



CENTRO DE REFLEXIÓN EN POLÍTICA INTERNACIONAL

Análisis de coyuntura

Año 2025 / Mes: octubre / Nº 58

El **Centro de Reflexión en Política Internacional** fue creado en 1995 y tiene como objetivos principales: promover e impulsar una instancia de análisis, discusión y seguimiento de la política internacional argentina, analizada en sus diversas fases pasadas, presentes y futuras; y constituir un ámbito de capacitación, actualización y producción académica en Política Exterior Argentina.

Coordinador: Alejandro Simonoff, **Secretarios:** Abril Bidondo, Sebastián Russo
Integrantes: Juan Gutauskas, Lucrecia Pasos, María Delicia Zurita, Matías Mendoza, Micaela Rognone, Pablo Bezus, Sebastián Schulz, Viviana Viublioment

EEUU: Entre la segunda enmienda y la agenda de seguridad nacional

Juan Gutauskas

Introducción

Cuando la humanidad entró al siglo XXI, ingresó en lo que Manuel Castells denominó como “La Era de la Información”, un término impulsado por los avances tecnológicos en las comunicaciones, especialmente por la penetración de Internet en la vida cotidiana (Castells, 1999). Se trata de un periodo histórico caracterizado por una revolución tecnológica centrada en las tecnologías digitales de información y comunicación, a la vez que emerge una suerte de estructura social dependiente de la red, que extiende su influencia a todos los ámbitos de la actividad humana.

El espacio digital o informático se hizo muy relevante para la construcción de nuevas subjetividades entre la población, más sometida que nunca a una competencia por la atención que lleva a un debate público constante y profundo, plagado de información parcial o falsa mediante el fenómeno de las *fake news*. La información se convierte en un arma poderosa que los Estados buscan dominar mediante el

control de sus espacios informáticos. La Web 2.0, con su explosión de datos, establece este nuevo territorio como un elemento central para la construcción de nuevas subjetividades políticas, un espacio de disputa competitiva entre países y como una potente herramienta para la administración pública.

La regla general que podemos establecer para este análisis es que los Estados no han permanecido impasibles frente a estos procesos históricos novedosos. Si en una primera etapa se evidenciaron lentos avances en su regulación sobre este nuevo espacio, diversos eventos han impulsado una progresiva intervención de los mismos en la red con el objetivo de construir aparatos informacionales autónomos.

La necesidad de los Estados de accionar e intervenir en este nuevo espacio informativo se enmarcan también en las transformaciones actuales del capitalismo moderno. Las clases capitalistas, nos dice Zuboff, reclaman unilateralmente para sí la experiencia humana en internet, entendiéndola como una materia prima gratuita que puede traducirse en datos de comportamiento. Los datos de navegación son insumos fundamentales para las grandes empresas quienes utilizan estos para elaborar modelos predictivos del comportamiento humano. Estos productos predictivos son comprados y vendidos en un nuevo tipo de mercado de predicciones de comportamientos que se denomina como mercados de futuros conductuales. Esto da origen a un nuevo poder que impone su dominio sobre la sociedad, la instrumentación e instrumentalización de la conducta se hace a efectos de su modificación, predicción, monetización y control del comportamiento de los individuos en sociedad (Zuboff, 2020). El cambio radical tanto en la forma de participación de usuarios en foros tradicionales como en la masividad y novedad de las redes sociales como Facebook y X (antes Twitter) e incluso el surgimiento de los sistemas de mensajería instantánea como Telegram y Whatsapp.

Argumentamos que, a partir del advenimiento de la web 2.0 estamos viviendo en un período de transición entre la sociedad de la información propuesta por Castells y el capitalismo de vigilancia de Zuboff. En este período de transición los estados en occidente incrementaron sus avances sobre el aparato informático dentro de sus fronteras mediante estrategias diversas que incluyen la asociación del Estado con sectores o fracciones de clase dentro de las denominadas *Big Tech*.

Esta lógica de poder influye directamente en la política internacional, donde estas corporaciones promueven normas globales afines a sus modelos de negocio. Esta pugna responde a una realidad estructural, descrita por Renata Ávila Pinto (2018):

Las tecnologías de la información y la comunicación (TIC), la innovación en inteligencia artificial y la capacidad de desplegar sistemas e infraestructura rápidamente en mercados emergentes, están concentradas en algunos pocos países, que ahora han entrado en una carrera por ser el número uno.

Este ensayo sostiene que se está configurando un mundo tecnopolar, alejado de las utopías promovidas por los gurús empresariales (Walt, 2021). Este nuevo orden se expresa, más bien, mediante la creación de esferas de influencia digital compuestas por una diversidad de actores, pero fundamentalmente dirigidas por intereses estatales. Se trata de una expresión novedosa de la jurisdicción y la soberanía, que trasciende el concepto tradicional de territorialidad para establecerse como un campo de competencia abierta entre potencias. Para analizar esta dinámica, examinaremos el caso de Estados Unidos, donde es posible rastrear en su evolución reciente la conformación de un bloque de poder que asocia a una fracción de las Big Tech con el proyecto político del neoconservadurismo occidental.

Internet y su transformación

La forma que toma Internet en la actualidad es muy particular, para comprender estas particularidades debemos analizar el desarrollo de lo que algunos autores han denominado Web 1.0 y Web 2.0. El primer desarrollo masivo de la infraestructura digital que conforma internet presentaba características específicas que nos llevan a denominarlo Web 1.0 (siguiendo una convención utilizada para nombrar las versiones de programas informáticos de manera consecutiva según sus actualizaciones). Esta etapa histórica surge con la masificación del uso particular de Internet y se desarrolla aproximadamente entre los años 1989 y 2004 (Cormode & Krishnamurthy, 2008). Los usuarios de esta red eran principalmente consumidores de contenido, mientras que los creadores eran pocos y poseían un conocimiento tecnológico superior al del resto, lo que les permitía desarrollar páginas web personales, comunes en esa época. Se trataba de una red más estática, con una intervención limitada por parte de los usuarios, cuyo contenido central se basaba en el texto.

Los cambios ocurridos en el espacio informático desde 2004 hasta la actualidad nos llevan a hablar de un cambio de paradigma, cuyo eje central es la transformación de la vasta mayoría de los usuarios de la web en creadores de contenido, impulsada por la aparición de redes sociales con interfaces simplificadas. Esta aparente naturaleza democrática de lo que conocemos como Web 2.0 sitúa a los usuarios en un rol protagónico, generando una conexión más profunda entre ellos gracias a la mayor diversidad de contenido, como la incorporación de imágenes, audio y videos, y la posibilidad de compartir dicho contenido de manera sencilla (Cormode & Krishnamurthy, 2008). Esto facilitó la difusión de historias, experiencias y testimonios en la red, promoviendo la creación de lazos sociales novedosos en este entorno digital. El volumen de datos que comparten los individuos se amplía hasta tal punto que su acumulación permite analizar patrones de comportamiento, aprovechados tanto por empresas como por gobiernos. Pero las apariencias engañan, como nos anticipó el escándalo de Cambridge Analytica, donde esta máscara democrática se transformó en una sutil manipulación del contenido que los usuarios visualizan. El nuevo foro democrático y libre se reveló como un juego de luces y sombras coordinado por empresas de gestión de datos y el establishment político (Amnistía Internacional, 2019).

Ante esta reconfiguración del espacio público digital, los Estados con intereses geopolíticos definidos han reconocido la imperativa necesidad de intervenir en los espacios informáticos para proteger su seguridad y soberanía. Para ello, moviliza una diversidad de actores, tanto privados como estatales, y configuran lo que se denomina "soberanía digital": un ámbito donde se favorecen o se sancionan puntos de conversación y actividades consideradas perjudiciales para la sociedad de cada Estado.

EEUU y el avance del aparato de inteligencia

Este análisis se centrará en las transformaciones del espacio informático vinculadas al ámbito de la seguridad nacional y la inteligencia, por ser dimensiones donde los objetivos estratégicos de los Estados se manifiestan con mayor claridad. Para ello, se examinará de manera particular el accionar de agencias estadounidenses como la CIA (Central Intelligence Agency) y el ICE (*United States Immigration and Customs Enforcement*), junto con las políticas implementadas durante el gobierno de Donald Trump, como un caso emblemático de esta tendencia.

El caso Snowden es un claro ejemplo de cómo, dentro de una sociedad supuestamente libre y democrática, pueden encontrarse las semillas del autoritarismo y el control. Justificado bajo la premisa de velar por la seguridad nacional, este caso reveló prácticas inquietantes de la NSA (*National Security Agency*) que datan de 2006. Basándose en una interpretación expansiva de la Patriot Act, la agencia introdujo debilidades en estándares internacionales de cifrado, facilitando la interceptación de comunicaciones. A través de proyectos como Edgehill y Cheesy Name, la NSA trabajó en descifrar el tráfico encriptado de empresas y VPNs, debilitando así la seguridad global de los sistemas de cifrado (The Guardian, 6 Sep 2013).

Asimismo, se dio inicio al programa PRISM (nombre en código del programa prisma), que se basaba en la recolección de datos y comunicaciones de ciudadanos estadounidenses en alianza con varias empresas de comunicaciones. Esto permitió a la NSA acceder directamente a los servidores de empresas como Google, Facebook, Apple y otras. Este programa abarcaba datos sensibles, como historiales de búsqueda, correos electrónicos, transferencias de archivos y chats en vivo. Aunque las empresas implicadas afirmaron colaborar solo bajo exigencias legales, PRISM elimina la necesidad de autorizaciones individuales al operar bajo "sospechas razonables" (The Guardian, 7 Jun 2013).

Además, bajo una orden judicial secreta, la NSA recolectó registros telefónicos de millones de usuarios de Verizon en Estados Unidos, incluyendo información sobre la identidad de los interlocutores, duración de las llamadas y localización. Esto se llevó a cabo de forma indiscriminada, sin requerir una conexión directa con actividades sospechosas (The Guardian, 6 Jun 2013).

En la era de la Web 2.0 y la inteligencia artificial estas herramientas de control no han hecho más que diversificarse y fortalecerse. El caso de la empresa de procesamiento de datos (también conocido como Big Data) Palantir ofrece una ventana por la que podemos observar el cambio de las políticas informáticas llevadas adelante por EEUU. Palantir es una empresa norteamericana especializada en software de gestión de datos, fundada en 2003 por Peter Thiel, un capitalista tecno-libertario y cuyos accionistas mayoritarios incluyen a fondos de inversión como Blackrock o In-Q-Tel, asociado a la CIA.

Esta empresa que creció al amparo inicial de la CIA, con una inversión de 2 millones de dólares (Buzzfeed News, 2017), para luego trabajar en conjunto con la policía de gobiernos como el alemán (Reuters, 2021) y las Fuerzas de Defensa Israelíes (Bloomberg, 2025) ofreciendo servicios de software de alerta temprana, análisis geoespaciales, y proyecciones de comportamiento, esto se traduce en la elaboración de perfiles criminales y/o insurgentes, acciones que son criticadas por llevar adelante políticas de clasificación racial.

La actual administración de Donald Trump utiliza las herramientas que provee la empresa Palantir a través de su secretario de seguridad nacional, Stephen Miller, quien además posee más de 100 mil dólares en acciones de dicha empresa (POGO, 2025). La empresa profundizó sus operaciones en el país del norte a partir de los contratos millonarios que le confirió el ICE (NPR, 2025), donde realizan tareas de vigilancia a partir de la acumulación de los datos personales de los habitantes de EEUU, sus hábitos de compras, sus redes sociales, toda la experiencia de usuario en internet puesta a disposición del gobierno estadounidense en pos de controlar el flujo migratorio.

La historia reciente de expansión continuada de estos programas no permite otorgar un beneficio de la duda al gobierno estadounidense en torno a la utilización de estas herramientas; por el contrario,

sugiere la consolidación de una infraestructura de vigilancia permanente y escalable, cuyos límites dependen más de contingencias políticas que de restricciones técnicas o legales.

Conclusiones

El análisis del caso estadounidense y su evolución en el tiempo reciente nos da una pauta del cambio que atravesó el rol del Estado a partir de la incorporación a lo que Castells denominó como la Era de la información, estableciendo una alianza estratégica con sectores de la Big tech, quienes a su vez compiten al interior del sector informático por contratos lucrativos del Estado así como por el propio mercado de las tecnologías de la comunicación.

Esto a su vez lo podríamos analizar en el plano internacional, con las *big tech* como elementos del soft power de las potencias globales. Esto lo podemos ver en el involucramiento de empresas como Palantir en distintos niveles de la administración pública de los países pertenecientes al Eje EEUU-OTAN e Israel e incluso lo podríamos ampliar a las disputas que la expansión de estos gigantes tecnológicos llevan adelante interviniendo en la política interna de los países, como lo demuestra la disputa entre X (ex Twitter) y el gobierno de Brasil (Russo, 2024). Estos casos demuestran que las herramientas de gestión de datos han dejado de ser meros instrumentos de política doméstica para convertirse en piezas centrales de la disputa interestatal. En este nuevo tablero, la hibridación público-privada se erige como un factor estratégico fundamental (Schulz, 2025).

El análisis de esta creciente intervención estatal admite múltiples lecturas. Por una parte, una perspectiva neorrealista y estado-céntrica, como la de Stephen Walt, quien afirma que las Big Tech están inevitablemente destinadas a servir a los intereses de sus Estados de origen. Por otra parte, esta transformación puede interpretarse a la luz de la teoría marxista del Estado, que lo concibe como garante de los intereses de las clases dominantes. Dicha dinámica se hace evidente en la íntima relación entre el proyecto político conservador y los intereses bursátiles, materializada en la adopción de herramientas como Palantir para la gestión estatal. Estos lazos ideológicos y económicos no son meros episodios aislados, sino transformaciones estructurales inherentes al desarrollo de la sociedad de la información, donde el capital y el poder estatal se reconfiguran mutuamente en el nuevo espacio digital.

Fuentes

- Schulz, S. (2025). Trump vs. Musk: entre aranceles y motosierras. Instituto de Relaciones Internacionales, Universidad Nacional de La Plata. <https://www.iri.edu.ar/index.php/2025/07/14/analisis-de-coyuntura-n-55-trump-vs-musk-entre-aranceles-y-motosierras/>
- Russo, S. (2024). Estados 1 – Tecnotopismo ¿0? El conflicto Brasil-Elon Musk en clave de Relaciones Internacionales. Instituto de Relaciones Internacionales, Universidad Nacional de La Plata. <https://www.iri.edu.ar/index.php/2024/11/04/analisis-de-coyuntura-n-50-estados-1-tecnotopismo-0-el-conflicto-brasil-elon-musk-en-clave-de-relaciones-internacionales/>
- Walt, S. M. (2021, 8 de noviembre). Big tech won't remake the global order. Foreign Policy. <https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order/>

- Castells, M. (1999). La era de la información: economía, sociedad y cultura (Vol. 1). Siglo xxi.
- ZUBOFF, Shoshana: La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder, trad. cast. Albino Santos, Paidós, Barcelona, 2020, 910p. Agora. Papeles de Filosofía, 41(2).
- PINTO, R. Á. (2024). ¿Soberanía digital o colonialismo digital? Nuevas tensiones alrededor de la privacidad, la seguridad y las políticas nacionales.
- Cormode, G., & Krishnamurthy, B. (2008). Key differences between Web 1.0 and Web 2.0. First Monday.
- Ball, J., Borger, J., & Greenwald, G. (2013, 6 de septiembre). Revealed: how US and UK spy agencies defeat internet privacy and security. The Guardian. <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>
- Alden, W. (2017, 21 de abril). Palantir's relationship with the intelligence community has been worse than you'd think. BuzzFeed News. <https://www.buzzfeednews.com/article/williamalden/palantirs-relationship-with-americas-spies>
- Neslen, A. (2021, 20 de octubre). Pushback against AI policing in Europe heats up over racism fears. Reuters. <https://www.reuters.com/article/europe-tech-police-idINL8N2R92HQ/>
- Schwellenbach, N. (2025, 24 de junio). Stephen Miller's financial stake in ICE contractor Palantir. Project On Government Oversight. <https://www.pogo.org/investigations/stephen-miller-conflicts-of-interest>
- Allyn, B. (2025, 1 de mayo). How Palantir, the secretive tech company, is rising in the Trump era. NPR. <https://www.npr.org/2025/05/01/nx-s1-5372776/palantir-tech-contracts-trump>
- Amnistía Internacional. (2019, 24 de julio). "El gran hackeo": Cambridge Analytica es sólo la punta del iceberg. <https://www.amnesty.org/es/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>