COMUNICACIÓN ORAL · 15 MINUTOS

Imperios digitales y poder estatal: análisis prospectivo de las relaciones conflictivas entre empresas tecnológicas y gobiernos

Una lectura criminológica desde el modelo VULCAN de geopolítica algorítmica

Dr. Abel González-García
Universidad a Distancia de Madrid (UDIMA)
abel.gonzalez@udima.es · ORCID 0000-0001-6808-1503

A Coruña, 10–12 de junio de 2026 · Facultade de Dereito (UDC)

1. Apertura

Muy buenos días. Quiero agradecer al comité organizador de la Sociedad Española de Investigación Criminológica y al grupo ECRIM de la Universidade da Coruña la oportunidad de compartir con ustedes esta comunicación, que se inscribe de lleno en el espíritu de "horizontes compartidos" que vertebra este congreso.

Permítanme empezar con una afirmación deliberadamente provocadora: el Leviatán del siglo XXI no está hecho ni de carne ni de acero, sino de código. Durante siglos el poder se definió por el control del territorio, el acceso a los recursos estratégicos y la capacidad militar. Hoy se ejerce a través de infraestructuras digitales, arquitecturas de datos y algoritmos. Y el actor central de este nuevo orden ya no es únicamente el Estado-nación: son también las grandes corporaciones tecnológicas, capaces de influir en la política, la seguridad y la cognición a escala planetaria.

Lo que les propongo en los próximos quince minutos es analizar, con mirada criminológica y prospectiva, las relaciones conflictivas —pero también simbióticas— entre lo que denomino imperios digitales, esto es, los Estados, e imperios tecnológicos, las corporaciones. Y lo haré apoyándome en un marco analítico propio, el modelo VULCAN, para terminar proyectando cuatro escenarios posibles para el período 2025–2035.

2. Del orden territorial al orden algorítmico

La criminología nació para comprender el delito en un mundo de fronteras, comisarías y tribunales. Pero el espacio en el que hoy se ejerce el poder —y donde se cometen, previenen y castigan buena parte de los delitos— ya no es territorial: es informacional. El territorio ya no se mide en kilómetros cuadrados, sino en flujos de datos e infraestructuras. Los cables submarinos, los servidores en la nube y los centros de datos constituyen el sustrato físico de una soberanía virtual.

Conviene detenerse en un dato que resume bien esta fragilidad estructural: aproximadamente el 95 % del tráfico intercontinental de datos circula por menos de

quinientos cables submarinos, en su mayoría de propiedad privada, y la mayor parte del almacenamiento en la nube reside en infraestructuras operadas por apenas cinco corporaciones radicadas en dos países. Esta concentración produce un riesgo sistémico: cualquier fallo técnico, sabotaje o conflicto geopolítico puede propagarse en cascada a escala global.

La consecuencia para nosotros, como criminólogos, es decisiva. La pregunta clásica de la geopolítica —"quién controla el territorio"— se desplaza hacia otra mucho más inquietante: quién controla la predicción. Porque la inteligencia artificial no amplifica el músculo ni la comunicación, como hicieron tecnologías anteriores: amplifica la decisión y la anticipación.

3. El modelo VULCAN como lente analítica

Para captar esta transformación propongo el modelo VULCAN, un acrónimo de seis dimensiones: Volatilidad, Incertidumbre, Limitación, Complejidad, Ansiedad y No-linealidad. Frente a marcos previos como VUCA, de origen militar, o BANI, surgido tras la pandemia, VULCAN incorpora dos elementos que aquellos descuidaban: la limitación estructural —la dependencia material de semiconductores, ancho de banda y energía— y la ansiedad colectiva, esa reacción psicosocial ante la automatización y la vigilancia que alimenta el tecnoescepticismo y la reacción populista.

El nombre no es casual. Vulcano, el dios herrero de la mitología romana, forjaba en su fragua las armas de los dioses. La metáfora del fuego está en el centro de mi propuesta: el poder digital no se posee ni se hereda, se forja —y se vuelve a forjar continuamente— en las crisis. El fuego es, a la vez, creación y destrucción. Manejado con responsabilidad, ilumina; desatado sin control, consume. Esa es la tensión ética que define la era algorítmica.

Las seis variables de VULCAN explican por qué el poder digital se comporta de manera impredecible. La volatilidad nace de unos ciclos de innovación que se miden en meses mientras las instituciones reaccionan en años. La incertidumbre proviene de la opacidad de unos sistemas cuyos resultados no pueden predecir ni sus propios creadores. La no-linealidad describe cómo un incidente menor —un bulo viral, un fallo de código, un ciberincidente— desencadena efectos desproporcionados. En este mundo, fragilidad e incertidumbre dejan de ser obstáculos para convertirse en instrumentos de poder.

4. Cinco niveles de poder algorítmico

¿Cómo se ejerce concretamente ese poder? Lo articulo en cinco niveles jerárquicos. El primero es el poder predictivo: la capacidad de extraer patrones de grandes flujos de datos y anticipar comportamientos, que sostiene desde la prevención del delito hasta el perfilado político. El segundo es el poder cognitivo, ejercido mediante la manipulación de los entornos informativos —los algoritmos de recomendación y los buscadores deciden qué se ve y qué se oculta—. El tercero es el poder decisional, que emerge cuando los sistemas algorítmicos asumen funciones de juicio antes reservadas a las personas: evaluaciones judiciales de riesgo, policía predictiva, puntuaciones crediticias. Su pretensión de

neutralidad esconde, en realidad, una automatización de la autoridad.

El cuarto nivel es el poder estratégico, asociado a la militarización de la IA: sistemas autónomos, plataformas de fusión de inteligencia, ciberdefensa algorítmica. Y el quinto es el poder simbólico, la capacidad de producir legitimidad: proclamar el liderazgo en IA funciona como un mecanismo de influencia que se autocumple.

Para la criminología, el nivel decisional es especialmente sensible. Cuando un algoritmo determina la concesión de una libertad condicional o el acceso a un crédito, la responsabilidad se diluye entre diseñadores, conjuntos de datos e instituciones. Surge así una nueva gubernamentalidad que no gobierna a través de la deliberación, sino de la optimización; y una lógica de gobierno preventivo en la que el riesgo sustituye a la culpa como base de la intervención. En los regímenes autoritarios esto habilita una vigilancia omnipresente; en las democracias, erosiona la frontera entre seguridad y control, y amenaza la autonomía cognitiva que es el cimiento de la deliberación democrática.

5. Imperios digitales frente a imperios tecnológicos

Llegamos al núcleo de esta comunicación: la relación conflictiva entre Estados y corporaciones. Los imperios digitales —Estados Unidos, China, Rusia, India, la Unión Europea— proyectan poder mediante políticas digitales, ciberdefensa y estrategias de soberanía tecnológica. Los imperios tecnológicos —Google, Amazon, Meta, Microsoft, Apple, Alibaba, Huawei, Tencent— ejercen una soberanía de facto a través del control de las plataformas, los datos y los canales de comunicación.

Cada imperio digital encarna un modelo distinto. Estados Unidos mantiene una hegemonía algorítmica basada en la innovación, donde las corporaciones privadas operan como extensiones del poder nacional. China consolida un modelo de autoritarismo digital que fusiona Partido, empresas estatales y plataformas privadas, y que exporta a través de su Ruta de la Seda Digital. Y la Unión Europea, que carece de la escala industrial de las otras dos, compensa con poder normativo: a través del Reglamento de IA y de la legislación de servicios y gobernanza de datos convierte la ética y el derecho en instrumentos de influencia geopolítica. Es lo que denomino geopolítica legislativa.

Pero si los Estados gobiernan a través de la ley, las corporaciones gobiernan a través del código. Operan como entidades cuasi-soberanas: la capitalización de algunas supera el PIB de la mayoría de los países. Ejercen una gobernanza de plataforma capaz de imponer reglas privadas a miles de millones de usuarios sin límite territorial, una jurisdicción posnacional donde los términos de servicio sustituyen a la ley constitucional y la conformidad reemplaza a la ciudadanía. Y actúan, además, como actores diplomáticos: la cooperación de Microsoft con la OTAN en ciberdefensa o los contratos de Palantir con el Pentágono y con gobiernos europeos ilustran el ascenso de una verdadera diplomacia corporativa.

6. La doble atadura: competencia y dependencia

Aquí reside la paradoja que da título a esta comunicación. La relación entre imperios digitales y tecnológicos está marcada por una doble atadura de competencia y colaboración.

Los Estados dependen de las corporaciones para la innovación y el procesamiento de datos; las corporaciones dependen del Estado para su protección y su legitimidad. Esta interdependencia genera lo que denomino simbiosis algorítmica: las empresas proporcionan a los gobiernos herramientas predictivas, y los gobiernos proporcionan a las empresas datos y tolerancia regulatoria.

Esta alianza, sin embargo, entraña un riesgo profundo. La infraestructura de gobierno se privatiza, de modo que unas pocas decisiones corporativas pueden alterar funciones nacionales críticas. La caída global de Facebook en 2021, que dejó incomunicados a varios países en desarrollo, demostró una verdad incómoda: hoy la estabilidad de la plataforma equivale a la estabilidad política. La dependencia de proveedores privados para la propia ciberseguridad crea un ecosistema de defensa compartida, pero también de vulnerabilidad compartida: un ataque contra una corporación puede reverberar en toda la infraestructura de un Estado.

El conflicto se manifiesta también como fragmentación regulatoria. Estados Unidos defiende la libertad de innovación; China prioriza el control y la seguridad; la Unión Europea enfatiza el cumplimiento ético. Tres regímenes incompatibles y, a la vez, interdependientes, que producen una tensión triangular y amenazan con fragmentar Internet en zonas normativas rivales: un splinternet de sistemas de valores.

7. Análisis prospectivo 2025–2035: cuatro escenarios

Permítanme proyectar esta dinámica hacia el futuro. Combinando las variables estructurales, dinámicas y disruptivas, y empleando metodología prospectiva, propongo cuatro escenarios sobre los ejes control–autonomía y cooperación–conflicto.

El primero, tendencial, es la hegemonía algorítmica gestionada: un orden bipolar entre Estados Unidos y China, donde la IA mantiene cierta supervisión humana y la interdependencia sostiene una "paz fría" de los algoritmos.

El segundo, optimista, es la gobernanza multilateral ética: la cooperación global cristaliza en tratados vinculantes y nace una Agencia Internacional para la Gobernanza de la IA, análoga al Organismo Internacional de Energía Atómica, con auditorías algorítmicas como práctica estándar.

El tercero, pesimista, es la vigilancia total y la fragmentación digital: las crisis económicas y ambientales justifican un gobierno de emergencia permanente, Estados y corporaciones despliegan la IA para el control poblacional, e Internet se fractura en enclaves soberanos mientras los deepfakes erosionan la confianza pública.

Y el cuarto, disruptivo, es la autonomía algorítmica y la geopolítica poshumana: sistemas autónomos que superan el control regulatorio, una diplomacia máquina-a-máquina que reemplaza la negociación humana, y algoritmos que actúan como actores de pleno derecho en el sistema internacional.

La variable crítica que atraviesa los cuatro escenarios es la legitimidad política de la inteligencia artificial. Aquí formulo lo que llamo la paradoja de la legitimidad: la tecnología

deriva su autoridad del rendimiento, pero corre el riesgo de colapsar por la desconfianza. El futuro dependerá de si avanzamos hacia un constitucionalismo algorítmico —incrustar la rendición de cuentas en el propio código— o descendemos hacia un absolutismo algorítmico, el gobierno de sistemas que nadie controla.

8. Implicaciones criminológicas y cierre

Concluyo regresando a nuestra disciplina. Hemos asistido a la transición del complejo militar-industrial del siglo XX al complejo algorítmico-inteligente del siglo XXI. El campo de batalla ya no es geográfico, sino epistemológico. Y de esta transformación emerge un nuevo horizonte de investigación que propongo llamar tecnocriminología: el estudio del cruce entre poder, tecnología y seguridad global, que vincula el cibercrimen, la gobernanza algorítmica y la victimización en un marco coherente.

Frente a este escenario, planteo cinco recomendaciones. Primera: institucionalizar la rendición de cuentas algorítmica mediante mecanismos auditables de transparencia. Segunda: incrustar la ética en el diseño, trasladando la "IA confiable" de eslogan a estándar operativo, en colaboración entre ingenieros, juristas, eticistas y criminólogos. Tercera: reforzar la diplomacia tecnológica como nueva rama de la política exterior. Cuarta: fortalecer la resiliencia social a través de la alfabetización digital y el pensamiento crítico. Y quinta: adoptar una política basada en la prospectiva, capaz de anticipar las disrupciones en lugar de limitarse a reaccionar ante ellas.

Termino con la frase que sintetiza mi argumento: en la fragua del mundo VULCAN, el poder no se conquista ni se hereda; se programa. La tarea de la criminología y de la gobernanza global es templar esa fragua algorítmica, para asegurar que la inteligencia —artificial o no— permanezca al servicio de la humanidad y no se convierta en su dueña.

Muchas gracias.

Comunicación elaborada a partir de González García, A. (2025), Digital Empires and Algorithmic Power: The VULCAN Model of Geopolitics in the Age of Artificial Intelligence. Referencias principales movilizadas: González García (2025); Floridi (2020); Floridi & Cowls (2022); Bratton (2021); Nye (2011); Zuboff (2019); Morozov; Creemers (2022); Schwab (2023); CSIS (2024); ENISA (2025); NATO StratCom COE (2023); European Commission (2024); Godet (2010). Fuente del congreso: SEIC — Congreso 2026.