitarias globales recientes, cada emergencia ha servido como catalizador para la implementación de tecnologías de monitoreo cada vez más invasivas, presentadas invariablemente como medidas temporales y excepcionales que, sin embargo, se sedimentan como características permanentes del paisaje político[2]. La normalización de esta vigilancia ubicua plantea interrogantes filosóficos profundos sobre la naturaleza misma de la libertad en condiciones de visibilidad total y sobre los límites legítimos del poder estatal en democracias liberales.

El concepto foucaultiano de biopolítica proporciona un marco analítico particularmente fértil para comprender esta reconfiguración. Foucault argumentó que las sociedades modernas se caracterizan por un desplazamiento desde formas soberanas de poder, centradas en el derecho de muerte, hacia formas biopolíticas enfocadas en la administración de la vida poblacional[3]. El poder ya no opera primariamente mediante la amenaza de violencia contra cuerpos individuales, sino a través de la gestión estadística de poblaciones, la optimización de procesos vitales y la modulación de conductas mediante incentivos y arquitecturas de elección. Las tecnologías digitales contemporáneas representan la culminación de esta lógica biopolítica,

1 FOUCAULT, Michel. *The history of sexuality, Volume 1: An introduction*. 1978. New York: Pantheon Books, pp. 136-140; LYON, David. *Surveillance society: Monitoring everyday life*. Open University Press. 2001, pp. 1-5.

2 AGAMBEN, Giorgio. *State of exception*. Chicago: University of Chicago Press, 2005, pp. 1-10.

3 FOUCAULT, Michel. *The history of sexuality* . Op.cit. p. 140-143

permitiendo formas de monitoreo, predicción y modulación conductual que operan en tiempo real y a escala masiva[4].

Sin embargo, la digitalización de la vigilancia introduce transformaciones cualitativas que exceden los marcos analíticos desarrollados para sociedades disciplinarias del siglo XX. Los algoritmos predictivos no simplemente observan comportamientos pasados, sino que construyen perfiles probabilísticos de acciones futuras, interviniendo preventivamente antes de que transgresiones potenciales se materialicen[5]. Esta lógica actuarial transforma la presunción de inocencia en un cálculo perpetuo de riesgo donde todos los ciudadanos son simultáneamente sospechosos y protegidos, vigilantes y vigilados. La datificación exhaustiva de la existencia cotidiana genera registros permanentes de movimientos, preferencias, relaciones e incluso estados emocionales, construyendo lo que Zuboff ha denominado capitalismo de vigilancia, donde la experiencia humana misma se convierte en materia prima para extracción comercial[6].

La presente investigación se fundamenta en un paradigma cualitativo de carácter analítico-descriptivo, empleando el método dogmático-jurídico en convergencia con la hermenéutica crítica. A través de una revisión de literatura especializada y un análisis dialéctico de fuentes documentales contemporáneas, el estudio descompone las racionalidades biopolíticas subyacentes a las infraestructuras de vigilancia. Dicho enfoque permite no solo describir el fenómeno tecnológico, sino evaluar reflexivamente la erosión de las categorías normativas tradicionales frente al avance de la gubernamentalidad algorítmica, asegurando el rigor interpretativo necesario para la propuesta de nuevos marcos regulatorios.

Esta investigación argumenta que la tensión entre seguridad y libertad no puede resolverse mediante ajustes incrementales o equilibrios pragmáticos dentro de los marcos conceptuales existentes. Por el contrario, se sostiene que la arquitectura misma de las tecnologías digitales contemporáneas embebidas en estructuras de capitalismo de vigilancia genera formas de poder que operan mediante la producción de subjetividades particulares, donde la libertad es experimentada precisamente a través de mecanismos que simultáneamente la constriñen. Los individuos son interpelados como consumidores soberanos ejerciendo elecciones autónomas mientras algoritmos invisibles construyen las arquitecturas de esas elecciones, un fenómeno que Han ha caracterizado como psicopolítica[7].

4 DELEUZE, Guilles. "Postscript on the societies of control". *October*, 1992, vol. 59, pp. 3-7.

5 AMOORE, Louise. *The politics of possibility: Risk and security beyond probability*. Durham: Duke University Press, 2013, pp. 7-12.

6 ZUBOFF, Shoshana. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs, 2019, pp. 8-15.

7 HAN, Byung-Chul. *Psychopolitics: Neoliberalism and new technologies of power*. Verso Books. 2014, pp. 1-4.

La relevancia de esta investigación reside en su capacidad para trascender la mera descripción fenomenológica de la técnica, proponiendo una actualización crítica de las categorías del pensamiento político que han quedado rezagadas ante la celeridad de la innovación digital. El impacto del estudio se proyecta en la desarticulación de la pretendida 'neutralidad algorítmica', aportando un marco analítico que permite identificar la transmutación de la seguridad en dominación biopolítica. Al proponer criterios de 'explicabilidad humana' e 'inalienabilidad biométrica', la investigación busca impactar directamente en la praxis legislativa contemporánea, proveyendo los fundamentos necesarios para revertir la erosión de la esfera privada en las democracias liberales.

El objetivo de este análisis es triple. Primero, examinar los fundamentos teóricos de la tensión entre seguridad y libertad en el pensamiento político moderno, rastreando cómo esta dialéctica ha sido conceptualizada desde Hobbes hasta Foucault. Segundo, analizar las transformaciones específicas introducidas por tecnologías digitales de vigilancia, enfocándose particularmente en algoritmos predictivos, reconocimiento biométrico y datificación masiva. Tercero, evaluar críticamente las justificaciones filosóficas y políticas ofrecidas para estas prácticas, argumentando que el paradigma securitario contemporáneo requiere repensamiento fundamental de categorías políticas heredadas. A través de este examen, se busca contribuir a desarrollar marcos normativos más adecuados para sociedades donde la distinción entre seguridad y control, entre protección y dominación, se ha vuelto inquietantemente difusa.

2. FUNDAMENTOS FILOSÓFICOS DE LA TENSIÓN ENTRE SEGURIDAD Y LIBERTAD

La relación entre seguridad y libertad constituye uno de los problemas perennes del pensamiento político occidental, manifestándose de formas distintivas en diferentes tradiciones teóricas. En el contractualismo hobbesiano, esta tensión encuentra su formulación paradigmática. Hobbes argumentó que, en el estado de naturaleza, caracterizado por guerra de todos contra todos, los individuos poseen libertad absoluta, pero carecen de seguridad. El contrato social representa precisamente el intercambio mediante el cual los sujetos ceden libertades naturales ilimitadas al soberano a cambio de protección contra la violencia recíproca[8]. Esta formulación establece seguridad y libertad como magnitudes inversamente proporcionales, donde incrementos en una necesariamente implican disminuciones en la otra.

Sin embargo, la tradición liberal desarrollada por Locke y refinada por Mill rechazó esta conceptualización, argumentando que seguridad y libertad no son opuestos sino complementarios. Locke sostuvo que el propósito fundamental del gobierno es precisamente proteger las libertades naturales

8 HOBBES, Thomas. *Leviathan*. Londres: Andrew Crooke, 1651, pp. 82-88.

de vida, libertad y propiedad, no anularlas[9]. El poder político legítimo opera dentro de límites estrictamente circunscritos, y cualquier invasión más allá de estos límites constituye tiranía independientemente de justificaciones securitarias. Mill articuló el principio del daño, según el cual la única justificación para interferir con la libertad individual es prevenir daño a otros, estableciendo así un criterio normativo para evaluar restricciones legítimas[10]. Esta tradición construyó la libertad no como ausencia de restricción sino como ausencia de interferencia arbitraria, permitiendo así formas de regulación que protejan libertades sin anularlas.

La conceptualización liberal, no obstante, descansa en supuestos problemáticos sobre la naturaleza del poder y la constitución de subjetividades. Foucault demostró que el poder no opera primariamente mediante prohibiciones legales externas sino a través de la producción de sujetos normalizados mediante dispositivos disciplinarios y biopolíticos[11]. Las instituciones modernas como escuelas, hospitales, prisiones y fábricas no simplemente reprimen libertades preexistentes sino que constituyen tipos específicos de subjetividad mediante tecnologías de vigilancia, examen y normalización. El sujeto liberal autónomo, lejos de ser un dato natural que el poder restringe, es el producto histórico de regímenes disciplinarios particulares. Esta genealogía desmantela la oposición binaria entre libertad y poder, mostrando cómo modalidades específicas de libertad son producidas por y funcionan dentro de matrices de poder determinadas.

El concepto de biopolítica desarrollado en cursos posteriores de Foucault radicaliza este argumento[12]. Mientras el poder disciplinario opera sobre cuerpos individuales mediante instituciones cerradas, la biopolítica gestiona poblaciones mediante técnicas estadísticas, actuariales y regulatorias que modulan procesos vitales agregados como natalidad, mortalidad, salud pública y productividad económica. El liberalismo, argumenta Foucault, no representa la limitación del poder gubernamental sino una reconfiguración de sus objetivos y técnicas. El gobierno liberal opera mediante la producción de libertad como recurso que debe ser administrado, protegido y optimizado. La libertad de mercado, de circulación, de expresión no son limitaciones al poder sino precondiciones para su ejercicio eficaz. La seguridad ya no se opone a la libertad, sino que constituye el marco dentro del cual ciertas libertades son posibilitadas mientras otras son forcluidas.

Esta perspectiva permite repensar radicalmente el problema contemporáneo de vigilancia digital. Las tecnologías de monitoreo no simplemente restringen libertades preexistentes, sino que reconfiguran los términos mismos en que libertad y seguridad son experimentadas y

9 LOCKE, Juan. *Two treatises of government*. Cambridge University Press, 1689, pp. 270-275.

10 MILL, John Stuart. *On liberty*. Londres: John W. Parker and Son, 1859, pp. 12-18.

11 FOUCAULT, Michel. *Discipline and punish: The birth of the prison*. Random House, 1975, pp. 170-177.

12 FOUCAULT, Michel. *The history of sexuality.* Op.cit. p. 138-140

conceptualizadas. Los sujetos contemporáneos no viven la vigilancia digital primariamente como opresión externa sino como infraestructura invisible que habilita prácticas cotidianas valoradas. Las mismas plataformas que extraen datos masivos proporcionan servicios de comunicación, información y entretenimiento experimentados como expansión de capacidades individuales. Esta ambigüedad no puede ser capturada mediante marcos que asumen sujetos autónomos preexistentes cuyas libertades son limitadas externamente por poder represivo[13].

La revisión de las matrices contractualistas, liberales y biopolíticas evidencia que la dicotomía entre seguridad y libertad no constituye una oposición estable, sino una construcción histórica dependiente de racionalidades específicas de gobierno. Precisamente por ello, el análisis debe desplazarse desde la teoría normativa clásica hacia el estudio de las formas concretas en que el poder contemporáneo organiza conductas y gestiona riesgos. La sección siguiente profundiza en el concepto de gubernamentalidad y en el paradigma securitario actual como marco operativo donde aquella tensión adquiere configuración tecnológica.

3. GUBERNAMENTALIDAD Y EL PARADIGMA SECURITARIO CONTEMPORÁNEO

El concepto foucaultiano de gubernamentalidad proporciona herramientas analíticas cruciales para comprender las racionalidades políticas que subyacen al despliegue contemporáneo de tecnologías de vigilancia. Gubernamentalidad refiere a las mentalidades, racionalidades y técnicas mediante las cuales gobiernos y otras autoridades intentan modelar conductas de poblaciones e individuos hacia fines considerados deseables[14]. Esta perspectiva desplaza el foco desde instituciones estatales formales hacia el ensamblaje heterogéneo de prácticas, conocimientos expertos, tecnologías y racionalidades que constituyen el gobierno en sentido amplio.

El paradigma securitario que caracteriza las sociedades contemporáneas representa una modalidad específica de gubernamentalidad centrada en la gestión de riesgos y amenazas. Desde finales del siglo XX, discursos sobre terrorismo, criminalidad, pandemias y colapso ambiental han legitimado expansión dramática de capacidades estatales y corporativas de vigilancia presentadas como necesarias para protección colectiva[15]. Esta securitización de esferas crecientes de existencia social opera mediante lógica actuarial que transforma eventos potenciales en riesgos calculables que deben ser prevenidos mediante intervención anticipatoria. La seguridad ya no responde

13 HAGGERTY, Kevin D.; ERICSON, Richard V. "The surveillant assemblage". *British Journal of Sociology*, vol. 51, n° 4, 2000, pp. 605-622.

14 FOUCAULT, Michel. *Security, territory, population: Lectures at the Collège de France 1977-1978*. Palgrave Macmillan, 2007, pp. 1-20.

15 ARADAU, Claudia; VAN MUNSTER, Rens. "Governing terrorism through risk: Taking precautions, (un)knowing the future." *European Journal of International Relations*, 2007, vol.13, nº1, pp. 89-115.

reactivamente a amenazas manifiestas, sino que opera preventivamente sobre campos de posibilidad, identificando poblaciones y conductas que presentan probabilidades elevadas de desviación futura. Esta pretensión de dirección centralizada sobre los campos de posibilidad social constituye la reactualización técnica del riesgo de servidumbre, donde la planificación del destino individual es transferida desde el sujeto hacia un aparato burocrático que asume el control de los medios para fines colectivos de seguridad[16].

Esta lógica actuarial tiene implicaciones profundas para libertades civiles tradicionales. El principio liberal según el cual individuos no deben ser sancionados por acciones no realizadas se erosiona cuando algoritmos predictivos clasifican sujetos según perfiles de riesgo construidos mediante agregación de patrones poblacionales[17]. Individuos que no han cometido ninguna transgresión pueden ser sometidos a escrutinio intensificado, restricciones de movilidad o exclusión de oportunidades basándose en correlaciones estadísticas entre sus características demográficas o conductuales y patrones asociados con criminalidad. Esta gubernamentalidad algorítmica no requiere comprensión de causalidad ni intencionalidad individual, operando mediante identificación de patrones en volúmenes masivos de datos que exceden capacidad de interpretación humana[18].

Las tecnologías de vigilancia digital contemporáneas amplían dramáticamente el alcance y penetración de esta racionalidad securitaria. Sistemas de reconocimiento facial desplegados en espacios públicos permiten rastrear movimientos de individuos en tiempo real, identificando patrones anómalos o presencias en ubicaciones consideradas sospechosas[19]. Análisis de comunicaciones digitales mediante procesamiento de lenguaje natural identifica expresiones categorizadas como amenazantes o radicales, alimentando bases de datos que informan decisiones sobre vigilancia intensificada o intervención preventiva. Plataformas de redes sociales construyen grafos de relaciones que permiten identificar individuos conectados con sujetos bajo investigación, expandiendo redes de sospecha mediante asociación. Dispositivos de internet de las cosas generan flujos continuos de datos sobre ubicación, consumo y conductas domésticas que, agregados, proporcionan retratos exhaustivos de rutinas cotidianas.

Esta infraestructura de vigilancia ubicua constituye lo que Haggerty y Ericson denominaron ensamblaje de vigilancia, caracterizado por convergencia de sistemas previamente discretos en arquitecturas integradas

16 HAYEK, Friedrich A. *Camino de servidumbre*. Madrid: Alianza Editorial, 2007, pp. 125-135.

17 GANDY, Oscar H. *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Ashgate Publishing. 2009, pp. 1-15.

18 ROUVROY, Antoinette; BERNS, Thomas. "Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships?". *Réseaux*. 2013, vol. 177, nº1, pp.163-196. Disponible en: <https://doi.org/10.3917/res.177.0163>

19 GATES, Kelly A. *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press. 2011, pp. 1-20.

que capturan y procesan información sobre individuos en múltiples dominios simultáneamente [20]. El cuerpo vigilado es desagregado en flujos de datos que circulan entre bases heterogéneas, siendo reensamblado en perfiles construidos para propósitos variables. Esta vigilancia no opera desde un centro panóptico singular sino mediante redes distribuidas de captura, almacenamiento, procesamiento y circulación de información. La metáfora benthamiana del panóptico, aunque útil, captura inadecuadamente esta multiplicidad de miradas que operan mediante lógicas algorítmicas opacas.

Tal ensamblaje desborda la geografía política clásica al configurarse como una topología compleja en la que el Estado intenta proyectar su autoridad sobre estratos heterogéneos que abarcan desde la infraestructura material, como cables submarinos y centros de datos, hasta las capas lógicas asociadas a servicios en la nube y sistemas de inteligencia artificial[21]. En tal configuración digital, la soberanía deja de vincularse exclusivamente a un territorio delimitado y pasa a definirse como la capacidad de inscribir principios de gobernanza y orientaciones normativas directamente en el código y en la arquitectura técnica que organiza el ciberespacio.

La opacidad algorítmica constituye problema epistemológico y político fundamental. Los sistemas de aprendizaje automático que procesan datos masivos para identificar patrones predictivos operan mediante técnicas matemáticas cuya lógica inferencial es frecuentemente ininterpretable incluso para diseñadores[22]. Las decisiones sobre quién es clasificado como riesgo elevado, qué conductas activan alertas o qué individuos son sometidos a escrutinio intensificado emergen de procesos computacionales que no pueden ser traducidos a justificaciones causales comprensibles para humanos. Esta caja negra algorítmica socava principios fundamentales de responsabilidad democrática y debido proceso legal, donde decisiones que afectan libertades individuales deben ser justificables mediante razones públicamente accesibles y sujetas a contestación.

El examen de la racionalidad securitaria y de sus ensamblajes algorítmicos muestra que la vigilancia digital no puede comprenderse exclusivamente como expansión estatal, sino como articulación compleja entre saber experto, cálculo actuarial e infraestructuras técnicas distribuidas. Sin embargo, esta racionalidad política se encuentra imbricada con dinámicas económicas específicas que incentivan la captura sistemática de datos. Por tanto, la sección siguiente analiza el capitalismo de vigilancia como lógica estructural que mercantiliza la experiencia humana y potencia el despliegue de dispositivos securitarios.

---

20 HAGGERTY, Kevin D.; ERICSON, Richard V. Op.cit. p. 610-615

21 PIERUCCI, Federico. “Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace”. *Digital Society*, 2025, vol. 4, nº 27, pp. 7-10. Disponible en: <https://doi.org/10.1007/s44206-025-00189-4>

22 BURRELL, Jenna. “How the machine 'thinks': Understanding opacity in machine learning algorithms”. *Big Data & Society.* 2016, vol 3, nº1, pp. 1-12. Disponible en: <https://doi.org/10.1177/2053951715622512>

4. CAPITALISMO DE VIGILANCIA Y LA MERCANTILIZACIÓN DE LA EXPERIENCIA HUMANA

El análisis de gubernamentalidad securitaria debe complementarse con examen de las dinámicas económicas que impulsan proliferación de vigilancia digital. Zuboff argumenta que el capitalismo contemporáneo ha desarrollado una lógica distintiva que denomina capitalismo de vigilancia, donde la experiencia humana es unilateralmente apropiada como materia prima gratuita para traducción en datos comportamentales[23]. Estos datos son procesados mediante algoritmos propietarios para fabricar productos predictivos que son vendidos en mercados comportamentales donde empresas apuestan por conductas futuras de usuarios. Esta lógica económica trasciende modelos previos basados en venta de productos o servicios, centrándose en cambio en extracción de superávit conductual que permite predicción y modificación de comportamiento.

Las plataformas digitales dominantes como Google, Facebook, Amazon y equivalentes operan mediante este modelo extractivo. Los servicios aparentemente gratuitos proporcionados a usuarios constituyen interfaces para captura de datos que son el producto real vendido a anunciantes y otros actores que buscan influenciar conductas[24]. Cada búsqueda, cada publicación, cada clic, cada pausa al leer, cada expresión facial capturada por cámaras frontales, cada inflexión vocal en asistentes activados por voz genera registros que alimentan modelos predictivos cada vez más sofisticados. Esta datificación exhaustiva construye lo que Andrejevic denomina lateral *surveillance*, donde individuos son vigilados no verticalmente por autoridades estatales sino horizontalmente por corporaciones que monetizan información personal[25].

La arquitectura del capitalismo de vigilancia genera convergencia problemática entre imperativos comerciales y securitarios. Las mismas bases de datos y capacidades analíticas desarrolladas para publicidad dirigida son utilizadas por agencias estatales de seguridad nacional, frecuentemente mediante acuerdos voluntarios o compulsivos entre corporaciones y gobiernos[26]. Las revelaciones de Snowden en 2013 expusieron programas masivos de vigilancia donde agencias de inteligencia accedían directamente a servidores de corporaciones tecnológicas o interceptaban comunicaciones en puntos de infraestructura crítica[27]. Esta relación simbiótica entre vigilancia

23 ZUBOFF, Shoshana. *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* New York: Public Affairs, 2019. Op.cit. p. 18-25

24 FUCHS, Christian. "A contribution to the critique of the political economy of Google." *Fast Capitalism*. 2011, vol. 8, nº1. Disponible en: https://doi.org/10.32855/fcapital.201101.006

25 ANDREJEVIC, Mark. *iSpy: Surveillance and power in the interactive era*. Kansas: University Press of Kansas, 2007, pp. 2-10.

26 BALL, Kirstie; WEBSTER, Frank. *The intensification of surveillance: Crime, terrorism and warfare in the information age*. Londres: Pluto Press, 2003, pp. 5-20.

27 LYON, David. "Surveillance, Snowden, and Big Data: Capacities, consequences,

comercial y estatal genera ensamblaje público-privado donde distinciones tradicionales entre esferas gubernamentales y mercantiles se disuelven.

Esta convergencia tiene implicaciones profundas para teorías liberales de limitación del poder. El constitucionalismo liberal desarrolló restricciones sobre poder estatal basadas en derechos fundamentales protegidos contra interferencia gubernamental. Sin embargo, cuando vigilancia es ejecutada por corporaciones privadas operando en mercados, estas protecciones constitucionales frecuentemente no aplican o son evadidas mediante doctrinas de consentimiento[28]. Los usuarios supuestamente consienten vigilancia mediante aceptación de términos de servicio extensos escritos en lenguaje legal incomprensible que nadie lee. Este formalismo contractual oscurece relaciones de poder fundamentalmente asimétricas donde individuos no tienen alternativas reales para participar en infraestructuras digitales que se han vuelto esenciales para empleo, educación y participación social.

La conceptualización marxista de alienación proporciona marco sugerente para comprender esta dinámica. Así como trabajadores bajo capitalismo industrial son alienados de productos de su labor que se vuelven propiedad de capitalistas, usuarios bajo capitalismo de vigilancia son alienados de sus propias experiencias y conductas que son apropiadas como datos propiedad de corporaciones[29]. Esta alienación es doblemente mistificada porque los sujetos experimentan plataformas digitales como espacios de autoexpresión, conexión social y realización personal, no reconociendo que estas prácticas generan valor económico apropiado por otros. La subjetividad misma se convierte en sitio de extracción, donde aspectos más íntimos de existencia personal son transformados en mercancías circulando en mercados de datos.

En consecuencia, la economía política de la extracción de datos revela que la vigilancia no solo administra riesgos externos, sino que reorganiza la producción misma de valor y subjetividad. En ese contexto, la captura conductual no actúa únicamente sobre prácticas observables, sino que incide en la constitución psíquica de los sujetos. En consecuencia, la sección siguiente examina la dimensión psicopolítica de los regímenes digitales, explorando cómo las tecnologías de plataforma producen formas específicas de subjetividad adaptadas a lógicas de rendimiento y autooptimización.

5. SUBJETIVIDAD Y PSICOPOLÍTICA EN REGÍMENES DE VIGILANCIA DIGITAL

Las transformaciones descritas no operan simplemente sobre sujetos preexistentes sino que producen formas específicas de subjetividad

---

critique". *Big Data & Society*, 2014, vol. 1, nº 2, pp. 4-7. Disponible en: <https://doi.org/10.1177/2053951714541861>

28 COHEN, Julien E. *Configuring the networked self: Law, code, and the play of everyday practice*. Yale University Press, 2012, pp. 10-25.

29 FUCHS, Christian. Op.cit. Disponible en: <https://doi.org/10.32855/fcapital.201101.006>

adaptadas a regímenes de vigilancia digital. Han[30] argumenta que las sociedades contemporáneas han transitado desde sociedades disciplinarias foucaultianas hacia sociedades de rendimiento caracterizadas por lógicas de autoexplotación donde sujetos se conciben como empresarios de sí mismos responsables de optimización perpetua. Esta psicopolítica opera no mediante prohibiciones externas sino mediante modulación de estados mentales y emocionales, produciendo sujetos que experimentan compulsión sistémica como motivación autogenerada.

Las plataformas digitales constituyen tecnologías psicopolíticas paradigmáticas. Algoritmos de recomendación en redes sociales modulan exposición informativa para maximizar *engagement*, explotando vulnerabilidades neuropsicológicas relacionadas con validación social y comparación interpersonal[31]. Arquitecturas de retroalimentación inmediata mediante *likes*, *shares* y comentarios generan ciclos de reforzamiento que condicionan conductas sin que usuarios experimenten esta modulación como coacción externa. El sujeto neoliberal se constituye mediante estas tecnologías como un ser perpetuamente disponible, conectado, cuantificando y optimizando rendimiento en múltiples dominios simultáneamente.

Esta forma de poder se distingue cualitativamente de la disciplina foucaultiana. Mientras instituciones disciplinarias operaban mediante confinamiento espacial, horarios rígidos y vigilancia arquitectónicamente inscrita, la psicopolítica digital opera mediante modulación continua en espacios abiertos donde sujetos se experimentan como libres. La libertad misma deviene técnica de poder cuando sujetos internalizan imperativos de autooptimización presentados como expresiones de autonomía personal[32]. La vigilancia digital proporciona retroalimentación continua sobre rendimiento en relación con normas construidas algorítmicamente, generando formas de normalización más sutiles, pero potencialmente más penetrantes que mecanismos disciplinarios visibles.

La gamificación de esferas crecientes de existencia cotidiana ejemplifica esta lógica. Aplicaciones de fitness rastrean actividad física, competencia con pares y progreso hacia metas autoimpuestas. Plataformas educativas generan scores de rendimiento y rankings comparativos. Aplicaciones de productividad cuantifican tiempo utilizado en tareas diversas, proporcionando métricas de eficiencia. Esta cuantificación del yo transforma aspectos cualitativos de experiencia en datos comparables y optimizables, produciendo subjetividades estructuradas por lógicas de mejora continua y comparación perpetua[33]. El

30 HAN, Byung-Chul. *Psychopolitics: Neoliberalism and new technologies of power*. Verso Books. 2014. Op. Cit. p. 5-10

31 WILLIAMS, J. *Stand out of our light: Freedom and resistance in the attention economy*. Cambridge University Press, 2018, pp. 12-25.

32 ROSE, Nicholas. *Powers of freedom: Reframing political thought*. Cambridge University Press. 1999, pp. 1-15.

33 LUPTON, Deborah. *The quantified self: A sociology of self-tracking*. Cambridge: Polity Press. 2016, pp. 3-18.

sujeto deviene tanto vigilante de sí mismo como objeto de vigilancia externa, colapsando la distinción entre autocontrol y control heterónomo.

Si la psicopolítica digital modula deseos, afectos y conductas mediante arquitecturas invisibles de retroalimentación, ciertas tecnologías condensan de manera paradigmática esta transformación al inscribir la vigilancia directamente sobre el cuerpo. Entre ellas, el reconocimiento facial destaca por su capacidad de suprimir el anonimato en el espacio público y reconfigurar la experiencia misma de visibilidad. Por ello, la sección siguiente aborda específicamente esta tecnología como punto crítico en la rearticulación contemporánea entre identidad, espacio y control.

6. RECONOCIMIENTO FACIAL Y LA ELIMINACIÓN DEL ANONIMATO

Entre las tecnologías de vigilancia contemporáneas, los sistemas de reconocimiento facial representan quizás la amenaza más dramática a espacios tradicionales de anonimato y privacidad en lugares públicos. Estas tecnologías permiten identificación biométrica automática de individuos en multitudes, vinculando presencias físicas con identidades digitales y bases de datos de información personal[34]. La masificación de cámaras en espacios urbanos, combinada con capacidades crecientes de procesamiento algorítmico, posibilita rastreo continuo de movimientos poblacionales en tiempo real a escala de ciudades enteras.

Las implicaciones de esta eliminación del anonimato público son profundas. Las teorías liberales tradicionales distinguieron entre esferas públicas donde individuos aceptan visibilidad y esferas privadas protegidas de escrutinio externo. Sin embargo, esta distinción asumía que visibilidad en público era transitoria y anónima, no generando registros permanentes vinculables a identidades específicas[35]. El reconocimiento facial automatizado destruye esta expectativa, transformando cada aparición pública en registro permanente disponible para análisis retrospectivo. Esta datificación exhaustiva de presencia espacial habilita formas de control y modulación conductual que no requieren intervención coercitiva explícita, sino que operan mediante conocimiento de posibilidad perpetua de monitoreo.

Los efectos de este monitoreo ubicuo sobre conducta pública constituyen preocupación central. La literatura sobre efectos de vigilancia documenta fenómenos de autocensura y conformidad cuando individuos se saben observados[36]. Si cada expresión pública, cada manifestación, cada asociación es registrada y potencialmente evaluada según criterios de normalidad o desviación construidos algorítmicamente, los espacios

34 GATES, Kelly A. *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press. 2011, pp. 25-30.

35 NISSENBAUM, Helen. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2010, pp. 12-22.

36 MARX, Gary T. *Windows into the soul: Surveillance and society in an age of high technology*. University of Chicago Press. 2016, pp. 1-15.

para disenso político, experimentación cultural y no conformidad social se contraen. La libertad de reunión, expresión y asociación garantizada constitucionalmente deviene limitada de facto cuando ejercicio de estas libertades genera rastros permanentes que pueden ser utilizados para perfilamiento, discriminación o intimidación.

Las aplicaciones comerciales de reconocimiento facial agregan dimensiones adicionales de preocupación. *Retailers* utilizan esta tecnología para rastrear comportamiento de consumidores dentro de tiendas, identificando patrones de movimiento, expresiones emocionales ante productos y tiempo de atención en *displays* específicos[37]. Esta vigilancia afectiva busca extraer información sobre estados emocionales para optimizar estrategias de marketing y arquitectura de espacios comerciales. El sujeto deviene legible no simplemente mediante acciones manifiestas sino mediante microexpresiones faciales interpretadas algorítmicamente como indicadores de estados mentales internos. Esta pretensión de transparencia psicológica total mediante lectura automatizada de señales corporales involuntarias representa intensificación cualitativa del proyecto de vigilancia.

La erosión del anonimato público no solo altera la espacialidad de la libertad, sino que prepara el terreno para un desplazamiento más profundo: la anticipación algorítmica del comportamiento futuro. Una vez que identidades y trayectorias pueden ser rastreadas con precisión biométrica, la intervención preventiva deviene técnica central de gobierno. En consecuencia, la sección siguiente analiza los algoritmos predictivos y la transformación de la temporalidad del control que introducen.

7. ALGORITMOS PREDICTIVOS Y LA TEMPORALIDAD DEL CONTROL

Los sistemas algorítmicos de predicción conductual introducen transformación fundamental en la temporalidad del poder y control social. Mientras formas tradicionales de gobierno operaban reactivamente, respondiendo a transgresiones ya ocurridas mediante castigo o corrección, la gubernamentalidad algorítmica opera preventivamente, interviniendo sobre campos de posibilidad antes de actualización de eventos problemáticos[38]. Esta temporalidad anticipatoria transforma radicalmente relación entre sujetos y autoridad, donde individuos son responsabilizados no por acciones realizadas sino por propensiones probabilísticas atribuidas mediante perfilamiento algorítmico.

El policiamiento predictivo ejemplifica esta lógica. Departamentos policiales utilizan algoritmos que procesan datos históricos de criminalidad, características demográficas de vecindarios y variables ambientales para

37 McSTAY, Andrew. *Emotional AI: The rise of empathic media*. SAGE Publications. 2018, pp. 10-25.

38 AMOORE, Louise. *The politics of possibility: Risk and security beyond probability*. Durham: Duke University Press, 2013. Op. cit. p. 15-20.

identificar ubicaciones geográficas y periodos temporales con probabilidad elevada de actividad criminal[39]. Los recursos policiales son entonces concentrados preventivamente en estas zonas calientes, con expectativa de disuadir crímenes que de otro modo habrían ocurrido. Sin embargo, esta estrategia genera bucles de retroalimentación problemáticos. Incremento de presencia policial en áreas identificadas algorítmicamente como riesgosas resulta en más arrestos en esas áreas, lo cual a su vez alimenta algoritmos que interpretan estos arrestos como validación de predicciones iniciales, perpetuando y amplificando sesgos incorporados en datos históricos[40].

Los sistemas de *scoring* crediticio y evaluación de riesgo en dominios como empleo, vivienda y seguros operan mediante lógicas similares. Decisiones sobre acceso a recursos y oportunidades son automatizadas mediante algoritmos que procesan volúmenes masivos de variables para predecir probabilidades de incumplimiento, deserción o comportamiento problemático futuro[41]. Estos sistemas frecuentemente incorporan *proxies* que correlacionan con categorías protegidas como raza, género o clase social, generando efectos discriminatorios sin referencia explícita a estas categorías. La opacidad de estos procesos y su justificación mediante racionalidad tecnocrática de eficiencia y gestión de riesgo oscurecen dimensiones políticas de distribución de oportunidades y perpetuación de desigualdades estructurales.

La lógica actuarial de estos sistemas es fundamentalmente antiliberal en que rechaza individualización en favor de tratamiento de sujetos como miembros de categorías estadísticas[42]. Los principios liberales de responsabilidad individual y juicio basado en acciones específicas son desplazados por clasificación grupal donde individuos heredan propensidades atribuidas a poblaciones con las que comparten características. Esta gubernamentalidad poblacional no requiere ni desea conocimiento de circunstancias particulares, intenciones subjetivas o narrativas biográficas que liberalismo clásico consideró relevantes para evaluación moral y legal. El sujeto es reducido a vector de atributos procesables algorítmicamente, donde agencia y particularidad son suprimidas en favor de subsunción en patrones agregados.

La gubernamentalidad anticipatoria, sustentada en perfiles probabilísticos y clasificación poblacional, revela un horizonte de control que opera antes del acto y más allá de la responsabilidad individual clásica. Frente a esta expansión preventiva del poder, emergen prácticas que buscan

39 FERGUSON, Andrew Guthrie. *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York: New York University Press, 2017, pp. 1-18.

40 O'NEIL, Cathy. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing, 2016, pp. 3-15.

41 PASQUALE, Frank. *The black box society: The secret algorithms that control money and information*. Harvard University Press. 2015, pp. 1-10.

42 HARCOURT, B. E. *Against prediction: Profiling, policing, and punishing in an actuarial age*. University of Chicago Press. 2007, pp. 12-28.

reinstaurar márgenes de indeterminación y opacidad. De ahí que la sección siguiente examine estrategias de resistencia, ofuscación y contestación política frente a regímenes de vigilancia algorítmica.

8. RESISTENCIA, OPACIDAD Y POLÍTICA DE OFUSCACIÓN

Frente a regímenes de vigilancia ubicua, han emergido diversas estrategias de resistencia y prácticas de opacidad que buscan limitar visibilidad sin retirarse completamente de infraestructuras digitales. Brunton y Nissenbaum[43] desarrollaron concepto de ofuscación, definido como producción deliberada de información ambigua, confusa o engañosa para interferir con vigilancia y minería de datos. Estas tácticas incluyen generación de búsquedas aleatorias para obscurecer patrones reales de interés, uso de servicios de anonimización como Tor para desconectar identidades de actividad online, y extensiones de navegador que clican automáticamente en anuncios para contaminar perfiles publicitarios.

Estas prácticas representan forma de resistencia cotidiana frente a asimetrías informacionales donde corporaciones y estados acumulan conocimiento exhaustivo sobre individuos mientras sus propias operaciones permanecen opacas. La ofuscación no busca invisibilidad total, frecuentemente imposible en infraestructuras digitales contemporáneas, sino generar suficiente ruido para volver datos individuales menos útiles para perfilamiento y predicción[44]. Esta política de opacidad invierte valoración liberal de transparencia, argumentando que, en condiciones de vigilancia asimétrica, opacidad constituye recurso político valioso para proteger autonomía individual.

Sin embargo, estas estrategias individuales de resistencia enfrentan limitaciones estructurales significativas. La efectividad de ofuscación depende de adopción suficientemente amplia para que prácticas de ofuscación no sean identificables como señales de comportamiento sospechoso que activen escrutinio adicional. Además, las capacidades técnicas de corporaciones y estados para procesar volúmenes masivos de datos y distinguir señales significativas de ruido exceden dramáticamente recursos disponibles para individuos[45]. La batalla por opacidad deviene carrera armamentista asimétrica donde usuarios despliegan herramientas limitadas contra instituciones con recursos virtualmente ilimitados para desarrollo de contramedidas algorítmicas.

Las limitaciones de resistencia individual subrayan necesidad de

43 BRUNTON, Finn y NISSENBAUM, Helen. *Obfuscation: A user's guide for privacy and proest*. Cambridge: MIT Press, 2015, pp. 1-15.

44 FINN, Rachel L.; WRIGHT, David; FRIEDEWALD, Michael.“ Seven types of privacy. In GUTWIRTH Serge; LEENES Ronald; DE HERT Paul; POULLET Yves (Eds.), *European data protection: Coming of age. Dordrecht: Springer, 2013,* pp. 3-32.

45 BAROCAS, Solon; NISSENBAUM, Helen. “Big data's end run around anonymity and consent”. In J. LANE, V. STODDEN, S. BENDER, & H. NISSENBAUM (Eds.), *Privacy, big data, and the public good.* Cambridge: Cambridge University Press, 2014, pp.44-75.

respuestas colectivas y regulatorias. Movimientos por privacidad digital han abogado por marcos legales que impongan límites obligatorios a recolección, procesamiento y retención de datos personales. El Reglamento General de Protección de Datos de la Unión Europea representa esfuerzo significativo en esta dirección, estableciendo principios como minimización de datos, consentimiento explícito y derecho al olvido[46]. Sin embargo, implementación efectiva enfrenta desafíos sustanciales. Las corporaciones han desarrollado interfaces de consentimiento diseñadas para maximizar aceptación de términos permisivos mediante patrones oscuros que explotan sesgos cognitivos. El derecho a portabilidad de datos presupone mercados competitivos que raramente existen en contextos de monopolios de plataforma con efectos de red masivos.

Más fundamentalmente, marcos regulatorios centrados en consentimiento individual y control sobre datos personales pueden ser inadecuados para abordar dimensiones estructurales de vigilancia digital. Cohen argumenta que privacidad no debe conceptualizarse simplemente como derecho individual a control informacional sino como bien colectivo necesario para preservar espacios de experimentación cultural y disenso político[47]. Esta reconceptualización desplaza foco desde gestión de preferencias individuales hacia configuración de infraestructuras que protejan capacidades colectivas para desarrollo político y cultural. Las políticas efectivas requerirían no simplemente regular usos de datos sino transformar arquitecturas de captura que hacen vigilancia ubicua técnicamente inevitable.

Las tácticas individuales y colectivas de ofuscación evidencian tanto la creatividad de la resistencia como sus límites estructurales ante infraestructuras globales de captura de datos. Dichos límites obligan a ampliar el análisis hacia las configuraciones geopolíticas que sostienen el extractivismo digital a escala planetaria. En consecuencia, la sección siguiente aborda las dimensiones coloniales y geopolíticas de la vigilancia contemporánea, situando el problema más allá del marco estrictamente nacional.

9. DIMENSIONES COLONIALES Y GEOPOLÍTICAS DE VIGILANCIA DIGITAL

El análisis de vigilancia digital debe atender a dimensiones geopolíticas y coloniales frecuentemente marginalizadas en discusiones centradas en contextos noratlánticos. Couldry y Mejias argumentan que capitalismo de datos constituye forma de colonialismo que extrae y apropia experiencia humana como recurso para acumulación corporativa, reproduciendo lógicas extractivas del colonialismo histórico en dominios digitales[48]. Esta perspectiva

46 VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. 2017, pp. 1-25.

47 COHEN, Julien E. *Configuring the networked self: Law, code, and the play of everyday practice*. Yale University Press, 2012. Op. Cit. p. 30-45.

48 COULDRY, Nick; MEJIAS, Ulises. A. *The costs of connection: How data is colonizing human*

revela continuidades entre apropiación de tierras, recursos y cuerpos bajo imperialismo histórico y apropiación contemporánea de datos, atención y vida social bajo plataformas digitales.

Las corporaciones tecnológicas dominantes mantienen control cuasi-monopolístico sobre infraestructuras digitales globales, concentrando poder económico y político en jurisdicciones específicas mientras extraen datos de poblaciones globales. Esta geografía desigual del capitalismo de vigilancia genera flujos unidireccionales donde datos generados en Sur Global alimentan algoritmos diseñados y monetizados en Norte Global[49]. Las decisiones sobre arquitecturas de plataformas, políticas de contenido y prioridades algorítmicas son tomadas por corporaciones basadas en Silicon Valley sin participación democrática de poblaciones globales afectadas. Esta gobernanza corporativa transnacional opera fuera de mecanismos de responsabilidad democrática tradicionales vinculados a territorios estatales.

Las exportaciones de tecnologías de vigilancia desde democracias occidentales hacia regímenes autoritarios generan preocupaciones adicionales. Corporaciones europeas y norteamericanas han vendido sistemas de reconocimiento facial, software de monitoreo de comunicaciones y capacidades de análisis de *big data* a gobiernos con historiales documentados de represión política y violaciones de derechos humanos[50]. Estas exportaciones permiten sofisticación sin precedentes de aparatos de control autoritario, facilitando identificación y represión de disidentes, minorías y movimientos sociales. La justificación comercial de neutralidad tecnológica obscurece responsabilidades éticas por usos previsibles de herramientas diseñadas específicamente para vigilancia y control poblacional.

China representa caso particularmente instructivo de despliegue estatal masivo de vigilancia digital integrada con sistemas de control social. El sistema de crédito social en desarrollo vincula comportamientos monitoreados digitalmente con scores que determinan acceso a servicios, oportunidades de empleo y movilidad[51]. La combinación de reconocimiento facial ubicuo, análisis de comunicaciones digitales y datafication de transacciones económicas genera infraestructura de monitoreo totalitario sofisticado técnicamente de maneras imposibles para regímenes autoritarios del siglo XX. Este modelo ha sido explícitamente promocionado como exportable, con corporaciones chinas vendiendo paquetes de ciudad inteligente que integran capacidades de vigilancia a gobiernos en Asia, África y América Latina.

life and appropriating it for capitalism. Stanford University Press, 2019, pp. 1-20.

49 GRAHAM, Mark; HALE, Scott A; STEPHENS, M. Geographies of the world's knowledge. *Convoco Foundation*. 2014, pp. 1-12.

50 FELDSTEIN, Steven. *The global expansion of AI surveillance*. Carnegie Endowment for International Peace, 2019, pp. 1-15.

51 LIANG, Fan; DAS, Vishnupriya; KOSTYUK, Nadiya; HUSSAIN, Muzammil M.“ Constructing a data-driven society: China's social credit system as a state surveillance infrastructure”. *Policy & Internet*, 2018, vol.10, nº4, pp. 415-453.

La expansión de la inteligencia artificial generativa en este ecosistema intensifica los riesgos de fuga de datos y erosión de la privacidad, evidenciando la obsolescencia de los sistemas de protección centrados en el control individual frente a modelos de procesamiento masivo y opaco que demandan una reconfiguración institucional hacia la denominada 'IA confiable'[52]. La integración de normas de derecho público y privado en el contexto asiático busca mitigar la vulnerabilidad técnica de los grandes modelos de lenguaje, aunque persiste una brecha crítica entre la innovación tecnológica y la capacidad de supervisión efectiva de los derechos de personalidad.

Sin embargo, conceptualizar vigilancia digital simplemente como amenaza autoritaria externa a democracias liberales reproduce binarios problemáticos que oscurecen convergencias. Como argumenta Lyon, regímenes de vigilancia en democracias liberales y estados autoritarios comparten lógicas, tecnologías e infraestructuras comunes, diferenciándose más en grados de penetración y propósitos explícitos que en arquitecturas fundamentales[53]. Las revelaciones sobre programas masivos de vigilancia en Estados Unidos y aliados demostraron que democracias liberales han construido capacidades de monitoreo que exceden cualitativamente prácticas de regímenes previamente considerados totalitarios. Esta convergencia sugiere que arquitecturas digitales contemporáneas generan tendencias hacia vigilancia ubicua relativamente independientes de regímenes políticos específicos.

En términos normativos, el presente análisis concluye que la superación de la paradoja entre seguridad y libertad exige transitar hacia un modelo de soberanía tecnológica proactiva. El marco debe cimentarse en la inalienabilidad de la huella biométrica, elevando el anonimato en espacios públicos a la categoría de derecho fundamental no negociable. Asimismo, se requiere instaurar una transparencia algorítmica obligatoria que garantice la explicabilidad humana auditable frente a la opacidad de las 'cajas negras' comerciales. Finalmente, es imperativo promover una descentralización de las infraestructuras mediante el *edge computing* y la interoperabilidad obligatoria, medidas orientadas a neutralizar la centralización extractiva que sustenta el actual paradigma biopolítico y a devolver la autonomía técnica a la esfera de la decisión democrática.

La lectura geopolítica demuestra que la vigilancia digital no es anomalía autoritaria, sino rasgo transversal de arquitecturas tecnológicas globalizadas que desafían los marcos clásicos de soberanía. Tal constatación impacta directamente en las teorías democráticas, cuya viabilidad depende

52 YE, Xiongbiao; YAN, Yuhong; LI, Jia; JIANG, Bo. "Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective". *Telecommunications Policy*, 2024, vol. 48, nº 10, art. 102851, pp. 2-6. Disponible en: https://doi.org/10.1016/j.telpol.2024.102851

53 LYON, David. *Surveillance society: Monitoring everyday life*. Open University Press. 2001, pp. 10-18.

de condiciones de publicidad, responsabilidad y conocimiento compartido. Por ello, la sección siguiente examina los efectos de la opacidad algorítmica sobre la democracia y los límites del conocimiento colectivo.

10. DEMOCRACIA, TRANSPARENCIA Y LOS LÍMITES DEL CONOCIMIENTO COLECTIVO

Las tecnologías de vigilancia plantean desafíos fundamentales para teorías democráticas que presuponen agencia ciudadana informada y capacidad de fiscalización pública de poder. La opacidad de sistemas algorítmicos complejos limita severamente posibilidades de comprensión colectiva de cómo decisiones que afectan vidas son tomadas. Los algoritmos propietarios que determinan quién recibe crédito, empleo o libertad condicional operan como cajas negras inaccesibles a escrutinio público, protegidas mediante secreto comercial y complejidad técnica que excede capacidades interpretativas incluso de expertos[54].

Esta opacidad genera crisis de responsabilidad democrática. Los principios de gobierno representativo presuponen que ciudadanos puedan evaluar decisiones gubernamentales, exigir justificaciones y responsabilizar autoridades mediante procesos electorales y judiciales. Sin embargo, cuando decisiones son delegadas a sistemas algorítmicos cuya lógica operativa es opaca, estos mecanismos de responsabilidad se vuelven inoperantes[55]. Las demandas por transparencia algorítmica enfrentan limitaciones técnicas y políticas. Técnicamente, la complejidad de redes neuronales profundas puede hacer genuinamente imposible proporcionar explicaciones causales comprensibles de decisiones específicas. Políticamente, transparencia total podría habilitar *gaming* donde sujetos manipulan sistemas al conocer criterios de evaluación, potencialmente socavando efectividad de herramientas diseñadas para detección de fraude o riesgo.

Danaher argumenta que este dilema requiere repensar relaciones entre transparencia, confianza y legitimidad democrática[56]. Si transparencia total es imposible o contraproducente, legitimidad debe basarse en otras formas de *accountability* como auditorías independientes, estándares de diseño obligatorios y derechos robustos de contestación de decisiones algorítmicas. Estas alternativas desplazan gobernanza democrática desde fiscalización directa por ciudadanía hacia delegación en instituciones expertas de supervisión, generando tensiones con ideales participativos de democracia, pero potencialmente más adecuadas para complejidades técnicas de sistemas contemporáneos.

54 PASQUALE, Frank. *The black box society: The secret algorithms that control money and information*. Harvard University Press. 2015. Op. Cit. p. 15-22.

55 ANANNY, Mike; CRAWFORD, Kate. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability." *New Media & Society*, 2018, vol. 20, nº3, pp. 973-989.

56 DANAHER, Juan. "The threat of algocracy: Reality, resistance and accommodation." *Philosophy & Technology*, 2016, vol. 29, nº3, pp. 245-268).

La vigilancia digital también transforma condiciones de formación de opinión pública y deliberación democrática. Las plataformas de redes sociales que median crecientemente discusión política utilizan algoritmos de curación de contenido que optimizan *engagement* mediante explotación de sesgos emocionales y presentación de información que refuerza creencias preexistentes[57]. Esta personalización algorítmica genera fragmentación de esferas públicas en burbujas informativas donde ciudadanos son expuestos a contenido homogéneo que confirma prejuicios y polariza actitudes. La manipulación de opinión mediante circulación dirigida de desinformación, amplificada por *bots* y cuentas automatizadas, socava capacidades colectivas de formar juicios informados sobre asuntos comunes.

Estas dinámicas generan lo que algunos teóricos han denominado crisis epistémica de democracia, donde condiciones de posibilidad de conocimiento compartido necesario para deliberación colectiva son erosionadas[58]. Si ciudadanos habitan universos informacionales radicalmente diferentes, construidos algorítmicamente mediante perfilamiento personalizado, las bases para formación de voluntad colectiva mediante argumentación pública se disuelven. La democracia presupone no consenso sustantivo sino al menos mundo compartido de hechos sobre el cual desacuerdos pueden ser articulados y potencialmente resueltos mediante deliberación. La fragmentación algorítmica de experiencia informativa destruye esta precondición, dejando coexistencia de realidades incompatibles sin posibilidad de adjudicación racional.

La crisis de responsabilidad y la fragmentación epistémica revelan que la vigilancia no solo administra comportamientos, sino que redefine las condiciones mismas de producción de verdad y deliberación pública. Tal reconfiguración alcanza su expresión más intensa cuando la cuantificación algorítmica se extiende a los procesos vitales y corporales. En consecuencia, la sección siguiente analiza la biopolítica algorítmica como modalidad de producción de vida calculable en dominios de salud y bienestar.

11. BIOPOLÍTICA ALGORÍTMICA Y LA PRODUCCIÓN DE VIDA CALCULABLE

La integración de inteligencia artificial en dominios de salud, bienestar y administración de vida introduce formas de biopolítica algorítmica que operan mediante cuantificación exhaustiva de procesos corporales y vitales. Dispositivos portátiles rastrean continuamente frecuencia cardíaca, patrones de sueño, niveles de actividad y múltiples parámetros fisiológicos, generando

57 PARISER, Eli. *The filter bubble: What the internet is hiding from you*. Penguin Press. 2011, pp. 1-20.

58 LEVY, Neil. "Echoes of COVID misinformation". *Philosophical Psychology.* 2021, vol. 34, nº 3, pp.417-433.

volúmenes masivos de datos biométricos[59]. Aplicaciones de salud digital proporcionan recomendaciones personalizadas sobre nutrición, ejercicio y comportamientos saludables basadas en análisis de estos datos comparados con patrones poblacionales. Esta cuantificación del yo biológico constituye intensificación de proyecto biopolítico foucaultiano de optimización de vida poblacional, ahora operando mediante modulación algorítmica individualizada.

Las implicaciones de esta datificación de vida van más allá de preocupaciones convencionales sobre privacidad médica. Cheney-Lippold argumenta que algoritmos no simplemente representan identidades preexistentes sino que las constituyen mediante clasificación, creando categorías de riesgo, normalidad y desviación que estructuran acceso diferencial a recursos y oportunidades[60]. En contextos de salud, perfiles de riesgo algorítmicos determinan primas de seguros, elegibilidad para tratamientos y priorización en asignación de recursos médicos escasos. Estos juicios probabilísticos transforman características corporales individuales en marcadores de valor actuarial, donde cuerpos son evaluados según su adherencia a normas de salud construidas estadísticamente.

La pandemia de COVID-19 aceleró dramáticamente adopción de tecnologías de vigilancia biopolítica presentadas como necesarias para gestión de crisis sanitaria. Aplicaciones de rastreo de contactos utilizaron datos de ubicación y proximidad *Bluetooth* para identificar individuos expuestos a personas infectadas, permitiendo intervenciones de aislamiento preventivo[61]. Sistemas de monitoreo de temperatura corporal mediante cámaras térmicas en espacios públicos identificaban sujetos potencialmente sintomáticos para restricción de acceso. Pasaportes de inmunidad digitales certificaban *estatus* de vacunación y recuperación, condicionando movilidad y participación en actividades sociales y económicas. Estas medidas, aunque justificadas como temporales y excepcionales, establecieron infraestructuras y precedentes para vigilancia sanitaria ubicua que persisten post-crisis.

La normalización de estas prácticas genera riesgos de función *creep* donde capacidades desarrolladas para propósitos específicos son expandidas incrementalmente a dominios adicionales[62]. Las infraestructuras de rastreo de contactos pueden ser repurposadas para vigilancia criminal o monitoreo de disidencia política. Los datos biométricos recolectados para verificación

59 LUPTON, Deborah. *The quantified self: A sociology of self-tracking*. Cambridge: Polity Press. 2016. Op. cit. p. 20-30.

60 CHENEY-LIPPOLD, John. *We are data: Algorithms and the making of our digital selves*. New York University Press, 2017, pp. 5-25.

61 ROWE, Frantz. "Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world". *International Journal of Information Management*, 2020, vol. 55, artículo 102178. https://doi.org/10.1016/j.ijinfomgt.2020.102178

62 MARX, Gary T. *Windows into the soul: Surveillance and society in an age of high technology*. University of Chicago Press. 2016, pp. 20-35.

de vacunación pueden integrarse en bases de datos más amplias utilizadas para perfilamiento y control social. La excepcionalidad invocada para justificar medidas intrusivas deviene normalizada, erosionando límites sobre poder gubernamental que emergencias fueron permitidas temporalmente transgredir.

La datificación del cuerpo y la clasificación probabilística de riesgos vitales evidencian que la optimización biopolítica se traduce en distribuciones diferenciales de oportunidades y cargas. Tales distribuciones no son neutrales, sino que interactúan con desigualdades históricas preexistentes. Por ello, la sección siguiente se centra en la justicia algorítmica y en los modos en que los sistemas automatizados reproducen y amplifican jerarquías estructurales.

12. JUSTICIA ALGORÍTMICA Y LA PERPETUACIÓN DE DESIGUALDADES ESTRUCTURALES

La literatura creciente sobre equidad algorítmica examina cómo sistemas automatizados de decisión reproducen y amplían desigualdades históricas basadas en raza, género, clase y otras categorías de estratificación social. O'Neil[63] documentó numerosos casos donde algoritmos incorporan sesgos discriminatorios, frecuentemente porque son entrenados con datos históricos que reflejan patrones previos de discriminación. Sistemas de *scoring* de riesgo criminal utilizados en sentencias judiciales asignan puntajes más altos a defendientes negros comparados con blancos con historiales equivalentes, perpetuando disparidades raciales en encarcelamiento. Algoritmos de selección de personal discriminan contra candidatos de género femenino porque aprenden de datos históricos de contratación sesgados hacia hombres.

Estos patrones ilustran problema fundamental de lo que Barocas y Selbst[64] denominan disparate *impact*, donde sistemas que no incluyen explícitamente categorías protegidas generan efectos discriminatorios mediante uso de *proxies* correlacionados con esas categorías. Códigos postales, patrones de consumo, redes sociales y múltiples variables aparentemente neutrales están estadísticamente asociadas con raza, clase o género, permitiendo discriminación algorítmica que evade prohibiciones legales de discriminación directa. La opacidad de estos procesos complica identificación y remediación, porque mecanismos mediante los cuales inputs aparentemente inocentes producen outputs discriminatorios están obscurecidos en arquitecturas algorítmicas complejas.

Las respuestas a estos problemas han generado debates sobre qué constituye equidad algorítmica y cómo puede ser operacionalizada técnicamente. Investigadores han propuesto múltiples definiciones

63 O'NEIL, Cathy. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing, 2016. Op. Cit. p. 20-30.

64 BAROCAS, Solon; SELBST, Andrew. D. "Big data's disparate impact". *California Law Review*, 2016, vol.104, pp. 671-732. Disponible <https://doi.org/10.15779/Z38BG31>

matemáticas de fairness, incluyendo paridad demográfica, calibración entre grupos y equidad individual, demostrando que estos criterios son frecuentemente mutuamente incompatibles[65]. Esta imposibilidad matemática de satisfacer simultáneamente nociones intuitivas diversas de equidad subraya que justicia algorítmica no es problema técnico resoluble mediante optimización sino cuestión fundamentalmente política sobre qué valores y compromisos deben estructurar sistemas sociotécnicos.

Benjamin argumenta que enfoque exclusivo en sesgo algorítmico puede obscurecer cómo tecnologías aparentemente neutrales participan en proyecto más amplio de lo que denomina *New Jim Code*, reproduciendo jerarquías raciales mediante diseño técnico presentado como objetivo y basado en datos[66]. Esta crítica sugiere que corrección técnica de algoritmos individuales es insuficiente sin transformación de estructuras sociales más amplias que generan patrones discriminatorios que algoritmos aprenden. La justicia algorítmica requiere no simplemente ajuste de modelos sino redistribución de poder sobre diseño, despliegue y gobernanza de sistemas que estructuran crecientemente vidas y oportunidades.

El análisis de sesgos y efectos discriminatorios demuestra que la cuestión no se limita a corregir errores técnicos, sino que interpela los fundamentos políticos del diseño sociotécnico contemporáneo. Ante tal diagnóstico, la crítica debe abrirse a la imaginación institucional y tecnológica de alternativas viables. En consecuencia, la sección siguiente explora futuros posibles y arquitecturas democráticas de tecnología orientadas a limitar la lógica extractiva dominante.

13. HACIA FUTUROS ALTERNATIVOS: IMAGINANDO ARQUITECTURAS DEMOCRÁTICAS DE TECNOLOGÍA

La crítica de vigilancia digital contemporánea debe complementarse con imaginación de alternativas posibles que preserven beneficios de tecnologías digitales mientras limitan capacidades de control y dominación. Movimientos por soberanía digital abogan por desarrollo de infraestructuras controladas democráticamente que prioricen autonomía individual y colectiva sobre maximización de extracción comercial[67]. Estas propuestas incluyen cooperativas de plataforma propiedad de usuarios, redes sociales descentralizadas basadas en protocolos federados y servicios públicos digitales operados por gobiernos o instituciones sin fines de lucro con mandatos de proteger derechos ciudadanos.

65 CHOULDECHOVA, Alexandra. "Fair prediction with disparate impact: A study of bias in recidivism prediction instruments". *Big Data. 2017,* vol 5, nº 2, pp. 153-163.

66 BENJAMIN, Ruha. *Race after technology: Abolitionist tools for the new jim code*. New Jersey: Polity Press, 2019, pp. 1-20.

67 MILAN, Stefanie; VAN DER VELDEN, Lonneke. "The alternative epistemologies of data activism". *Digital Culture & Society*, 2016, vol. 2, nº2, pp. 57-74.

El concepto de *privacy by design* propone integrar protección de privacidad en arquitecturas técnicas desde etapas iniciales de desarrollo en lugar de añadirla posteriormente mediante políticas o regulaciones[68]. Esto incluye técnicas como minimización de datos donde sistemas recolectan solamente información estrictamente necesaria, cifrado de punta a punta que impide acceso de proveedores de servicio a contenido de comunicaciones y procesamiento local en dispositivos que evita transmisión de datos sensibles a servidores centralizados. Estas estrategias técnicas pueden hacer ciertas formas de vigilancia técnicamente imposibles o prohibitivamente costosas, desplazando protección de privacidad desde políticas contingentes hacia restricciones arquitectónicas.

Tal reconfiguración arquitectónica debe resolver la denominada paradoja soberanía-internacionalismo, que describe la tensión estructural entre la necesidad del Estado de ejercer un control soberano sobre los sistemas algorítmicos y la naturaleza intrínsecamente transfronteriza de la infraestructura digital. Ante este escenario, emerge el modelo del Federalismo Digital, una estructura de gobernanza multinivel que integra el principio de subsidiariedad para coordinar la toma de decisiones entre los niveles local, nacional y global[69]. A diferencia de los modelos policéntricos descentralizados, este enfoque preserva la coordinación jerárquica necesaria para la rendición de cuentas, permitiendo que la regulación de la inteligencia artificial sea sensible al contexto cultural y político sin fragmentar la cooperación internacional indispensable para mitigar riesgos globales

Sin embargo, soluciones técnicas enfrentan límites estructurales en contextos de concentración corporativa masiva y dependencia de infraestructuras propietarias. Alternativas como redes sociales descentralizadas luchan por alcanzar masas críticas de usuarios frente a efectos de red que favorecen plataformas dominantes. Servicios que priorizan privacidad sobre conveniencia enfrentan desventajas competitivas porque vigilancia genera datos que permiten personalización y funcionalidades que usuarios valoran. Esta tensión sugiere que transformación tecnológica requiere cambios en modelos económicos y regulatorios que actualmente incentivan maximización de extracción de datos.

Morozov argumenta por ruptura radical con lógica de internet corporativo mediante construcción de infraestructuras públicas digitales concebidas como servicios esenciales comparables a agua, electricidad o transporte público[70]. Esta visión socialdemócrata digital imagina plataformas

68 CAVOUKIAN, Ann. "Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario".* Ontario, 2009, pp. 1-10.

69 ISHKHANYAN, Artur. "The sovereignty-internationalism paradox in AI governance: digital federalism and global algorithmic control". *Discover Artificial Intelligence*, 2025, vol. 5, nº 1, art. 123, pp. 1-6. Disponible en< https://doi.org/10.1007/s44163-025-00374-x>

70 MOROZOV, Evgeny. "Digital socialism? The calculation debate in the age of big data". *New*

operadas sin fines de lucro, financiadas públicamente y gobernadas democráticamente con participación ciudadana en decisiones sobre diseño y políticas. Los datos personales serían tratados como derechos inalienables que no pueden ser apropiados mediante consentimiento contractual, análogo a prohibiciones de venta de órganos o esclavitud voluntaria que reconocen que mercantilización de ciertos aspectos de persona humana es incompatible con dignidad.

Tales transformaciones requieren voluntad política para confrontar poder de corporaciones tecnológicas dominantes mediante regulación antimonopolio, tributación de ganancias extraordinarias derivadas de extracción de datos o incluso nacionalización de infraestructuras digitales críticas. El precedente histórico de regulación de industrias de red como telecomunicaciones o servicios públicos sugiere que monopolios naturales basados en efectos de red pueden justificar intervención estatal para proteger intereses públicos. Sin embargo, carácter transnacional de corporaciones digitales y dependencia de gobiernos de servicios proporcionados por estas compañías generan asimetrías de poder que complican enormemente regulación efectiva.

Las propuestas de soberanía digital y diseño centrado en la privacidad evidencian que la transformación requiere no solo innovación institucional, sino también sujetos capaces de comprender críticamente las infraestructuras que median su existencia. Sin una ciudadanía tecnopolíticamente alfabetizada, incluso las mejores reformas estructurales carecerían de sostén democrático duradero. Por ello, la sección siguiente aborda la educación crítica digital como dimensión estratégica de cualquier proyecto emancipador.

14. EDUCACIÓN CRÍTICA DIGITAL Y ALFABETIZACIÓN TECNOPOLÍTICA

Transformaciones estructurales deben complementarse con cultivo de capacidades críticas entre poblaciones para navegar y resistir vigilancia digital. La alfabetización digital tradicional enfocada en competencias técnicas básicas es insuficiente sin desarrollo de comprensión crítica de economía política de plataformas, funcionamiento de algoritmos y estrategias de protección de privacidad[71]. Esta alfabetización tecnopolítica incluye comprensión de cómo datos personales son extraídos, procesados y monetizados, habilidades para evaluar confiabilidad de información en ecosistemas saturados de desinformación y conocimiento de herramientas y prácticas para limitar exposición a vigilancia.

Sin embargo, pedagogías críticas digitales deben evitar responsabilizar exclusivamente a individuos por problemas estructurales. La retórica de responsabilidad personal obscurece asimetrías de poder fundamentales

Left Review. 2019, vol. 116/117, pp. 33-67.

71 PANGRAZIO, Lucy; SELWYN, Neil. "'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data". *New Media & Society*, 2019, vol.21, nº2, pp. 419-437.

donde corporaciones y estados poseen recursos y capacidades técnicas que exceden dramáticamente posibilidades de resistencia individual[72]. Estrategias individuales de protección de privacidad, aunque valiosas, no pueden sustituir transformaciones regulatorias y tecnológicas necesarias para construir ecosistemas digitales que respeten derechos fundamentales por diseño en lugar de exigir vigilancia perpetua y trabajo de autoprotección de usuarios.

La educación crítica también debe cultivar imaginación política para concebir alternativas al status quo tecnológico. La naturalización de modelos extractivos de plataformas como inevitables consecuencias de innovación tecnológica obscurece contingencia histórica de trayectorias de desarrollo que reflejan decisiones políticas y económicas específicas, no necesidades técnicas inherentes[73]. Pedagogías que historicen internet, examinando momentos de elección donde caminos alternativos fueron previsibles, pero no tomados, pueden desnaturalizar presente y abrir espacios para imaginar futuros diferentes. Esta imaginación utópica, lejos de ser escapismo, constituye precondición para acción política orientada hacia transformación.

CONCLUSIONES

Este análisis ha explorado la paradoja entre seguridad y libertad en la era digital desde perspectivas biopolíticas y filosóficas, argumentando que esta tensión no representa simplemente conflicto entre valores competitivos que pueden ser equilibrados mediante compromisos pragmáticos, sino que constituye contradicción estructural producida por arquitecturas tecnopolíticas contemporáneas. Las tecnologías de vigilancia digital no operan meramente restringiendo libertades preexistentes sino reconfigurando los términos mismos en que subjetividad, autonomía y poder son constituidos y experimentados.

El marco foucaultiano de biopolítica y gubernamentalidad proporciona herramientas conceptuales esenciales para comprender cómo vigilancia contemporánea trasciende modelos disciplinarios de modernidad temprana. Mientras instituciones disciplinarias operaban mediante confinamiento arquitectónico y supervisión jerárquica visible, la gubernamentalidad algorítmica opera mediante modulación continua en espacios aparentemente abiertos, produciendo sujetos que experimentan compulsión sistémica como expresión de libertad personal. Esta psicopolítica digital constituye forma de poder más sutil pero potencialmente más penetrante porque opera mediante producción de deseos y estructuración de elecciones en lugar de prohibición directa.

El capitalismo de vigilancia, como Zuboff articula, representa lógica

72 TUFEKCI, Zeynep. “Engineering the public: Big data, surveillance and computational politics”. *First Monday*, 2014, vol. 19, nº 7.

73 NOBLE, Safiya Umoja. *Algorithms of oppression: How search engines reinforce racism*. New York University Press, 2018, pp. 1-30.

económica distintiva donde experiencia humana es unilateralmente apropiada como materia prima para producción de mercancías predictivas. Esta convergencia entre imperativos comerciales y securitarios genera ensamblajes público-privados de vigilancia que evaden restricciones constitucionales tradicionales diseñadas para limitar poder estatal. La alienación producida por esta apropiación es doblemente mistificada porque sujetos experimentan plataformas extractivas como espacios de autoexpresión y realización, no reconociendo que prácticas valoradas generan valor económico capturado por corporaciones.

Las tecnologías específicas examinadas como reconocimiento facial, algoritmos predictivos y datificación biométrica introducen transformaciones cualitativas en modalidades de control social. El reconocimiento facial elimina anonimato en espacios públicos, generando registros permanentes de presencia que habilitan formas de rastreo y modulación conductual imposibles bajo regímenes de visibilidad previos. Los algoritmos predictivos invierten temporalidad de poder, operando preventivamente sobre campos de posibilidad en lugar de reactivamente a transgresiones manifiestas, socavando principios liberales de responsabilidad individual.

Las dimensiones geopolíticas y coloniales de vigilancia digital revelan continuidades entre apropiaciones imperiales históricas y extractivismo contemporáneo de datos, recursos y atención. La concentración de infraestructuras y capacidades algorítmicas en corporaciones transnacionales basadas en Norte Global genera flujos unidireccionales de extracción desde Sur Global, reproduciendo jerarquías globales en dominios digitales. La exportación de tecnologías de vigilancia a regímenes autoritarios por corporaciones democráticas subraya contradicciones entre valores proclamados y prácticas materiales del capitalismo digital.

Resolver esta paradoja requiere transformaciones simultáneas en múltiples niveles. Técnicamente, desarrollo de arquitecturas que incorporen protección de privacidad por diseño puede limitar capacidades de vigilancia mediante restricciones arquitectónicas en lugar de políticas contingentes. Regulatoriamente, marcos legales robustos que impongan límites obligatorios a recolección y procesamiento de datos, fortalezcan derechos de contestación de decisiones algorítmicas y fragmenten monopolios de plataforma mediante regulación antimonopolio son esenciales. Económicamente, exploración de modelos alternativos como cooperativas de plataforma, servicios públicos digitales y tratamiento de datos como derechos inalienables puede romper lógica extractiva dominante [74].

Este trabajo ha argumentado que la tensión entre seguridad y libertad en la era digital no puede resolverse mediante equilibrios pragmáticos dentro de marcos conceptuales heredados de modernidad temprana. Las

74 MOROZOV, Evgeny. "Digital socialism? The calculation debate in the age of big data". *New Left Review.* 2019, vol. 116/117, pp. 33-67. Op. cit. p. 33-67.

transformaciones cualitativas introducidas por tecnologías algorítmicas requieren repensamiento fundamental de categorías políticas, desarrollando marcos normativos adecuados para condiciones donde poder opera mediante modulación y producción de subjetividad en lugar de coerción directa. La tarea crítica urgente es construir coaliciones capaces de confrontar poder de corporaciones y estados que se benefician de vigilancia ubicua, imaginando y materializando alternativas que protejan dignidad humana y autonomía colectiva sin sucumbir a ilusiones de seguridad absoluta o transparencia total.

Las libertades fundamentales que sociedades democráticas proclaman proteger requieren espacios de opacidad donde individuos y colectivos puedan experimentar, disentir y desarrollarse sin supervisión perpetua. La paradoja contemporánea es que estas libertades son simultáneamente celebradas discursivamente y erosionadas materialmente mediante infraestructuras que hacen privacidad técnicamente imposible y comportamiento disidente identificable y sancionable. Resolver esta contradicción demanda no simplemente regulación de tecnologías específicas sino transformación de estructuras económicas y políticas que incentivan vigilancia, construyendo instituciones democráticas capaces de gobernar poderes tecnológicos que actualmente operan como soberanías extraterritoriales.

El futuro de libertad en sociedades digitales depende de capacidad colectiva para resistir naturalizaciones que presentan configuraciones tecnológicas actuales como inevitables, recuperando agencia política sobre diseño de infraestructuras que estructuran crecientemente existencia cotidiana. Esta tarea es simultáneamente técnica, legal, económica y cultural, requiriendo alianzas entre movimientos sociales, comunidades técnicas, legisladores y ciudadanos comprometidos con visión de tecnología como instrumento de emancipación colectiva en lugar de dominación. La paradoja de seguridad y libertad solo puede ser resuelta mediante rechazo de términos en que actualmente se plantea, construyendo alternativas que reconozcan interdependencia de autonomía individual, solidaridad colectiva y gobernanza democrática de poder tecnológico.

CONFLICTO DE INTERÉS

El autor declara no tener conflicto de interés en el artículo presentado.

FINANCIAMIENTO

El autor participó en la conceptualización, investigación, metodología, recursos y redacción del manuscrito, no contó con financiamiento para su elaboración.

REFERENCIAS BIBLIOGRÁFICAS

AGAMBEN, Giorgio. *State of exception*. Chicago: University of Chicago Press, 2005.

AMOORE, Louise. *The politics of possibility: Risk and security beyond*

probability. Durham: Duke University Press, 2013.

ANANNY, Mike; CRAWFORD, Kate. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability." *New Media & Society*, 2018, vol. 20, nº3, pp. 973-989.

ANDREJEVIC, Mark. *iSpy: Surveillance and power in the interactive era*. Kansas: *University Press of Kansas, 2007*.

ARADAU, Claudia; VAN MUNSTER, Rens. "Governing terrorism through risk: Taking precautions, (un)knowing the future." *European Journal of International Relations*, 2007, vol.13, nº1, pp. 89-115.

BALL, Kirstie; WEBSTER, Frank. *The intensification of surveillance: Crime, terrorism and warfare in the information age*. Londres: Pluto Press, 2003.

BAROCAS, Solon; NISSENBAUM, Helen. "Big data's end run around anonymity and consent". In J. LANE, V. STODDEN, S. BENDER, & H. NISSENBAUM (Eds.), *Privacy, big data, and the public good.* Cambridge: Cambridge University Press, 2014, pp.44-75.

BAROCAS, Solon; SELBST, Andrew. D. "Big data's disparate impact". *California Law Review*, 2016, vol.104, pp. 671-732. Disponible en: <https://doi.org/10.15779/Z38BG31>

BENJAMIN, Ruha. *Race after technology: Abolitionist tools for the new jim code*. New Jersey: Polity Press, 2019.

BRUNTON, Finn; NISSENBAUM, Helen. *Obfuscation: A user's guide for privacy and protest*. Cambridge: MIT Press, 2015.

BURRELL, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms". *Big Data & Society.* 2016, vol 3, nº1, pp. 1-12. Disponible en: <https://doi.org/10.1177/2053951715622512>

CAVOUKIAN, Ann. "Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario".* Ontario, 2009.

CHENEY-LIPPOLD, John. *We are data: Algorithms and the making of our digital selves*. New York University Press, 2017.

CHOULDECHOVA, Alexandra. "Fair prediction with disparate impact: A study of bias in recidivism prediction instruments". *Big Data. 2017,* vol 5, nº 2, pp. 153-163.

COHEN, Julien E. *Configuring the networked self: Law, code, and the play of everyday practice*. Yale University Press, 2012.

COULDRY, Nick; MEJIAS, Ulises. A. *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press, 2019.

DANAHER, Juan. "The threat of algocracy: Reality, resistance and accommodation." *Philosophy & Technology*, 2016, vol. 29, nº3, pp. 245-268.

DELEUZE, Guilles. "Postscript on the societies of control". *October*, 1992, vol. 59, pp. 3-7.

FELDSTEIN, Steven. *The global expansion of AI surveillance*. Carnegie Endowment for International Peace, 2019.

FERGUSON, Andrew Guthrie. *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York: New York University Press, 2017.

FINN, Rachel L.; WRIGHT, David; FRIEDEWALD, Michael." Seven types of privacy. In GUTWIRTH Serge; LEENES Ronald; DE HERT Paul; POULLET Yves (Eds.), *European data protection: Coming of age. Dordrecht: Springer, 2013,* pp. 3-32.

FOUCAULT, Michel. *The history of sexuality, Volume 1: An introduction*. New York: Pantheon Books, 1978.

FOUCAULT, Michel. *Discipline and punish: The birth of the prison*. Random House, 1975.

FOUCAULT, Michel. *Security, territory, population: Lectures at the Collège de France 1977-1978*. Palgrave Macmillan, 2007.

FUCHS, Christian. "A contribution to the critique of the political economy of Google." *Fast Capitalism*. 2011, vol. 8, nº1. Disponible en: <https://doi.org/10.32855/fcapital.201101.006>

GANDY, Oscar H. *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Ashgate Publishing. 2009.

GATES, Kelly A. *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press. 2011.

GRAHAM, Mark; HALE, Scott A; STEPHENS, M. Geographies of the world's knowledge. *Convoco Foundation*. 2014.

HAGGERTY, Kevin D.; Ericson, Richard V. "The surveillant assemblage". *British Journal of Sociology*, vol. 51, nº 4, 2000, pp. 605-622.

HAN, Byung-Chul. *Psychopolitics: Neoliberalism and new technologies of power*. Verso Books. 2014.

HARCOURT, B. E. *Against prediction: Profiling, policing, and punishing in an actuarial age*. University of Chicago Press. 2007.

HAYEK, Friedrich A. *Camino de servidumbre*. Trad. de José Vergara. Madrid: Alianza Editorial, 2007.

HOBBES, Thomas. *Leviathan*. Londres: Andrew Crooke, 1651.

ISHKHANYAN, Artur. "The sovereignty-internationalism paradox in AI governance: digital federalism and global algorithmic control". *Discover Artificial Intelligence*, 2025, vol. 5, nº 1, artículo 123. Disponible en: < https://doi.org/10.1007/s44163-025-00374-x>

LEVY, Neil. "Echoes of COVID misinformation". *Philosophical Psychology.* 2021, vol. 34, nº 3, pp.417-433.

LIANG, Fan; DAS, Vishnupriya; KOSTYUK, Nadiya; HUSSAIN, Muzammil M." Constructing a data-driven society: China's social credit system as a state surveillance infrastructure". *Policy & Internet*, 2018, vol.10, nº4, pp. 415-453.

LOCKE, Juan. (1689). *Two treatises of government*. Cambridge University Press, 1689.

LUPTON, Deborah. *The quantified self: A sociology of self-tracking*. Cambridge: Polity Press. 2016.

LYON, David. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique". *Big Data & Society*, 2014, vol. 1, nº 2, pp. 1-11. Disponible en: < <https://doi.org/10.1177/2053951714541861>

LYON, David. *Surveillance society: Monitoring everyday life*. Open University Press. 2001.

MARX, Gary T. *Windows into the soul: Surveillance and society in an age of high technology*. University of Chicago Press. 2016.

McSTAY, Andrew. *Emotional AI: The rise of empathic media*. SAGE Publications, 2018.

MILAN, Stefanie; VAN DER VELDEN, Lonneke. "The alternative epistemologies of data activism". *Digital Culture & Society*, 2016, vol. 2, nº2, pp. 57-74.

MILL, John Stuart. *On liberty*. Londres: John W. Parker and Son, 1859.

MOROZOV, Evgeny. "Digital socialism? The calculation debate in the age of big data". *New Left Review.* 2019, vol. 116/117, pp. 33-67.

NISSENBAUM, Helen. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2010.

NOBLE, Safiya Umoja. *Algorithms of oppression: How search engines reinforce racism*. New York University Press, 2018.

O'NEIL, Cathy. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing, 2016.

PANGRAZIO, Lucy; SELWYN, Neil. "'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data". *New Media & Society*, 2019, vol.21, nº2, pp. 419-437.

PARISER, Eli. *The filter bubble: What the internet is hiding from you*. Penguin Press, 2011.

PASQUALE, Frank. *The black box society: The secret algorithms that control money and information*. Harvard University Press, 2015.

PIERUCCI, Federico. "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace". *Digital Society*, 2025, vol. 4, nº 27. Disponible en: < https://doi.org/10.1007/s44206-025-00189-4>

ROSE, Nicholas. *Powers of freedom: Reframing political thought*. Cambridge University Press, 1999.

ROUVROY, Antoinette; BERNS, Thomas. "Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships?". *Réseaux.* 2013, vol. 177, nº1, pp.163-196. Disponible en: <https://doi.org/10.3917/res.177.0163>

ROWE, Frantz. « Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world". *International Journal of Information Management*,

2020, vol. 55, artículo 102178. Disponible en:<https://doi.org/10.1016/j.ijinfomgt.2020.102178>

TUFEKCI, Zeynep. "Engineering the public: Big data, surveillance and computational politics". *First Monday*, 2014, vol. 19, nº 7. Disponible en: < https://doi.org/10.5210/fm.v19i7.4901>

VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer, 2017.

WILLIAMS, J. *Stand out of our light: Freedom and resistance in the attention economy*. Cambridge University Press, 2018.

YE, Xiongbiao; YAN, Yuhong; LI, Jia; JIANG, Bo. "Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective". *Telecommunications Policy*, 2024, vol. 48, nº 10, artículo 102851. Disponible en: <https://doi.org/10.1016/j.telpol.2024.102851>

ZUBOFF, Shoshana. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs, 2019.

RESUMEN BIOGRÁFICO

Fernando Ramos-Zaga. Abogado. Licenciado en Administración. Magister en Gerencia Social. Magíster en Informática y Tecnología Educativa. Magister en Derecho de la Empresa. Magister en Gestión Pública. Su trabajo académico se concentra en la bioética, filosofía del derecho, regulación de nuevas tecnologías y economía del comportamiento, campos en los que se articulan enfoques interdisciplinarios para analizar las implicancias sociales de la innovación.
mail: fernandozaga@gmail.com
ORCID: http://orcid.org/0000-0001-6301-9460