SEGURIDAD HIPNÓTICA: DESDE HOBBES AL PANÓPTICO DIGITAL

HYPNOTIC SECURITY: FROM HOBBES TO THE DIGITAL PANOPTICON

José María Seco Martínez
Universidad Pablo de Olavide, Sevilla, España
jmsecmar@upo.es
Orcid id: https://orcid.org/0000-0001-5468-6122

Recibido: julio de 2025
Aceptado: octubre de 2025

Palabras clave: seguridad, tecno-capitalismo, vigilancia, democracia, algoritmos, biopolítica, "securitización", datos, demopedia, transparencia
Key words: security, techno-capitalism, surveillance, democracy, algorithms, biopolitics, "securitization", data, demopedia, transparency

Resumen: En este artículo se analiza críticamente la transformación del concepto de seguridad desde la modernidad clásica hasta la era tecno-capitalista actual, y sus implicaciones para la democracia. Mediante una genealogía que parte de la teoría hobbesiana del Estado Leviatán hasta los desafíos digitales de 2025, se muestra cómo la noción de seguridad ha pasado de ser una garantía frente al miedo y la violencia a convertirse en un dispositivo ideológico que estabiliza el statu quo del capitalismo global. El marco teórico combina la crítica ideológica, la biopolítica, la teoría de la "securitización" y el estudio de la vigilancia de datos para tratar de desentrañar los mecanismos contemporáneos de control social algorítmico. Se abordan casos actuales -como el Reglamento de Inteligencia Artificial de la UE (2024), la reautorización de la FISA §702 en EEUU (2024) y los cambios algorítmicos en Twitter/X (2024) - que ejemplifican la tensión entre seguridad, tecnología y libertades. Finalmente, a la hora de concluir se anticipan, para su posterior desarrollo, iniciativas (demopedia, transparencia algorítmica, sindicatos de datos, plataformas públicas) para reconducir la seguridad hacia el interés público democrático.

Abstract: His article critically analyzes the transformation of the concept of security from classical modernity to the current techno-capitalist era, and its implications for democracy. Through a genealogy that traces the evolution from Hobbes's theory of the Leviathan State to the digital challenges of 2025, it shows how the notion of security has shifted from being a guarantee against fear and violence to becoming an ideological device that stabilizes the status quo

of global capitalism. The theoretical framework combines ideological critique, biopolitics, securitization theory, and data surveillance studies to unravel the contemporary mechanisms of algorithmic social control. Current cases—such as the EU Artificial Intelligence Act (2024), the reauthorization of FISA §702 in the United States (2024), and the algorithmic changes in Twitter/X (2024)—illustrate the tension between security, technology, and freedom. Finally, the conclusion anticipates, for further development, several initiatives (demopedia, algorithmic transparency, data unions, and public platforms) aimed at redirecting security toward the democratic public interest.

1. Introducción

A principios del siglo XX, Elizabeth Magie creó un juego llamado The Landlord`s Game, precursor del popular *Monopoly,* que ofrecía dos modalidades claramente opuestas. La versión estrictamente monopolista celebraba la acumulación individual de la riqueza, la competición despiadada y el beneficio egoísta. Por otro lado, la modalidad "Prosperity" promovía un modelo cooperativo centrado en el bienestar colectivo y en la justicia social. En esta modalidad, los impuestos y las multas recaudados no terminaban en manos de un banco anónimo, sino que se colocaban en un fondo común al alcance de todos los jugadores para cuando estos lo necesitasen, encarnando así los ideales de solidaridad y de responsabilidad compartida.

En 1935, Parker Brothers adquirió la patente del juego y decidió deliberadamente eliminar la modalidad cooperativa "Prosperity", optando exclusivamente por la versión monopolista. Sobra decir que esta decisión no fue simplemente una mera elección comercial; simbolizaba algo más: la consolidación ideológica de un modelo que privilegia la codicia personal, la competencia ilimitada y la acumulación individualista, relegando al margen cualquier atisbo de lógica cooperativa y/o de bienestar social.

Hoy, en plena era tecno-capitalista, la noción de seguridad experimenta una transformación similar. La seguridad, que inicialmente representaba un pacto colectivo para enfrentar el miedo, la incertidumbre y la violencia, ha evolucionado hacia un entramado muy complejo de vigilancia algorítmica y de control predictivo dominado por corporaciones tecnológicas como Google, Amazon, Facebook/Meta, Apple y Microsoft. Estas empresas acumulan y explotan enormes cantidades de datos personales para predecir y manipular comportamientos individuales y colectivos, siempre bajo la misma promesa de certidumbre pero generando nuevas formas de exclusión y vigilancia ubicua.

El concepto original de seguridad, entendido como fondo común necesario para el bienestar de todos, está siendo desplazado por un sistema privatizado y tecnificado que privilegia intereses corporativos y reproduce nuevas desigualdades sociales. Este trabajo busca precisamente rescatar esa otra visión democrática, ahora supeditada, de la seguridad, re-introduciendo principios como el de transparencia, el de cooperación, el de solidaridad y, como no, el de corresponsabilidad ciudadana, como contrapunto esencial al dominio tecno-capitalista actual.

Esta transformación de la idea de seguridad - de garantía colectiva a mecanismo

ideológico de control algorítmico - es el tema central que guía el análisis crítico de este trabajo. Comenzaremos explorando sinópticamente cómo desde la teoría del Leviatán de Hobbes a la lógica hipnótica de las plataformas digitales contemporáneas, la seguridad ha servido no solo como medio de protección, sino como dispositivo clave para mantener el *statu quo* que el orden tecno-capitalista necesita.

Ahora bien, ¿no será esta retórica de la seguridad otra forma más de naturalizar la preservación del *statu quo*? Dicho de otra manera, la seguridad operaría como una suerte de dispositivo ideológico que vendría a legitimar de manera muy sutil, casi subliminal, políticas y estructuras que concentran el poder en élites político-económicas, frenando la llegada de cambios radicales. En la era del tecno-capitalismo, marcada por plataformas digitales que todo lo abarcan y por la extracción masiva de datos, la seguridad adquiere un nuevo cariz: ya no se trata solo de prevenir delitos o ataques, sino de gestionar la conducta de poblaciones enteras mediante algoritmos, el big data y la vigilancia ubicua. De este modo, la idea de seguridad provee la coartada perfecta para intensificar la recolección de datos personales y el control social, siempre bajo la promesa de mayores dosis de eficiencia y orden.

Esta es la tesis *peregrin*i de la que aquí partimos: que la noción contemporánea de seguridad ha dejado de ser un valor neutral orientado a proteger a la ciudadanía, para convertirse en un mecanismo de estabilización del orden tecno-capitalista. Lejos de garantizar libertades, la seguridad neoliberal y algorítmica desplaza el poder de decisión fuera de la soberanía popular -hacia mega-corporaciones tecnológicas y órganos opacos. Lo que antes se entendía como la necesaria protección de la comunidad se ha metamorfoseado ahora en una suerte de neo-gestión tecnificada de los riesgos, cuyo fin último no es otro que neutralizar conflictos y salvaguardar la acumulación capitalista, aun a costa de todo lo demás.

Nuestra contribución aquí, por tanto, es triple. Primero, ofrecemos una breve genealogía histórica (1651-2025) que revela cómo la seguridad ha sido redefinida en cada etapa del desarrollo capitalista: desde el Leviatán de Hobbes hasta la "sociedad de la vigilancia" de Zuboff. Después, articulamos un marco teórico interdisciplinar -crítica ideológica, crítica biopolítica desde Foucault, teoría de la "securitización" y estudios de vigilancia- para elucidar que la seguridad es una construcción política e ideológica y no tanto una condición objetiva. Y, tercero, analizamos casos empíricos recientes en Europa y EEUU que ilustran cómo opera este afán por la "securitización" algorítmica y cuáles son sus resistencias, anticipando al final, algunas alternativas (como la *demopedia* o los sindicatos de datos) para reequilibrar la relación entre tecnología, seguridad y democracia.

Con este recorrido, esperamos demostrar la necesidad de un enfoque crítico que "deshipnotice" el discurso de la seguridad y reubique al *demos* en el centro del control sobre las tecnologías.

2. Genealogía de la seguridad (1651-2025)

La historia moderna de la seguridad puede trazarse desde la temprana era hobbesiana hasta nuestro presente hiper-tecnológico. Hobbes, en su obra *Leviatán* (1651),

sentó las bases del imaginario moderno de la seguridad: en el estado de naturaleza la vida humana era "solitaria, pobre, desagradable, brutal y demasiado corta" por el miedo constante a la muerte violenta; de ahí que los individuos acuerden ceder parte de su libertad a un poder soberano absoluto que garantice la paz y el orden. El Leviatán hobbesiano -representado aquí como un gigante formado por la suma de los ciudadanos, empuñando la espada y un cetro en su frontispicio- encarna de sobra la idea de que no existe poder en la Tierra que se le compare ("*Non est potestas super terram quae comparetur ei*", Job 41:24)[1]. En la concepción de Hobbes, la seguridad del Estado es la única condición de posibilidad de la vida civilizada: solo un poder central, como concentración objetiva de la fuerza, puede disipar el miedo y, por tanto, permitir el auge de las actividades humanas más constructivas (el comercio, el arte, la ciencia, la filosofía, etc) libres ya del caos de la guerra civil. De este modo, la seguridad en el liberalismo clásico quedó asociada primariamente a la protección jurídico-militar, esto es, a reprimir el crimen interno, a garantizar la propiedad y a hacer frente a los enemigos externos. El Estado, debía infundir suficiente temor como para disuadir la violencia doméstica y a la vez proteger a sus súbditos de agresiones extranjeras.

Con la llegada de la modernidad, especialmente tras la Revolución Industrial y el ascenso del capitalismo como sistema económico dominante, la seguridad pasó a convertirse en un aspecto creciente de la estabilidad económica y social de la sociedad capitalista. Ya no se trataba únicamente de proteger fronteras, sino de garantizar el orden que posibilitara la acumulación de capital, el intercambio comercial y el desarrollo de las fuerzas productivas. Paulatinamente, el concepto de seguridad se fue ramificando hacia la protección de las transacciones mercantiles, la seguridad jurídica de la propiedad y la confianza de los inversores en la continuidad del sistema.

Por tanto, durante los siglos XVIII y XIX, a medida que se consolidaban el Estado de Derecho y las repúblicas liberales, la noción de seguridad se fue expandiendo más allá de lo meramente militar. Surgieron las policías modernas y los sistemas judiciales para mantener el orden interno de forma institucionalizada, así como las primeras redes de "seguridad social" para mitigar los riesgos de pobreza, las enfermedades y la vejez que aparejaban las nacientes sociedades industriales. La seguridad empezaba a contemplarse así, desde una perspectiva más amplia, como una forma de *bienestar público* - ahí estaban ya la "seguridad sanitaria" o la "se-

1. Basta con echarle un vistazo al grabado original de Abraham Bosse para la portada de *Leviatán* (1651). En el centro, se alza una figura colosal que fusiona lo divino y lo político: un soberano coronado cuya silueta, al observarse de cerca, está compuesta por cientos de pequeños cuerpos humanos - sus súbditos -, representando visualmente la idea hobbesiana de que el poder del Estado surge de la cesión de las voluntades individuales. En su mano derecha empuña una espada (símbolo del poder militar) y en la izquierda un cetro (símbolo del poder eclesiástico), afirmando su soberanía absoluta sobre lo temporal y lo espiritual. El fondo muestra un paisaje dividido entre una ciudad fortificada y el campo abierto, remarcando el contraste entre el caos del estado de naturaleza y el orden civil bajo el Leviatán. En la parte superior, la cita del *Libro de Job* consagra su autoridad como incomparable en la Tierra. Esta imagen encarna, en clave visual, la tesis de Hobbes: que solo el sometimiento al poder soberano garantiza la seguridad y la vida social; el punto de partida de la genealogía crítica que aquí se desarrolla

guridad social"-, aunque eso sí, siempre supeditadas a la estabilidad del orden liberal burgués y a su propia ética (libertad económica, protección de la propiedad privada y cumplimiento de los contratos).

No obstante, con la entrada en el siglo XX y especialmente tras la Segunda Guerra Mundial, el término "seguridad" se recargó aún más. Esta vez de contenido geopolítico. La Guerra Fría alumbró la idea de seguridad nacional, justificando la creación de vastos complejos militar-industriales y aparatos de inteligencia para contener la amenaza enemiga (a la sombra del discurso bipolar capitalismo/comunismo). La estabilidad del propio sistema mundial pasó a articularse así en torno al concepto de seguridad, pero ahora elevado a prioridad absoluta de Estado en todas las superpotencias.

Pero ya en la década de los 90, llega un punto de inflexión en esta genealogía: la transición hacia la llamada "sociedad del riesgo". El sociólogo Ulrich Beck (Beck: 1992) introdujo este concepto para describir una nueva fase del desarrollo de la modernidad en la que los riesgos sociales, políticos, económicos e industriales comenzaban a escaparse del control de las instituciones tradicionales. Mientras que en la sociedad industrial el foco se situaba en la distribución de la riqueza, en la sociedad del riesgo la atención se centra en la distribución de los riesgos, como producto del propio proceso de modernización y desarrollo tecnológico. A diferencia de las amenazas naturales del pasado, los riesgos contemporáneos (como la contaminación ambiental, los accidentes nucleares, las crisis financieras, el terrorismo transnacional, las pandemias, etc…) generan riesgos sistémicos cada vez más complejos, que difuminan las fronteras entre la seguridad interna y la externa, entre otras cosas porque tales riesgos ya no entienden ni de fronteras ni de clases sociales. Un auténtico desafío para las estructuras políticas y sociales tradicionales, que ahora tienen que adaptarse para gestionar las incertidumbres de esta nueva era.

La seguridad, en consecuencia, deja de ser un asunto acotado al territorio y a la soberanía estatal, para extenderse prácticamente a todos los ámbitos de la vida: seguridad energética, alimentaria, medioambiental, económica, informática, etc. Ahora la promesa es otra: controlar la incertidumbre en cualquier campo mediante la anticipación técnica de los riesgos. En palabras de Beck, vivimos en una época obsesionada por evitar cualquier sorpresa desagradable, lo que paradójicamente engendra nuevas formas de incertidumbre al confiar ciegamente en sistemas tecnológicos que también pueden fallar.

Los atentados del 11 de septiembre de 2001 marcaron otra vuelta de tuerca en esta etapa crucial: inauguraron la era de la "seguridad global" y de la "guerra contra el terror", desde la cual los Estados occidentales expandieron, como nunca antes, sus poderes de vigilancia y coerción alegando prevenir amenazas terroristas difusas. Bajo el efecto del 11-S, la retórica política consolidó la percepción de un estado de excepción permanente (Agamben, 2005) donde, en nombre de la seguridad, se suspenden o recortan garantías legales. Se aprobaron leyes como la *USA PATRIOT Act* (2001) en EEUU que ampliaron la vigilancia estatal sobre las comunicaciones y las actividades privadas. Del mismo modo, en Europa se establecieron políticas antiterroristas y de

uso de datos, que permitieron la retención masiva de registros telefónicos e Internet. El procedimiento siempre es el mismo: se aprovecha la urgencia post-crisis para implementar medidas extraordinarias que luego se normalizan. Los ciudadanos, atemorizados, aceptamos mayores dosis de control a cambio de promesas de seguridad, lo que gradualmente va desdibujando la frontera entre legalidad ordinaria y excepcionalidad. Esta dinámica las hemos visto muchas veces desde entonces: en la crisis financiera de 2008 (rescate de instituciones bancarias sin escrutinio ciudadano, recortes generalizados en servicios públicos, etc), tras los atentados en Europa (en Londres 2005, en París 2015, etc.) y durante la pandemia de COVID-19, en la que muchos gobiernos, entre ellos el nuestro, asumieron poderes de excepción.

El resultado no ha sido otro que la consolidación de un nuevo paradigma de la seguridad bajo el cual el Estado actúa desde una lógica militar/policial, incluso en tiempos de paz, con el consiguiente debilitamiento de las instituciones del Estado de derecho. El ejemplo más reciente lo tenemos en las protestas masivas que estallaron tras las redadas realizadas por ICE, por las políticas anti-migratorias de Trump, en diversos puntos de Los Ángeles entre el 6 y el 18 de junio de 2025. La declaración gubernativa de asambleas ilegales, los arrestos masivos (que superaron los 850 detenidos), y la aplicación de toques de queda, junto a un despliegue policial descomunal y la llegada de la Guardia Nacional junto a 700 marines. Estas acciones, justificadas por las autoridades como necesarias para restaurar el orden, ejemplifican hasta qué punto se van incorporado prácticas excepcionales en la gestión de la seguridad cotidiana, validando la lógica militar/policial incluso sin un estado de emergencia real.

Pero es que hay que añadir un factor nuevo: la irrupción de un nuevo actor, si cabe, más protagonista. Nos referimos a las corporaciones tecnológicas y a la infraestructura digital global. Con el auge del big data, la seguridad dejó de apoyarse únicamente en el monopolio estatal de la violencia para volcarse en el monitoreo masivo de información y en la predicción algorítmica del comportamiento. Este desplazamiento desde la protección *ex post* a la predicción *ex ante* del riesgo encarna lo que algunos autores como Deleuze ya denominaron, hace más de 30 años, el paso de una sociedad disciplinaria a una sociedad de control (Deleuze: 1990). Ya no se trata tanto de castigar infracciones cometidas, como de prevenir que estas ocurran, anticipándose a ellas estadísticamente. La lógica del riesgo sube de escalón y se convierte el algo más: en el factor decisivo en la gestión cotidiana de la política. Ahora la seguridad es la consigna decisiva a la hora de movilizar los recursos, ya sean públicos o privados, porque ahora deviene esencial conjurar cualquier tipo de situación que amenace o pueda amenazar la continuidad del orden existente, desde la volatilidad financiera hasta la más mínima protesta social (Neocleous: 2008).

De la mano de esta "mutación digital" de la seguridad, las grandes empresas tecnológicas -Google, Amazon, Facebook/Meta, Apple, Microsoft, Twiter/X, etc.-, no solo ejercen como actores centrales de la economía mundial (V. Srnicek: 2017), sino que se sitúan a la par de los Estados. Manejan tal volumen de información y de datos personales, controlan de tal manera a las infraestructuras críticas de comunicación, que han pasado a convertirse en los guardianes de facto de la seguridad informacional de millones de personas.

Gobiernos de todo el mundo se apoyan en sus soluciones tecnológicas y en sus plataformas para fines de seguridad (desde la vigilancia antiterrorista hasta el seguimiento de contagios).

Ejemplos hay muchos. Pensemos en uno de los más notorios: el de Palantir Technologies, compañía de big data fundada con capital de riesgo de la CIA, que provee software de análisis predictivo a agencias de inteligencia, departamentos de policía y ejércitos. O en el caso (este más sonado aquí en España por sus vinculaciones con el llamado Catalangate español) del NSO Group - la empresa israelí creadora del spyware *Pegasus*, que vende a gobiernos la capacidad de infiltrar teléfonos móviles y extraer toda su información[2]. Estas alianzas público-privadas han ido tejiendo una suerte de consorcio de vigilancia masiva, donde el Estado externaliza sus capacidades de control en manos privadas legitimando la intrusión en la vida de las personas bajo el mantra de la "seguridad nacional". La influencia de tales corporaciones es de tal envergadura en las políticas de seguridad de ciertos países, que los límites entre el poder estatal y el corporativo comienzan ya a difuminarse.

En fin, lo que venimos a elucidar aquí es cómo ha ido evolucionando este proceso histórico de ampliación y/o abstracción del concepto de seguridad: de la espada del soberano hobbesiano que garantiza la paz interna, a la policía y al Estado social que protege el orden liberal-capitalista; para luego transitar hacia la seguridad nacional militarizada durante la Guerra Fría, y finalmente acabar hoy en la seguridad difusa y ubicua del capitalismo digital global.

En todas estas etapas, la seguridad se ha erigido en una suerte de acelerador de la vida política, pero también -y este es un eje crítico de nuestro análisis- como un discurso legitimador que puede llegar a encubrir la preservación de jerarquías y privilegios. Hoy, en 2025, la seguridad se disfraza de alta tecnología e "inteligencia artificial", prometiendo soluciones infalibles a la incertidumbre. Empero, esta promesa tiene también un reverso oscuro: opera asimismo como una estrategia para blindar el modelo tecno-capitalista dominante, enmascarando sus desigualdades bajo la retórica neutral de la gestión eficiente de los riesgos. La pregunta que subyace a este análisis es siempre la misma. Seguridad, sí, pero, *"¿para quién?"*. Entender cómo hemos llegado aquí es el primer paso para develar ese interrogante.

2. Este programa espía, una vez instalado de forma encubierta en un teléfono móvil -incluso sin necesidad de que el usuario haga clic en ningún enlace -, permite el acceso total al dispositivo: mensajes, llamadas, correos electrónicos, cámara y micrófono incluidos. Aunque NSO afirma vender *Pegasus* únicamente a gobiernos para combatir el crimen organizado y el terrorismo, se ha desvelado su uso contra activistas, periodistas, abogados y opositores políticos. En nuestro caso, el escándalo estalló en 2022 cuando se conoció que los móviles de más de 60 dirigentes independentistas catalanes - incluidos civiles y diputados autonómicos de Cataluña - fueron presuntamente infectados con *Pegasus*, en lo que se conoció como "Catalangate". Posteriormente, también se descubrió que los móviles del presidente Pedro Sánchez y de las ministras Margarita Robles y Fernando Grande-Marlaska fueron también infectados, aunque en este caso se atribuyó la autoría a agentes externos no identificados. La polémica generó una grave crisis institucional sobre los límites de la vigilancia estatal, el control democrático de los servicios de inteligencia y la falta de transparencia en la adquisición y uso de estas tecnologías de intrusión.

3. Marco teórico y metodología: crítica ideológica, biopolítica, "securitización" y vigilancia de datos

Para este análisis el enfoque teórico por el que hemos querido transitar es, desde luego, crítico e interdisciplinar. Nuestro marco se apuntala en cuatro pilares: (i) en la crítica ideológica (particularmente desde la teoría crítica), (ii) en el concepto foucaultiano de biopolítica, (iii) en la teoría de la "securitización" proveniente de los estudios de seguridad y de las relaciones internacionales, y (iv) en los estudios de vigilancia de datos y capitalismo de vigilancia.

i) *Crítica ideológica*: Partimos de la premisa de que las ideas y los discursos sobre la seguridad no son neutros ni universales; antes bien cumplen una función ideológica en el sentido marxiano/gramsciano: legitiman ciertas relaciones de poder presentándolas como necesarias o naturales. Por tanto, una de las tesis *peregrini* de la que aquí partimos podría resumirse así: la seguridad, en su formato neoliberal y tecnológicamente más actualizado, ha dejado de actuar como lo que quiso ser, una garantía para las libertades y los derechos de las personas, para convertirse ahora en un mecanismo de estabilización del orden tecno-capitalista. Al cabo, aquello que se definía clásicamente como el "resguardo necesario de la comunidad" se ha ido convirtiendo progresivamente en un dispositivo ideológico de gestión de los riesgos diseñado exclusivamente para neutralizar conflictos y salvaguardar la dinámica de acumulación, incluso a costa de nuestros derechos esenciales y de la vitalidad de nuestras democracias. Podríamos decir que la idea de seguridad se ha convertido así en la "religión civil" del capitalismo (Neocleous, 2008), incuestionable e incuestionada, pero utilizada para justificar desde políticas públicas cada vez más autoritarias, hasta gastos militares desorbitados. Para muestra un botón: pensemos en la última cumbre de la OTAN en la Haya donde todos los Estados (salvo el español), se han comprometido a invertir hasta el 5% del PIB en defensa hasta el 2035.

La crítica ideológica implica aquí "desenmascarar" cómo esta retórica de la seguridad puede ocultar intereses particulares (piénsese por ejemplo en la protección de inversiones corporativas presentada como seguridad "económica" general); o industriales a través de entramados empresariales-estatales (militar[3], tecnológico, consultoras, etc.) que se benefician materialmente de la perpetua demanda de seguridad. En este sentido, esta especie de "economía de la vigilancia" resulta muy útil: numerosas empresas privadas compiten por vender soluciones de seguridad (desde cámaras de reconocimiento facial hasta software de análisis de re-

3. Por ejemplo, el 5 de junio de 2025 los ministros de defensa respaldaron elevar el límite del 2% del PIB a la OTAN hasta el 5 % del PIB, formalizando así que el rearme no es excepcional sino estructural. Paralelamente, el presupuesto militar común de la Alianza para 2025 representa un salto de casi un 18 % frente a 2024. Alemania ilustra esta deriva: tras el fondo especial de 100 000 000 000 EUR aprobado en 2022, Berlín proyecta un gasto ordinario por encima de 60 000 000 000 EUR anuales, quebrando de facto su "freno de la deuda" constitucional. Presentadas como mera protección - seguridad "económica", "energética" o "territorial"- estas cifras enmascaran la consolidación de un complejo empresarial-estatal que convierte la seguridad en dispositivo ideológico al servicio de la acumulación.

des sociales) a Estados y otros actores, lucrándose con y desde el miedo social. La crítica ideológica nos previene para no tomar al pie de la letra los enunciados de seguridad con los que se nos inunda, y nos empuja a examinar "qué se hace en la práctica", esto es, a escrutar a quién benefician, a quién silencian y a qué costes para nuestras libertades y para la igualdad real de las personas.

b) *Crítica biopolítica*: Como ya sabemos, Foucault, en sus cursos *Seguridad, Territorio, Población* (1977-78) y *Nacimiento de la biopolítica* (1978-79), analizó cómo a partir del siglo XVIII el poder tiende no solo a disciplinar a los individuos (sociedad disciplinaria) sino a regular la vida de las poblaciones: tasas de natalidad, salud pública, flujos de circulación, etc. A esta forma de poder la denominó biopolítica. Desde esta perspectiva, la seguridad moderna es claramente un concepto biopolítico: en lugar de la ciudad fortificada (seguridad territorial clásica), Foucault nos recuerda que la seguridad funciona mediante dispositivos que permiten, previenen, calculan probabilidades y gestionan los riesgos en el entorno (por ejemplo, asegurando granos para prevenir hambrunas o estadísticas sanitarias para controlar epidemias). Las técnicas actuales de big data y los algoritmos predictivos son ahora la expresión más avanzada de esta racionalidad biopolítica, que busca un control preventivo y ubicuo de los acontecimientos antes de que estos ocurran.

Por otra parte, esta crítica biopolítica está ligada a la noción, también foucaultiana, de "gubernamentalidad": ese tipo de poder que actúa más por gestión técnica y/o "conducción de las conductas" que por imposición directa[4]. Y cada vez resulta más claro que en la era tecno-capitalista se va imponiendo poco a poco un régimen de "gubernamentalidad" algorítmica, donde las decisiones sobre lo que es peligroso o seguro, se toman dentro de sistemas automatizados (opacos) basados en datos poblacionales. Ahora son los algoritmos los que, por ejemplo, determinan quienes pueden o no pedir un crédito, quienes pueden ser asegurados o no con pólizas de seguro o quienes pueden considerarse peligrosos de cara a la vigilancia policial. Esta "seguridad algorítmica" es eminentemente biopolítica en la medida en que opera sobre poblaciones enteras (identifica patrones de grupos, no casos individuales) con el afán de optimizar la vida y prevenir disfunciones sistémicas. Empero, también introduce lo que Byung-Chul Han ha denominado como *psicopolítica*: el poder ya no reprime por la fuerza sino que seduce y manipula la psique, explotando la ilusión de libertad del sujeto digital para que éste coopere en su propia vigilancia (Chul Han: 2014). De ahí que también hablemos a lo largo de este trabajo de *hipnocracia* para referirnos a este nuevo régimen en el que la población, fascinada por las pantallas y las narrativas de seguridad, consiente pasivamente prácticas invasivas.

c) *Teoría de la "securitización"*: Con origen en la llamada Escuela de Copenhague (Barry Buzan, Ole Wæver, etc.), esta teoría explora cómo cualquier asunto puede

4. El concepto foucaultiano de gubernamentalidad, frente a la gobernabilidad - que evalúa la eficacia operativa de un régimen -, se detiene en la matriz de poder-saber que produce sujetos ajustados a lógicas liberales y neoliberales de acumulación, revelando así el trasfondo ideológico que normaliza políticas de seguridad, austeridad o militarización.

llegar a convertirse en una "cuestión de seguridad" mediante actos discursivos. "Securitizar" significa que un actor (generalmente una autoridad política) declara algo o señala a alguien como una amenaza existencial, lo que justifica medidas excepcionales para neutralizarla. Una vez securitizado un tema, se sustrae del debate público normal para ser tratado con urgencia y secretismo. Desde esta perspectiva podemos entender casos muy cercanos: ahí están, cómo los gobiernos securitizan la inmigración (presentándola como amenaza a la seguridad nacional o cultural, habilitando políticas de excepción en fronteras), o cómo se securitiza el activismo climático (tratándolo como extremismo peligroso que amerita la vigilancia especial). La teoría de la "securitización" nos sirve para mapear el proceso político a través del cual los nuevos espacios o dominios (Internet, big data, etc,) han sido subsumidos bajo el paraguas de la seguridad. *Ergo*, hay que preguntarse: ¿qué condiciones permiten que una innovación tecnológica (como la del reconocimiento facial) se legitime públicamente como una necesidad inaplazable de seguridad? ¿Quiénes aceptan ese discurso y por qué? ¿Qué efectos tiene en términos de poder y cuáles son sus excepciones legales?

d) *Capitalismo de vigilancia*: Shoshana Zuboff, en *The Age of Surveillance Capitalism* (2019), describe cómo las empresas tecnológicas explotan los datos de la experiencia humana como materia prima para predecir y modificar el comportamiento, creando un nuevo orden económico al que llama "capitalismo de la vigilancia". Este modelo busca la "certidumbre total" sobre la conducta de los usuarios, monetizando cada clic e interacción. Se nos podría decir que esto no es más que un problema de privacidad o de consumidores. Empero, para nosotros, alineándonos en este punto con Zuboff, constituye un profundo desafío político: quien controla los flujos de información y el conocimiento de nuestras preferencias, posee un poder inmenso para moldear la esfera pública y condicionar la democracia (Zuboff: 2019). Y por eso, también suscribimos, en este punto, la perspectiva de Frank Pasquale sobre la "sociedad de la caja negra": las decisiones automatizadas (desde aprobar un crédito hasta la posibilidad de dictar una sentencia penal en determinados delitos) se vuelven inescrutables, impidiendo la rendición de cuentas (Pasquale: 2015). También, asumimos aquí la perspectiva de Safiya Noble acerca de lo que denomina "algoritmos de opresión", pues pareciendo sistemas supuestamente neutrales reproducen de facto los sesgos racistas o sexistas de la sociedad (Noble: 2018). A lo largo de este trabajo, prestaremos atención a la relación vigilancia/discriminación: esto es, cómo las tecnologías de seguridad (por ejemplo, los sistemas de inteligencia artificial aplicados a vigilancia policial) pueden reforzar perfiles raciales, criminalizar a comunidades marginadas o silenciar voces disidentes en redes sociales. Por otra parte, tampoco podemos olvidar aquí lo que se conoce como el "chilling effect" o efecto disuasorio; es decir, en cómo la conciencia de sentirse/estar bajo vigilancia puede llegar a modular nuestra conducta, hasta el punto de autocensurarnos y/o abstenernos de participar políticamente por temor a efectos no deseados o represalias (V. Penney: 2016, pp. 117-182)[5].

5. En este estudio se demuestra cómo, tras las revelaciones de Snowden sobre la NSA, las visitas a artículos de Wikipedia sobre temas sensibles

Ahora bien, el enfoque crítico que aquí buscamos también nos exige una aclaración preliminar, porque, al cabo, ningún análisis está exento de valores; en nuestro caso, partimos de un compromiso normativo con los principios democráticos en su sentido más germinal y radical (léase derechos humanos, deliberación pública, pluralismo y control ciudadano del poder) y evaluamos la noción de seguridad desde cómo ésta los promueve o los socava. Esto no implica descartar la importancia de la seguridad *per se*; antes al contrario, lo que pretendemos es re-encuadrarla como un medio, no como un fin absoluto que todo lo justifica; es decir, como exigencia ética necesaria al servicio de las personas y de la democracia

4. Tecno-capitalismo y "securitización" algorítmica

Podemos decir, por tanto, que el tecno-capitalismo intensifica la función de la seguridad como fundamento ontológico de nuestra forma de ser gobernados. Las grandes corporaciones tecnológicas ya no se limitan a organizar y gestionar flujos enormes de datos; ahora también inciden de manera directa en cómo deben definirse las prioridades de los gobiernos y en cómo ha de entenderse la relación entre la seguridad pública y la privada. En nombre de la ciberseguridad y de la salvaguarda de los sistemas financieros, los Estados y las mega corporaciones asumen sobre nosotros potestades de vigilancia hasta ahora inéditas, y, lo que es peor aún, lo hacen sin apenas supervisión democrática. Se va configurando así un modelo muy peligroso en el que las normas tradicionales de control y de rendición de cuentas se ven desbordadas por la rapidez de la innovación tecnológica y por la conformación de estructuras de poder cada vez más opacas. Surge así, lo que podríamos denominar "securitización" algorítmica", esto es, el proceso por el cual la lógica de seguridad (anticipativa, controladora, etc) se integra en los sistemas algorítmicos automatizados que gestionan múltiples ámbitos de nuestra vida. En otras palabras, en el tecno-capitalismo, la seguridad deja de ser únicamente una función del Estado para convertirse en un *modus operandi* distribuido entre actores públicos y privados a través de tecnología. Tres serían sus elementos clave:

i) *La seguridad como motor de la innovación (tecnológica)*: Gran parte de las tecnologías digitales emergentes han sido impulsadas -al menos lo fueron en su origen- por objetivos de seguridad. Internet nació como un proyecto militar (ARPA-Net) orientado a garantizar comunicaciones resilientes en contextos de guerra; los sistemas de geoposicionamiento (GPS) también. Desde el 11-S, múltiples gobiernos invirtieron cantidades indecentes de dinero en tecnologías de vigilancia: cámaras CCTV, software de interceptación masiva de comunicaciones (como el programa PRISM de la NSA), bases de datos biométricos, drones de vigilancia, etc. Estas inversiones sembraron la semilla de la industria tecnológica actual. Uno de los ejemplos más clamorosos fue el caso de Clearview AI, la polémica empresa que recolectó miles de millones de fotos en redes sociales para entrenar un algoritmo de reconocimiento facial y que surgió precisamente para atender a departamentos de policía y agencias de seguridad bajo la

cayeron de forma significativa, evidenciando que la simple conciencia de vigilancia puede frenar la búsqueda de información y la participación cívica.

promesa de identificar a sospechosos casi instantáneamente. Aunque violaba claramente la privacidad de los ciudadanos (al crear una suerte de "panóptico digital" sin consentimiento), Clearview se amparó en la misma narrativa de seguridad de siempre: si contribuimos a la captura de criminales peligrosos, el mundo será un lugar mucho más seguro.

El resultado, como cabía esperar, fue el nacimiento de un nuevo mercado, muy lucrativo: el de la vigilancia. Vendió el acceso a su base de datos a entidades de nada menos que 24 países y fue utilizada asiduamente por cuerpos policiales en EEUU e, incluso, en Europa (antes de que sus autoridades de protección de datos intervinieran). En 2022 Italia y Francia le impusieron multas de 20 millones de euros y le prohibieron seguir recopilando imágenes de sus ciudadanos, reconociendo que su actividad vulneraba derechos fundamentales. Pero, esta tecnología ya se había desarrollado y otros actores -incluidos gobiernos no precisamente democráticos como Arabia Saudí o Catar - se interesaron por ella[6]. Este caso ilustra sobremanera cómo el incentivo de la seguridad acelera la innovación tecnológica, incluso a costa de sus límites éticos: se estrenan sistemas intrusivos sin evaluar plenamente sus impactos, y solo a posteriori se intenta regularlos, cuando ya es demasiado tarde.

ii) *La colaboración público-privada y la opacidad*: Como mencionamos al inicio de este trabajo, en los últimos años se ha ido configurado un suerte de consorcio "tecno-securitario" que implica tanto a empresas como a Estados. Las corporaciones privadas proveen infraestructura y know-how[7], y los Estados aportan legitimidad y aseguran la demanda. Un ejemplo paradigmático es, como ya hemos anticipado, el de *Pegasus*, el software espía de NSO Group capaz de infectar teléfonos móviles sin interacción del usuario. El uso extensivo (e intensivo, si se nos permite el calambur) de este software no solo se centró en terroristas y criminales, sino que también se empleó contra periodistas, opositores políticos y activistas de derechos humanos en decenas de países (incluidas no pocas democracias). Pegasus funciona como un software espía, donde NSO mantiene el control técnico mientras los gobiernos (clientes) ejecutan, en secreto, la vigilancia en nombre de la seguridad nacional. Huelga decir que este modelo plantea no pocos desafíos de cara a la asunción de responsabilidades:

6. Documentos filtrados por BuzzFeed en 2020-2021 mostraron que Clearview AI ofreció -o entregó en pruebas- su base biométrica a agencias de seguridad de al menos tres regímenes catalogados como autoritarios. (i) *Arabia Saudí*: el listado interno consignó búsquedas hechas desde unidades dependientes del Ministerio del Interior saudí; la filtración, reseñada por *The Register*, confirma que el acceso se concedió bajo la fórmula try-before-you-buy. (ii) *Emiratos Árabes Unidos*: la misma lista identifica a un fondo soberano emiratí e Interpol como "clientes activos", extremo ratificado por declaraciones de la propia empresa recogidas por *The Verge*, y (iii) *Qatar*: un dossier comercial citado por *Business Insider* incluye a la policía qatarí entre los destinatarios prioritarios de una "expansión rápida" hacia Estados del Golfo con historial de abusos de derechos humanos. En todos los casos la retórica de la seguridad abrió la puerta a una vigilancia biométrica sin debate público ni evaluación de impacto, cristalizando un mercado donde el riesgo se traslada a la ciudadanía mientras el beneficio queda en la industria de la vigilancia.

7. Este anglicismo se utiliza para referirse a ese conocimiento confidencial que confiere ventajas competitivas: procedimientos, algoritmos, manuales operativos, etc que la empresa guarda como secreto y licencia como activo inmaterial.

los gobiernos pueden negar los abusos al alegar que es la empresa quien opera sobre el sistema, y la empresa a su vez, puede escudarse, en que solo se los vende a Estados soberanos.

El poder, de esta forma, se privatiza. Empresas sin mandato democrático terminan gestionando datos íntimos de millones de personas y decidiendo - mediante sus algoritmos - qué información recibe cada uno o qué contenido se censura. Pensemos en Facebook (meta) o en Twitter (X) moderando discursos violentos (o dejándolos de moderar) según sus propias políticas internas; o en Google manipulando resultados de búsqueda que condicionan la visibilidad de ciertas ideas. Estas son funciones cuasi-gubernamentales que ahora son ejercidas por actores privados en nombre de sus intereses económicos o de su propio ideario empresarial.

iii) Y la *vigilancia algorítmica integral*: Como cabe imaginar este afán por la "securitización" algorítmica va implicando poco a poco cada vez a más aspectos de la vida social, que ahora son monitorizados, analizados y evaluados en tiempo real por sistemas de IA, en busca de "anomalías" o de riesgos. Esto ocurre tanto en el sector público como en el privado. En ciudades de China, por ejemplo, operan ya sistemas de crédito social que puntúan el comportamiento ciudadano (desde infracciones de seguridad vial hasta comentarios en redes) y según esa puntuación se otorgan beneficios o se imponen restricciones (menor acceso a préstamos, velocidad reducida de internet, etc.). Aunque con diferencias, los países occidentales tampoco son ajenos a este tipo de tendencias: ahí está la predicción policial en ciudades de EEUU y Europa, donde algoritmos analizan historiales delictivos y otros datos para predecir dónde o quién podría delinquir y orientar así el patrullaje (lo que ha sido criticado por reforzar sesgos raciales preexistentes); sistemas de "scoring" crediticio que combinan datos financieros tradicionales con información personal online; o el uso de IA en recursos humanos para filtrar candidatos "problemáticos" antes de la contratación. En todos estos casos, la promesa es la misma: seguridad y eficiencia mediante la prevención algorítmica -contratando solo empleados confiables, vigilando antes de que ocurra un delito, evitando fraudes antes de que se consuman, etc.

Empero, estas prácticas pueden llegar a reproducir discriminaciones sistémicas. Ahí están los algoritmos de predicción delictiva como PredPol (pionero en el "predictive policing" comercial)[8] que siempre

8. PredPol, rebautizado más tarde como Geolitica en 2021 y absorbido por ShotSpotter en 2023 surgió de una colaboración entre el Departamento de Policía de los Angeles (LAPD) y la Universidad de California. Se basaba en un modelo ideado para la identificación de réplicas sísmicas: básicamente partía de la idea de que cada delito tiene su "réplica" (aftershock), esto es, que desencadenaba otros en torno al mismo lugar y hora. En los primeros ensayos aleatorizados en los años 2012 y 2013 el algoritmo predijo entre 1,4 y 2,2 veces más delitos que los analistas humanos; y, con apenas 2 horas extra de patrulla, se redujeron los hurtos hasta en un 7,4 % de media. La empresa afirmó en 2019 tener unos 60 cuerpos policiales suscritos, lo que la convirtió en la referencia indiscutible del sector. Pero los hechos pronto desmontaron esta narrativa: la Inspección General del LAPD declaró en abril de 2019 que no existían datos sólidos sobre su pretendida eficacia y canceló el contrato en abril de 2020; Santa Cruz en California, fue aún más lejos y el 26-06-2020 se convirtió en la primera ciudad de EEUU en prohibir la predicción delictiva a golpe de ordenanza municipal. Las dudas sobre su fiabilidad se fueron ampliando cuando The Markup - un grupo de periodistas sin ánimo de lucro especializado

tienden a señalar a barrios pobres o minoritarios, sencillamente porque se alimentan de historiales policiales que ya vienen sesgados de origen. Los sistemas de reconocimiento facial comerciales fallan más con rostros negros que con los blancos, llevando a falsas identificaciones y arrestos de inocentes, como el caso de Robert Julian-Borchak Williams en 2020, un afroamericano en Detroit, que fue arrestado erróneamente porque un software de reconocimiento facial (DataWorks Plus) lo vinculó con una imagen borrosa de un delito de robo de relojes cometido en 2018[9].

5. Las consecuencias: Exclusión algorítmica, hiperpolarización informativa y desconexión cívica.

La idea de que nos encontramos ante nuevo régimen, *la Hipnocracia* es la tesis de un filósofo hongkonés (Jianwei Xunno) que no existe. Es el producto, según reveló la revista italiana L`Expresso, del ensayista Andrea Colamedici, que junto a dos plataformas de IA, publicó el ensayo titulado "Ipnocrazia. Trump, Musk e l'architettura della realtà" (Jianwei Xun: 2025)[10], en lo que explicó más tarde que se trataba de un "experimento filosófico y una *performance* artística".

Pero el hecho de que la firma de esta tesis sea apócrifa no le resta intensidad al concepto planteado. Representa, en cierta medida, lo que aquí decimos: la irrupción de lo que empieza a ser un nuevo régimen que ya no precisa - al menos no de manera predominante - de los métodos coercitivos clásicos (censura, represión física, prohibiciones explícitas), porque ya nos ha colonizado a todos. Puebla todo el imaginario y ya no necesita recurrir a la fuerza. Su manera de operar se sintetiza en la manipulación emocional y en la saturación informativa, con el propósito de inducir un especie de estado de "hipnosis" colectiva donde la verdad y la mentira se vuelven prácticamente indistinguibles. En un entramado como este, es donde la seguridad se erige en la coartada perfecta para justificar la recopilación masiva de datos, la vigilancia exponencial y la supresión de cualquier forma de disidencia que

en fiscalizar la tecnología - y la revista *Wired* copublicaron en octubre de 2023 una investigación titulada *Predictive Policing Software Terrible at Predicting Crimes*, en la que tras analizar 23631 predicciones de Geolitica se demostraba que solo el 0,5 % coincidía con un delito real denunciado, concentrándose los errores precisamente en barrios negros y latinos.

9. El 9 de enero de 2020 la Policía de Detroit detuvo a Robert Julian-Borchak Williams, afroamericano de 42 años, ante su esposa e hijas, porque un sistema de reconocimiento facial - DataWorks Plus, que tiene acceso a la base estatal SNAP -había vinculado su viejo carné de conducir con un fotograma borroso de un hurto de relojes Shinola ocurrido el 9 de octubre de 2018. El algoritmo propuso la "coincidencia", los agentes la tomaron por prueba y un vigilante externo señaló a Williams en una rueda fotográfica sesgada. Tras 30 horas de celda y un careo en que el detective advirtió a simple vista que el sospechoso y la imagen no coincidían, la fiscalía retiró los cargos el 2 de junio de 2020, convirtiendo el caso en la primera detención documentada en EE.UU. basada en un falso positivo de reconocimiento facial. Más tarde, Williams demandó a la ciudad; el litigio se saldó el 28 de junio de 2024 con una indemnización confidencial y la adopción de la directiva 307.5, que obliga a corroborar cualquier "match" algorítmico con pruebas independientes antes de solicitar una orden de arresto.

10. Existe además una versión inglesa autoeditada: *Hypnocracy: Trump, Musk and the Architecture of Reality*, en Amazon KDP, 20 feb. 2025.

amenace la "estabilidad" del orden tecnocapitalista.

El impacto sobre la democracia es evidente:

i) Por una parte, se generan ámbitos de "exclusión algorítmica"- utilizando de nuevo aquí la expresión de Noble (Noble: 2018) -, al marginalizar o censurar aquellas publicaciones o ideas que no encajan o no se subsumen en los patrones que van dictando los algoritmos. De todos es sabido que Twitter (ahora X), YouTube, Facebook (hoy Meta), Tik tok utilizan sistemas automatizados para promocionar o enterrar publicaciones, basándose en criterios que van desde la popularidad y las modas, hasta ideológicos o identitarios. Este fenómeno no solo afecta a actores individuales - que pueden ver censuradas sus opiniones - sino también a comunidades enteras que dejan de tener visibilidad en el debate público.

ii) Por otra, hay más polarización pública. Como usuarios de estas redes sociales habitamos en un suerte de entorno informativo a medida. La personalización algorítmica hace muy bien su trabajo, creando para nosotros "burbujas de información" a través de las cuales recibimos solo una visión parcial y sesgada de la realidad, pero afín a nuestros gustos o creencias. Dentro de estas burbujas reforzamos nuestras convicciones previas, evitándonos el contrate con puntos de vista diferentes. De esta forma, poco a poco se va potenciando en nosotros una suerte de sesgo de confirmación: se subraya lo que coincide con la opinión de cada uno y se relega a un segundo plano aquello que es disonante. El resultado parece obvio: se genera una falsa sensación de unanimidad en torno a determinados relatos o narrativas, lo que suscita no ya solo una polarización política cada vez más acusada (los grupos que divergen se suelen alejar mutuamente), sino, lo que es peor, la marginación de quienes no encajan o se sustraen a la opinión que construyen estos patrones algorítmicos.

iii) Pero, como quiera que estos algoritmos están optimizados para retener nuestra atención, descubren con facilidad que los discursos más extremos suscitan reacciones más intensas (ya fueren positivas o negativas). Ergo, se penaliza la información sosegada y la deliberación constructiva, que va reduciendo su visibilidad paulatinamente en la medida en que acarrean menos interacción viral. De esta forma, la lógica algorítmica premia la polémica y la emocionalidad en los extremos, propiciando artificialmente enfrentamientos en redes sociales y generando la sensación de que los matices ya no existen. Proliferan las "fake news" y la susceptibilidad frente a las mismas aumenta, alimentando así los mensajes de odio, pues dejamos de contrastar la información con criterios objetivos o fuentes diversas. Es la lógica polarizadora de la posverdad, la que ahora se abre paso y donde las emociones se anteponen casi siempre a los hechos.

iv) En un contexto como este de sobrecarga informativa y de polarización, los liderazgos populistas o demagógicos lo tienen más fácil; solo tienen que presentar soluciones claras y contundentes, aunque parezcan inverosímiles, frente al caos; y la ciudadanía, saturada y cansada, se plegará sin titubear al vigor de sus promesas de certeza o de seguridad: "American first" (América primero), "Make America Great Again" (Hacer a América Grande de Nuevo) o "He golden age of America begins right now" (ha llegado la edad dorada de

América) utilizados por Donald Trump; el "Take Back Control" (recuperar el Control) empleada por los defensores del Brexit en el Reino Unido, para sugerir que el país debía retomar su soberanía y autonomía perdidas, especialmente en asuntos legislativos y de inmigración; "¡Viva la libertad, carajo!" utilizado por Javier Milei, reflejando su postura libertaria y su rechazo a la "casta política", son algunos ejemplos de cuanto aquí decimos. Es precisamente aquí donde la *hipnocracia* encuentra su verdadero caladero: en la fragmentación y en la vulnerabilidad de un *demos* inerme frente a esta nueva fenomenología de manipulación colectiva.

v) Por otra parte, la consciencia de estar siendo siempre supervisados (o la sospecha de que esto ocurre) genera en nosotros esa suerte de efecto disuasorio, que anunciábamos al principio. Nos autocensuramos y tememos participar políticamente si nuestras opiniones son disidentes. Esto tiene efectos sobre nuestra subjetividad. El "efecto panóptico", que ya anticipara Foucault para su sociedad disciplinaria (Foucault, 1975)[11], es decir, la posibilidad de desplegar actitudes de autocensura al sentirnos observados, se multiplica en la era digital. Ya no nos vigila solo el Estado. Ahora también lo hacen los gobiernos, las agencias de publicidad, las tecnológicas, etc. Cualquiera con un smartphone puede registrar y difundir nuestras acciones. Esta nueva normalización de la vigilancia ubicua naturaliza la idea de que nuestros datos personales son un recurso accesible y comercializable, borrando definitivamente la frontera entre el ámbito privado y el público. El resultado es una ciudadanía menos propensa a organizarse y a confrontar el orden dominante, por temor a consecuencias de toda laya: laborales, financieras o incluso penales derivadas de su actividad política.

Son los tiempos de la *psicopolítica* digital; se adentra sin ruido - para luego explotar - en todos los rincones de nuestra mente; se sirve de nuestras ideas y percepciones, de nuestras emociones, del miedo, de la indignación, de nuestra constante necesidad de validación, etc., para mantenernos conectados a las redes en una suerte de enganche adictivo, de pulsión que nunca termina del todo, que debilita nuestra autonomía crítica como ciudadanos.

El efecto más significativo no va a salir en estas páginas, sino en futuros trabajos: la posverdad. Es decir, cuando los hechos objetivos ya no son determinantes en la opinión pública y ceden la voz a las emociones y a las creencias personales. Amplificado por algoritmos de recomendación que priorizan el contenido más emocionante o polémico, este fenómeno ha derivado en la difusión masiva y fulminante de noticias falsas, contenido pernicioso y teorías conspirativas, que minan el debate racional. La información veraz pierde terreno frente a las narrativas simplistas pero emocionalmente eficaces, lo que dificulta la construcción de consensos informados. Si a esto le sumamos la polarización informativa y afectiva - el rechazo visceral del otro - de la que ya hemos hablado, tenemos el coctel perfecto para una ciudadanía fragmentada y dividida donde el diálogo trasversal es poco menos que imposible, incluso entre quienes a priori

11. Esta obra presenta la base teórica del "panoptismo" inspirado en el diseño de Jeremy Bentham, y expone cómo la posibilidad de vigilancia constante moldea la subjetividad y refuerza la disciplina. Es interesante para un análisis de la era digital que profundiza en la recolección masiva de datos y la manipulación de la conducta mediante algoritmos.

están más preparados (más formados e informados). Ni tan siquiera estos permanecen inmunes, pues también reciben y exhiben, contrariamente a lo que cabría pensar, sesgos de confirmación en línea. No solo los más desinformados caen en la polarización irracional. Todos lo hacemos.

Esto, claro está, beneficia a determinados actores. No hay que esforzarse demasiado para comprobar como proliferan los discursos extremistas o demagógicos entre tanto caos informativo. Piénsese por ejemplo en los movimientos anti-vacunas o en los negacionistas climáticos que crecieron precisamente durante la pandemia alimentados por rumores en redes. Pero esa confusión extiende la desafección política: muchos ciudadanos, bombardeados por escándalos y negatividad, se hartan y optan por irse literalmente a una playa o al campo y retirarse de la participación. En nuestro país, sin ir más lejos, los últimos estudios del CIS evidencian cómo la desafección aumenta. Nada menos que la mitad de los españoles mencionan a "los políticos" como el principal problema del país, por encima incluso de preocupaciones galopantes como la de la vivienda.

Pero esto que decimos no es un simple contratiempo orgánico dentro de nuestras democracias; tiene efectos muy visibles sobre nuestros derechos y libertades. Para comprobarlo, examinaremos tres casos recientes en Europa y en Estados Unidos, que revelan cómo opera esta lógica de la "securitización" algorítmica y cuáles son sus efectos.

6. Caso UE: Reglamento de Inteligencia Artificial 2024 – seguridad, libertades y lobby tecnológico

La UE se ha posicionado a la vanguardia en la regulación del uso de las nuevas tecnologías con implicaciones éticas. El ejemplo más representativo es el Reglamento de Inteligencia Artificial (RIA) -conocido coloquialmente como la *Ley de IA de la UE* (EU AI Act)- cuyo texto definitivo se adoptó en 2024. Se trata de la primera regulación integral sobre sistemas de inteligencia artificial a nivel global, con un enfoque basado en riesgos: prohíbe algunos usos de IA considerados inaceptables, impone obligaciones estrictas a usos de "alto riesgo" y exige normas de transparencia para aplicaciones generales. A primera vista, el RIA representa el afán por conciliar la seguridad de los sistemas de IA con los derechos fundamentales. En su art. 1, establece precisamente que su objetivo "es mejorar el funcionamiento del mercado interior y promover la adopción de la inteligencia artificial (IA) centrada en el ser humano y digna de confianza, garantizando al mismo tiempo un alto nivel de protección de la salud, la seguridad, los derechos fundamentales consagrados en la Carta, incluida la democracia, el Estado de Derecho y la protección del medio ambiente….". Entre las prácticas prohibidas explícitamente figuran la vigilancia biométrica masiva en tiempo real en espacios públicos, la puntuación social estilo chino y ciertas formas de manipulación subliminal mediante IA. Sin embargo, una lectura detallada y un análisis del proceso de aprobación revelan una trama mucho más compleja, donde aparecen excepciones y/o presiones que ponen en entredicho la

eficacia de la norma en materia de seguridad y libertades.

En primer lugar, el Reglamento incluye múltiples excepciones y lagunas en nombre de la seguridad y el orden público. Aunque en principio se prohíbe el uso de sistemas de identificación biométrica remota en tiempo real (como cámaras con reconocimiento facial en la calle), se abren *excepciones* para que las fuerzas de seguridad los puedan emplear si buscan a víctimas de delitos o a sospechosos de crímenes graves o, en su caso, para prevenir amenazas terroristas. En la práctica, esto puede vaciar la prohibición: basta con alegar que se trata de una investigación criminal importante para que se pudiera desplegar esta tecnología sin cortapisas. De hecho, organizaciones de derechos digitales han criticado que la ley dibuja una prohibición "con forma de queso gruyere", llena de agujeros por los que colar usos policiales de IA sin apenas supervisión[12]. Es más, se excluyó de su ámbito de aplicación a la mayoría de sistemas de IA usados en actividades militares o de seguridad nacional, por la presión ejercida por muchos Estados miembros. Durante las negociaciones, se introdujo la llamada *"exención de seguridad"*, en virtud de la cual los sistemas de IA desarrollados o utilizados exclusivamente para fines de defensa, seguridad y aplicación de la ley no estarían sujetos a las mismas obligaciones hasta como mínimo el 2031. Esto significa que, por ejemplo, un algoritmo de vigilancia masiva operado por Europol o por los servicios de inteligencia de un país europeo queda fuera de la regulación de IA; o lo que es lo mismo, se fía a estos actores la capacidad para, nada menos, que autorregularse.

Uno de los informes más recientes de Statewatch (2025) ha documentado cómo, en la intrahistoria de los procesos de negociación del Reglamento, un órgano poco conocido llamado European Clearing Board -compuesto por funcionarios de policía de los Estados miembros- presionó para incorporar excepciones de "seguridad"[13]. El resultado final, claro está, fue un texto que enuncia grandes principios pero que, en la práctica, mantiene la puerta abierta a la "securitización" algorítmica por parte del Estado. Así, por ejemplo, aunque se prohíbe la categorización biométrica de personas (clasificarlas por raza, género, orientación sexual a partir de IA), el texto de la norma permite que las "autoridades competentes" puedan utilizarlas bajo la justificación de que es necesaria para la

12. Fue el caso de Amnistía Internacional, cuando a través de Damini Satija (jefa del Algorithmic Accountability Lab), advirtió que las excepciones para fuerzas de seguridad "hacen que la prohibición del reconocimiento facial en espacios públicos parezca un queso gruyere", al reaccionar cuando se consumó el acuerdo político sobre IA Act (Gizmodo, 15 dic 2023).

13. Statewatch detalla en *Automating Authority: Artificial Intelligence in European Police and Border Regimes,* publicado el 29 de abril de este mismo año 2025 que el European Clearing Board (EuCB) - creado en 2020 por los jefes de las unidades nacionales de Europol - actuó como grupo de presión para recortar salvaguardias en la Ley de IA. El capítulo 4.1.3 del informe explica que: i) la Strategic Group on AI del EuCB, copresidida por Francia y Países Bajos, "lobbyeó con éxito" al Consejo para introducir excepciones policiales en la definición de sistemas, la clasificación de riesgos y la publicidad obligatoria de algoritmos; ii) se celebraron al menos 19 reuniones dedicadas a la norma entre 2021 y 2024 y iii) esas gestiones "provocaron cambios importantes" a favor de la vigilancia biométrica y el secreto operativo. El informe completo y los documentos filtrados (términos de referencia del EuCB y actas de sus reuniones) pueden consultarse en la página de publicaciones de Statewatch.

aplicación de la ley. También, se regula la transparencia de los sistemas de IA (que se informe al usuario cuando interactúa con un chatbot o deepfake, etc), pero se exceptúa en los contextos de migración y fronteras. Así las cosas, proyectos impulsados por la UE como el *iBorderCtrl* -un controvertido sistema que usaba IA para detectar mentiras en entrevistas a viajeros y migrantes analizando micro-expresiones faciales[14]- podrían continuar sin la estricta supervisión del RIA, pues se enmarcan dentro del control fronterizo y, por tanto, "no afectan a sujetos dentro de la UE".

Otra tensión notable fue la del lobby empresarial. Es cierto que la UE se enorgullece de su rol regulatorio orientado en y por valores, pero también lo es que quiere fomentar la innovación en IA (como también reza su art. 1º) para no quedarse atrás frente a EEUU y China. Durante el proceso de elaboración, gigantes tecnológicos y asociaciones empresariales intervinieron activamente para suavizar ciertas disposiciones. Se redujo, por ejemplo, la carga de transparencia en sistemas de IA genéricos (como modelos de lenguaje tipo GPT) bajo el argumento de que podrían lastrar el desarrollo industrial. También se flexibilizaron criterios para determinar qué puede considerarse o no como un sistema de "alto riesgo", lo que condujo de facto a exceptuar algunas aplicaciones comerciales polémicas (como los algoritmos de moderación de contenido en redes sociales o de publicidad microdirigida). La presión corporativa logró, por tanto, suavizar el alcance de buena parte de sus disposiciones, tratando de preservar los intereses de los grandes proveedores de IA, especialmente en lo que hace a la vigilancia y el manejo de datos. Fue el caso, por ejemplo, de las entidades bancarias o de las empresas de marketing directo, que no dudaron en presionar para que las IAs de análisis de comportamiento de clientes no se considerasen de alto riesgo, evitando así auditorías obligatorias.

Ahora bien, no todo fueron problemas. Cabe una lectura muy positiva del texto final, pues sí contrae obligaciones hasta ahora inéditas que sirven para mejorar la seguridad entendida como protección de derechos. Por ejemplo, los sistemas de IA de alto riesgo (los utilizados en el control de infraestructuras críticas, evaluación de solvencia crediticia, selección de personal para empleos públicos, etc.) deberán ser evaluados antes de lanzarse al mercado, disponer de documentación técnica que asegure su trazabilidad, incorporar mecanismos de gestión de datos para minimizar sesgos, y someterse a revisiones periódicas. Asimismo, la UE planea crear un Consejo Europeo de IA para supervisar su implementación. Ni que decir tiene que no se trata de medidas anecdóticas. Bien implementadas, aportan transparencia y responsabilidad en los usos de IA que atañen a la segu-

14. Se trata de un proyecto que se enmarca en la estrategia H2020 (*Intelligent Portable Border Control System*, 2016-2019) financiado por la UE con 4,5 M € para probar un mini control fronterizo portátil basado en un avatar de IA que analiza "microexpresiones" faciales y declara si el viajero miente. El consorcio - coordinado por European Dynamics y coordinado por Hungría, Grecia y Letonia- pretendía acelerar el paso de terceros ciudadanos con un registro previo online y un kit biométrico en la frontera. Un reportaje de *The Guardian* reveló en 2020 que el sistema, criticado por sus sesgos y su falta de validez científica, había sido demandado ante el TJUE por opacidad y riesgo de discriminación. Puede consultarse en: https://cordis.europa.eu/project/id/700626 y https://www.theguardian.com/world/2020/dec/10/sci-fi-surveillance-europes-secretive-push-into-biometric-technology

ridad de las personas. Un algoritmo que decida acerca del acceso o no a prestaciones sociales no podrá ser una "caja negra" incuestionable, sino que deberá explicarse y auditarse. El desafío reside, por tanto, en garantizar que estas estructuras reguladoras funcionen de verdad.

Lo que sí está claro es que este Reglamento ejemplifica la ambivalencia de la que aquí hablamos. Por una parte, se enuncian principios progresistas y se prohíben distopías evidentes (como un Gran Hermano orweliano), pero, por otra, se ceden excepciones a los poderes establecidos. Se busca "garantizar la seguridad jurídica" para los innovadores y, a la vez, " para los ciudadanos"; pero, lo cierto es que, en la balanza final, la preocupación "securitaria" estatal sigue ocupando un lugar decisivo, con la consiguiente limitación del alcance transformador de la norma.

Queda abierta la pregunta de hasta qué punto el AI Act logrará en la práctica frenar los usos más lesivos de la Inteligencia Artificial. ¿Realmente evitará que en Europa se masifique el reconocimiento facial policial? ¿o que se usen IAs sesgadas en decisiones automatizadas?). Lo que sí es seguro es que, al menos, se establece un precedente importante y una base legal para exigir futuras responsabilidades. Por primera vez, la "seguridad algorítmica" tiene un marco explícito de derechos en la legislación de una potencia global. Veremos qué pasa.

7. Caso EE. UU.: Reautorización de la FISA 702 (2024) – vigilancia masiva vs. privacidad

Si nos vamos al otro lado del Atlántico, en Estados Unidos, este debate entre seguridad y libertades, también ha librado hace muy poco un enfrentamiento crucial en lo que hace al desarrollo de las leyes de vigilancia electrónica. Una de las herramientas más controvertidas en este punto ha sido la llamada Sección 702 de la Ley de Vigilancia de Inteligencia Extranjera (FISA, por sus siglas en inglés), que autoriza la recolección masiva de comunicaciones sin orden judicial cuando los objetivos son extranjeros fuera del país -aunque en la práctica también ha capturado cantidades significativas de datos de ciudadanos estadounidenses (aunque *incidentalmente*, según la propia terminología oficial). La Sección 702, introducida en 2008 tras revelarse los programas secretos de la NSA bajo el gobierno de Bush, se ha convertido en uno de los pilares sobre los que se apuntalan los servicios de inteligencia estadounidense, permitiendo programas como PRISM (acceso directo a servidores de grandes tecnológicas para extraer correos, chats, archivos en la nube, etc. de usuarios extranjeros) y Upstream (interceptación de tránsito de internet a gran escala). No obstante, debido a su propia configuración normativa, la sección 702 está sujeta a término y debe ser reautorizada por el Congreso. La última vez en que se procedió a su renovación, a finales del 2023 se produjo un debate muy clarificador en lo que aquí interesa, pues vino a elucidar las no pocas tensiones entre la comunidad de inteligencia, que abogaba

por la renovación argumentando la necesidad de disponer de una herramienta como esa para prevenir amenazas, y los defensores de derechos civiles y algunos congresistas que exigían reformas profundas para frenar los abusos y proteger la privacidad.

La administración Biden y altos mandos de inteligencia advirtieron que su no renovación significaría "quedar a ciegas" ante tramas terroristas, ciberataques extranjeros y espionaje. No en vano había contribuido a detener complots y proveía ya, según sus propias fuentes, prácticamente el 25% de la inteligencia contenida en informes de seguridad nacional. Pero del otro lado se presentaron evidencias de malos usos: informes desclasificados mostraron que el FBI -que tiene acceso a las bases de datos recolectadas bajo la sección 702- realizó consultas indebidas miles de veces, buscando información sobre personas estadounidenses sin las debidas justificaciones (incluyendo activistas, funcionarios locales e incluso a un congresista). También salieron a la luz casos en los que los propios analistas abusaron del sistema para espiar a parejas sentimentales o a rivales. Estos incidentes dieron munición a quienes pedían reformas. Organizaciones como la ACLU y el Center for Democracy & Technology reclamaban que cualquier reautorización debía incluir, al menos, el requisito de la orden judicial para que las agencias pudieran revisar comunicaciones de estadounidenses en los datos recolectados a través de puertas traseras.

Este debate aunó, en una curiosa coalición, tanto a libertarios republicanos como a demócratas progresistas. A finales de 2023, la Cámara de Representantes -entonces bajo control demócrata- se mostró reticente a una renovación sin más. El Departamento de Justicia y la Oficina del Director de Inteligencia Nacional hicieron ciertas concesiones, como endurecer las políticas internas en el FBI. Pero, pese a que muchos congresistas consideraron insuficiente la mera autorregulación de los servicios de inteligencia, pudo la presión de no dejar "caer" la herramienta en un contexto cada vez más complejo de tensiones geopolíticas (guerra en Ucrania, preocupación por China e Irán). Al final, en diciembre de 2023, prácticamente tocando la campana, el Congreso aprobó una ley de compromiso: la Reforming Intelligence and Securing America Act (RISAA), que reautorizó la 702, pero esta vez solo por dos años (hasta finales de 2025) en lugar de los cinco usuales, e incorporó varias reformas parciales orientadas a aumentar la supervisión. Esta corta extensión -la más breve desde que existe 702- fue interpretada como una victoria para los reformistas, ya que fuerza a reabrir el debate en el 2026 con un nuevo Congreso y bajo diferentes mayorías. En esencia, lo que se hizo fue posponer la pelea de fondo pero con algunas mejoras interinas.

Entre las reformas incluidas en podemos destacar: i) la exigencia de una orden judicial antes de revisar el contenido de comunicaciones, vía sección 702, cuando se busque información sobre un funcionario público electo (para evitar el espionaje político interno); ii) la imposición de más requisitos para que el FBI consulte la base de datos de ciudadanos estadounidenses; iii) más auditorías internas y formación anual obligatorias sobre su debido uso y iv), por supuesto, sanciones más claras para los abusos. Se prohibieron explícitamente las búsquedas relacionadas con delitos comunes (salvo en casos excepcionales de amenaza inminente) y se

ordenó la generación de un registro detallado de todas y cada una de las consultas que utilizasen datos de estadounidenses, con el fin de facilitar la supervisión del Congreso.

El compromiso temporal de 2 años aplazó el debate de fondo y ambos bandos cedieron. Los defensores de la seguridad no lograron una renovación larga sin cambios y los reformistas no consiguieron insertar todo lo que querían (como una orden judicial generalizada para cualquier consulta sobre estadounidenses). Es importante insistir aquí que esta reautorización salió adelante prácticamente apurando el límite y con votaciones muy ajustadas, lo que viene a elucidar la enorme polarización que suscita este debate. Fue la reautorización más difícil de la sección 702 desde su entrada en vigor. La administración tuvo que aceptar la posibilidad de reducir su vigencia para atraer suficientes votos, en particular la de un grupo de republicanos alineados con el entonces expresidente Trump, que ya por entonces instaba a "eliminar FISA", entre otras cosas por sus propias batallas con el FBI. Así, los sectores pro-privacidad encontraron aliados circunstanciales en los trumpistas anti-élite, un maridaje inusual[15] de motivaciones distintas que convergieron para restringir la discrecionalidad de los poderes de inteligencia. Ahora con Trump de nuevo en la Casa Blanca, está por ver.

¿Qué nos dice este caso sobre la relación entre seguridad hipnótica y democracia? En primer lugar, que la inercia "securitaria", como en el caso de la IA Act sigue siendo muy fuerte: pese a años de denuncias (desde Snowden 2013 hasta los informes recientes), la infraestructura de vigilancia masiva sobrevive con relativamente pocos cambios. La narrativa del miedo ("nos dejará vulnerables a otro 11-S") sigue siendo eficaz. Pero, también es cierto que cada vez detectamos señales de desencanto democrático frente a ese discurso hipnótico: la ciudadanía y muchos de sus representantes ya no compran sin más el *"confía, es por tu seguridad"*. En lo que aquí interesa, la saga de FISA 702 describe a la hipnocracia en acción, pero también nos muestra que hay contrapesos. Durante años, la opinión pública ha permanecido en una suerte de letargo acerca del alcance de la vigilancia estatal (se repetía: "solo espía a extranjeros, no nos afecta, porque somos ciudadanos honrados"). Los propios *big tech* (Google, Microsoft, etc.), implicados en PRISM[16], guardaron silencio o lo negaron. Ese secretismo se rompió con Snowden;

15. A diferencia de la UE, donde hay un mayor consenso multipartidista sobre privacidad (por razones históricas de regímenes autoritarios en Europa), en EEUU la cuestión se entrelaza con divisiones partidistas y coyunturales. Es interesante cómo la retórica pro-seguridad viene tanto de republicanos tradicionales como de demócratas centristas, mientras la defensa de libertades viene de polos opuestos del espectro (libertarios republicanos tipo Rand Paul y demócratas de izquierda tipo Ron Wyden). Esto crea alianzas inestables. En 2024 de hecho se veía como la gran incógnita si la proximidad de elecciones generales (noviembre 2024) haría de 702 un rehén político. Al final se optó por fiarlo todo a 2025.

16. PRISM fue el programa secreto de la NSA, activo desde 2007 y amparado en la sección 702 de la FISA, que permitía interceptar en tiempo real correos, chats y archivos directamente en los servidores de Microsoft, Google, Facebook, Apple y otras grandes plataformas. Su existencia se conoció gracias a las diapositivas filtradas por Edward Snowden en junio de 2013; un dictamen del tribunal FISC de 2011 calculo que PRISM generaba el 91 % de todos los datos recogidos con esa base legal. Documentos internos revelaron, además, que Microsoft colaboro para que la NSA sorteara el cifrado de Outlook y Skype.

fue el *momento anagnórisis* en que la ciudadanía vio tras el telón. Desde entonces, la desconfianza hacia la vigilancia estatal ha ido aumentando. Cada vez más jóvenes cifran sus mensajes o usan VPNs). Podemos decir, por tanto, que la *hipnosis securitaria* se ha ido debilitando, aunque no lo suficiente.

En fin, la reautorización de FISA 702 (2024) refleja la pugna, aún no resuelta entre un modelo "securitario" heredado del 11S y el impulso reformista que busca realinear la vigilancia con los valores democráticos (privacidad, debido proceso, etc). Merced a la misma, a sus revelaciones y a la presión pública, se anticipó siquiera un atisbo de reforma. También no enseña cómo la democracia -aun con sus defectos- tiene mecanismos para revisar sus propias excepciones: a base de debatir y negociar, se pudieron incorporar controles y sobre todo limitar temporalmente el poder, algo impensable en regímenes autoritarios donde una vez otorgadas, las prerrogativas de seguridad suelen perpetuarse. Que a finales de 2025 se vuelva a deliberar sobre el futuro y/o las condiciones de la sección 702 será otra prueba de la capacidad del sistema democrático para *aprender* de sus excesos y corregir los caminos. Ahora con Trump en la Casa Blanca, quién sabe.

8. Caso Twitter/X: el cambio algorítmico de julio 2024 – libertad de expresión y sesgo de plataforma

La red social Twitter -rebautizada como X en 2023 tras su compra por Elon Musk- ofrece un ejemplo revelador de cómo el poder sobre los algoritmos de visibilidad puede afectar a la esfera pública y, potencialmente, a la salud de nuestras democracias. Twitter, con cientos de millones de usuarios, llegó a convertirse en una suerte de *ágora digital* donde periodistas, políticos, activistas y ciudadanos comunes discutían en tiempo real. La prominencia o la invisibilidad de un mensaje en el feed de cada usuario dependía de algoritmos opacos que escalaban los tuits en función de múltiples factores (reciprocidad, intereses del usuario, popularidad del tuit, etc.). Históricamente, Twitter era más cronológico, pero desde 2016-2017 integró algoritmos de recomendación en la línea de tiempo. Con la llegada de Musk en octubre de 2022, se generó una gran incertidumbre sobre cómo podrían cambiar esas reglas, dadas sus declaraciones en pro de la "libre expresión absoluta" y su conocida afinidad con ciertos sectores ideológicos.

En julio de 2024, según investigaciones independientes, se produjo un cambio sustancial en el algoritmo de X que levantó polémica. Un estudio conducido por investigadores de la Universidad de Monash y de la Universidad Tecnológica de Queensland (Timothy Graham y Mark Andrejevic)[17] desveló que, a partir del 13 de julio de 2024, las publicaciones de Elon Musk y las de una serie de cuentas de tendencia conservadora experimentaron un salto drástico en términos de visibilidad, muy por encima del

17. El informe se llama *A computational analysis of potential algorithmic bias on platform X during the 2024 US election* (versión 4, octubre 2024). Analiza 56 184 tuits de diez cuentas políticas muy visibles - cinco republicanas, cinco demócratas - y del propio Elon Musk entre el 1 de enero y el 25-de octubre de 2024. El informe completo puede consultarse en el repositorio público de GitHub *AlgorithmicBiasX* y en una copia espejo alojada en Document Cloud.

crecimiento orgánico general de la plataforma. En concreto, los tuits de Musk comenzaron a obtener un 138% más de visualizaciones y 238% más retuits que el promedio antes de esa fecha. Otras cuentas identificadas como afines a posturas republicanas o de derecha también mostraron aumentos anómalos, aunque más modestos. Esto coincidió temporalmente con el anuncio de Musk de apoyar la candidatura presidencial de Donald Trump para 2024. Ese estudio concluía que era muy probable que X hubiera hecho un ajuste a nivel de plataforma para potenciar el alcance de Musk y de perfiles ideológicamente alineados con él. Aunque se desconoce la "instrucción" exacta añadida al algoritmo, lo cierto es que la evidencia estadística -comparando tendencias antes y después- sugiere una intervención deliberada.

Estas revelaciones, difundidas primero en foros técnicos y luego recogidas por medios como *The Washington Post*, despertaron inquietud sobre la neutralidad de la plataforma de cara a las elecciones. Twitter/X, a diferencia de Facebook, había tenido siempre un rol más "horizontal" en el debate público, con tendencias virales que a veces nacían de minorías (hashtags activistas, denuncias ciudadanas, etc). Si ahora su algoritmo priorizaba cierto sesgo ideológico, podría contraer una distorsión del espacio deliberativo. Es cierto que, bajo Musk, la empresa ya había tomado decisiones polémicas: restauró cuentas de extrema derecha previamente suspendidas, desmanteló gran parte del equipo de moderación de contenidos y cambió el sistema de verificación (ahora de pago, con la marca azul disponible para suscriptores, diluyendo la confianza en fuentes oficiales). Musk argumentaba que buscaba nivelar el campo y acabar con lo que consideraba un sesgo "liberal/progresista" previo en la moderación.

Estos hechos evidencian que Musk -como dueño único- utilizó su potestad de modelar el algoritmo en favor de su propia relevancia y agenda, como lo demuestra el hecho de que amplificara las narrativas republicanas en las elecciones estadounidenses de 2024. Un análisis del *Wall Street Journal* y el *Washington Post* demostraron que X estaba recomendando con más frecuencia contenidos de derecha radical que sus competidores, y que ciertos hashtags pro-Trump dominaban tendencias globales de forma sospechosa. Unos hechos que él mismo no solo no ha desmentido, sino que ha ratificado, después de su ruptura con Donald Trump, al llegar a decir "que sin él, Trump no habría ganado". Este es un claro ejemplo de privatización de la gobernanza informativa en su máxima expresión: decisiones que afectan el debate público global quedan a discreción de un sujeto con poder tecnocrático que no rinde cuentas ni se somete a ningún proceso democrático; es un ejemplo de cómo la opacidad y la arbitrariedad algorítmica pueden llegar a socavar la equidad del espacio público. Es como si, utilizando un símil en el mundo *offline*, el dueño de la mayor empresa de medios imprimiera millones de panfletos de su candidato y limitara la impresión a sus oponentes, y que lo hiciera además de manera automatizada e invisible para el público general.

Lo curioso aquí es que esta pretendida "alteración" fue descubierta precisamente merced al análisis de datos y a la vigilancia académica, y ello pese a las precauciones que en este sentido adoptara el propio Musk al limitar, a mediados de 2023, las API (*Application Programming*

Interface), o lo que es lo mismo, las puertas de enlace que una plataforma abre para que programas externos - scripts de investigación, bots, etc. - puedan leer, filtrar o publicar contenidos sin pasar por la interfaz web. Pero, aun así, pese a las dificultades para escrutar a la plataforma, ambos investigadores lograron obtener muestras y detectar la anomalía. Esta actitud resalta la importancia de la transparencia algorítmica: si X tuviera que publicar, por ejemplo, un informe de impacto de sus cambios de algoritmo (como algunos proponen regular), se podría debatir abiertamente si es aceptable o no potenciar ciertas voces. En lugar de eso, la plataforma no ofreció ninguna explicación sobre cómo y por qué lo hizo. Fue solo, tras la publicación del meritado estudio, cuando un portavoz de X (por supuesto bajo anonimato) desestimó los hallazgos esgrimiendo que "correlación no implica causalidad" y que siempre se sucedían cambios en la plataforma. Pero no refutó en concreto la acusación principal.

Este caso nos sirve para explicar la idea de exclusión algorítmica de la que ya hemos hablado. Al favorecer un tipo de contenido (en este caso posiciones de derecha pro-Musk) lo que ocurre simultáneamente, es el hundimiento de la visibilidad de los contenidos que le son opuestos. Usuarios de ideología progresista denunciaron, con razón, una drástica caída en el alcance de sus tuits durante el 2024; periodistas que cubrían negativamente a Musk se quejaban de que sus posts tenían menos interacciones que antes, algo difícil de probar anecdóticamente, pero que se compadece perfectamente con la tendencia descrita por ambos investigadores.

El sentimiento de indefensión informativa era evidente. De la noche a la mañana, muchos usuarios no sabían por qué su voz y sus mensajes, de repente, perdían visibilidad. El impacto en la pluralidad del debate empezaba a notarse: si X se convierte en un amplificador de ideas conservadoras, el valor que tenía como punto de encuentro multi-diverso (donde convergían ONG, disidentes de países autoritarios, expertos y gente común), sencillamente se difumina. Desde entonces, para no pocos colectivos (feministas, LGTB, antirracistas, etc), X pasó a ser una plataforma hostil; pero no ya solo por su menor visibilidad, sino por los abusos y acoso a los que se exponían tras la eliminación de las políticas de moderación. Ahora sólo les quedaba o callar o marcharse a otras plataformas. Se cumplía así una de las la profecías de la hipnocracia: cuando la gente crítica abandona la plaza, el *ágora,* la ilusión de consenso del resto se refuerza.

Podemos decir, por tanto, que la experiencia de X post-Musk pone de manifiesto la fragilidad de los comunes digitales: un espacio que funcionaba (más o menos) como bien público informativo cae bajo el control personalista de un magnate y pierde su neutralidad. Este "experimento" es un argumento claro a favor de las propuestas que de manera tentativa plantearemos en el último apartado de este trabajo, como la creación de plataformas públicas o la sujeción de algoritmos a auditorías independientes. En el fondo, la pregunta que nos debemos hacer es la siguiente: ¿debemos hoy, como ciudadanos en 2025, permanecer a merced de los caprichos de un magnate digital para expresar nuestras ideas y acceder a información? Si la respuesta es que no; la consecuencia está clara, la ciudadanía debe crear contrapesos. El caso Twitter/X nos sirve para concienciar a muchos sobre la necesidad de

diversificar las redes (no depender de una sola), fomentar modelos abiertos (ahí esta el protocolo ActivityPub de redes federadas[18]) y exigir responsabilidad algorítmica. Tenemos que despertar; las grandes plataformas no son "árbitros neutrales".

El cambio algorítmico de X en 2024, presuntamente orientado a favorecer ciertas voces políticas, constituye una alarma que no podemos ignorar sobre cómo el poder privado tecnológico puede comprometer la calidad de la democracia. Por eso lo traemos a colación aquí; porque nos sirve de recordatorio. Un recordatorio de que la seguridad de una democracia no consiste solo en impedir golpes militares o en evitar leyes represivas; sino también en garantizar un ecosistema informativo plural y justo. Cuando ese ecosistema se desequilibra por decisiones unilaterales, la democracia en su dimensión deliberativa se resiente. La "hiperseguridad" que Musk dice proveer contra la censura "woke" resultó ser en realidad otra forma de control, quizás más subliminal pero igualmente parcial. Deshipnotizar a la ciudadanía aquí implica hacer visible el rol que asumen los algoritmos en nuestras opiniones y dotarla de herramientas para exigir cambios. A medida que nuestra vida pública transcurre y (discurre) más online, quién escribe el código de las plataformas es tan crucial para nuestra forma de vivir como el que redacta las leyes.

9. Conclusiones

A modo de cierre, podemos concluir que la seguridad en la era tecno-capitalista se ha convertido en un arma de doble filo para las democracias. Por una parte, es incuestionable nuestra necesidad de seguridad -anhelamos vivir sin miedo, con estabilidad vital y sin complicaciones- y la tecnología, bien empleada, puede ofrecer mejoras genuinas en la prevención de delitos, en la gestión de riesgos sanitarios o ambientales, etc. No se aboga aquí, por tanto, por una abolición ingenua de la seguridad, sino por su reconceptualización radical. La genealogía histórica analizada (desde Hobbes hasta nuestros días 2025) evidencia que la seguridad jamás ha sido neutral: siempre estuvo ligada a las estructuras del poder imperante y a la manera histórica de entender y situar las "amenazas". Hoy, la seguridad se ha hipertrofiado y también sesgado: se absolutiza su importancia -justificando incluso la renuncia a derechos- pero al mismo tiempo se define sin reparos en función de los intereses de élites estatales y corporativas (protección del orden establecido, continuidad del consumo, control social ante disenso, etc). Esta es la esencia de nuestra tesis *peregrini*: bajo el barniz de la seguridad hipnótica, se oculta una operación ideológica de estabilización del capitalismo digital, que pospone transformaciones urgentes (como las que exige la crisis climática) y concentra poder en enclaves opacos.

18. Los modelos abiertos se basan en estándares públicos y código libre. El más usado es ActivityPub; define una API cliente-servidor y otra servidor-servidor sobre ActivityStreams 2.0. Con él miles de instancias autónomas - Mastodon, PeerTube, Pixelfed, etc. - se federan en el Fediverso, de modo que cualquier usuario puede seguir, responder o reenviar publicaciones alojadas en servidores ajenos sin crear cuentas nuevas. En junio de 2025 Meta activó en Threads un *feed* federado *opt-in* que lee ActivityPub, prueba de que incluso las grandes plataformas se ven empujadas hacia la interoperabilidad. Las ventajas clave: portabilidad de la cuenta, resiliencia (no hay punto único de fallo) y gobernanza distribuida que reduce la dependencia de APIs propietarias.

Hemos estudiado casos concretos -la regulación de IA en la UE, la vigilancia estadounidense, el sesgo de Twitter/X, - que ilustran las facetas de este fenómeno. En todos, hemos detectado la misma dinámica de normalización de la excepción: medidas antes extremas (vigilancia masiva sin orden, detención sin juicio, manipulación informativa) se vuelven rutinarias desde la retórica del miedo. Esto erosiona la calidad democrática a varios niveles: restringe libertades civiles, distorsiona la deliberación pública y desplaza la soberanía popular hacia tecnócratas y algoritmos no controlados. Se conforma así una suerte de *hipnocracia*, un orden en el que la gente cree libremente elegir mientras su campo de opciones ha sido subrepticiamente moldeado por sistemas de vigilancia y recomendaciones. La consecuencia es un debilitamiento de la democracia sustantiva: elecciones menos informadas, ciudadanía atemorizada y fragmentada, escasa capacidad para contrarrestar políticas que consolidan desigualdades.

Sin embargo, no todo está perdido. Como contrapeso, emergen resistencias y propuestas transformadoras: i) la *Demopedia* participativa como repositorio cívico colaborativo destinado a ofrecer información plural, verificada y actualizada sobre temas clave de vigilancia digital; ii) la transparencia algorítmica obligatoria, destinada a regular y auditar el funcionamiento de algoritmos utilizados en plataformas digitales y sistemas de IA, con el fin de reducir sesgos discriminatorios y abusos de poder; iii) los sindicatos o cooperativas de datos, esto es, organizaciones colectivas que permitan a la ciudadanía negociar condiciones justas para el uso de sus datos personales; iv) el desarrollo de plataformas digitales públicas o cooperativas como alternativa a las plataformas comerciales dominantes, para generar espacios digitales más éticos y menos vulnerables a la ganancia capitalista; etc, etc

La tarea no es abolir la seguridad, sino redefinirla democráticamente. Se trata de entenderla como un bien común, sometido a controles públicos y orientado al cuidado colectivo, no como excusa para el dominio estatal ni para la explotación corporativa. La seguridad digitalizada constituye un punto de inflexión para las democracias contemporáneas. Si se deja en manos de lógicas tecnocráticas y mercantiles, consolidará un régimen de control y exclusión. Si se somete a principios de transparencia, igualdad y deliberación, puede convertirse en una herramienta de emancipación. La elección sigue abierta, y dependerá de la capacidad de crítica, regulación y acción política que sepamos desplegar en los próximos años.

Bibliografía

Alkousaa, R., & Jabkhiro, J. (2023, 10 agosto). Insight: Europe cracks down after rise in “direct action” climate protests. *Reuters*. https://www.reuters.com/world/europe/after-rise-climate-direct-action-europe-cracks-down-2023-08-10/

Agamben, G. (2005). *Estado de excepción* (F. Costa e I. Costa, Trads.; 2.ª ed.). Adriana Hidalgo Editora.

Beck, U. (1992). *Risk society: Towards a new modernity* (M. Ritter, Trad.). SAGE.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.

Deleuze, G. (1992). Postscript on the societies of control. *October, 59*, 3-7. https://doi.org/10.2307/778828

Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977-1978* (M. Senellart, Ed.; G. Burchell, Trad.). Palgrave Macmillan. https://doi.org/10.1057/9780230245075

Graham, T., & Andrejevic, M. (2024). *A computational analysis of potential algorithmic bias on Platform X during the 2024 US election* [Preprint]. Queensland University of Technology. https://github.com/timothyjgraham/AlgorithmicBiasX

Han, B.-C. (2014). *Psychopolitik: Neoliberalismus und die neuen Machttechniken*. S. Fischer.

Han, B.-C. (2014). *Psicopolítica: Neoliberalismo y nuevas técnicas de poder* (A. Bergés, Trad.). Herder.

Jones, C. (2025, 29 abril). EU's secretive "security AI" plans need critical, democratic scrutiny. *Statewatch Analysis*. https://www.statewatch.org/news/2025/april/eu-s-secretive-security-ai-plans-need-critical-democratic-scrutiny-says-new-report/

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Neocleous, M. (2008). *Critique of security*. Edinburgh University Press.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117-182. https://doi.org/10.15779/z38ss13

Sankin, A., & Mattu, S. (2023, 2 octubre). Predictive-policing software terrible at predicting crimes. *The Markup*. https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes

Srnicek, N. (2017). *Platform capitalism*. Polity.

Viljoen, S. (2021). A relational theory of data governance. *Yale Law Journal, 131*(2), 573-654. https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.