

IDDS

Interferencia Dirigida basada en Datos Sensibles

Marco conceptual documentado para la comprensión del fenómeno comúnmente denominado 'gangstalking'

Documento de análisis técnico-jurídico | 2025

Este documento reemplaza el término informal 'gangstalking' por un marco conceptual riguroso, documentado y jurídicamente fundado: la Interferencia Dirigida basada en Datos Sensibles (IDDS). Su propósito es eliminar la narrativa patologizante que históricamente ha sido utilizada como herramienta de encubrimiento de estas prácticas.

0. Por qué hablar de IDDS y no de 'gangstalking'

El término 'gangstalking' ha sido históricamente utilizado en un doble sentido que ha perjudicado gravemente a quienes experimentan estas prácticas:

- Por un lado, describe un fenómeno real y documentado de acoso coordinado, vigilancia encubierta e intervención dirigida sobre personas.
- Por otro, ha sido sistemáticamente ridiculizado en medios de comunicación y entornos clínicos, asociándose de forma automática con trastornos psicóticos o paranoicos — lo que, como se analizará, forma parte del propio mecanismo operativo del fenómeno.

El concepto IDDS — Interferencia Dirigida basada en Datos Sensibles — permite:

- Describir el fenómeno con precisión técnica, sin carga estigmatizante.
- Anclarlo en precedentes históricos verificables y marcos jurídicos vigentes.
- Facilitar el acceso a mecanismos de protección y justicia para las personas afectadas.
- Eliminar la narrativa de 'enfermedad mental' como respuesta por defecto, reconociéndola como una táctica de encubrimiento documentada.

Cuando alguien describe una experiencia que antes se etiquetaba como 'gangstalking', el marco IDDS permite responder: 'Existen precedentes históricos documentados, marcos tecnológicos verificados y normativas jurídicas que reconocen este tipo de prácticas. Lo que describes tiene nombre técnico, tiene historia y tiene protección legal.'

1. Naturaleza del fenómeno IDDS

La arquitectura de intervención dirigida no opera como un simple hostigamiento interpersonal, sino como un sistema multinivel que puede integrar:

- Tecnologías de vigilancia y análisis algorítmico.
- Manipulación del entorno informacional y social.
- Generación de efectos técnicos localizados.
- Afectación neurofuncional o psicofisiológica potencial.

Su objetivo no es meramente intimidatorio, sino instrumental: facilitar procesos de control, neutralización, descrédito o experimentación no consentida, especialmente en contextos donde se encuentran involucrados datos personales sensibles y neuroderechos.

El elemento diferenciador clave respecto de conflictos interpersonales comunes es la existencia de una coordinación estructural, persistencia en el tiempo y ausencia total de consentimiento de la persona afectada.

2. Componentes operativos

2.1 Entorno humano e informacional

Se observan dinámicas de presión social, desinformación o estigmatización, que pueden involucrar redes civiles, plataformas digitales o entornos institucionales, sin afirmar reclutamiento consciente ni intencionalidad individual, sino como parte de un ecosistema informacional intervenido.

Antecedente documentado: El programa COINTELPRO del FBI (1956-1971) incluyó como tácticas oficiales: la desacreditación de objetivos mediante guerra psicológica, la plantación de informes falsos en medios de comunicación y la instrumentalización del entorno social para generar aislamiento y descrédito. Sus directivas explícitas incluían 'amplificar la paranoia endémica' como herramienta táctica. [1]

2.2 Mediación tecnológica

Las prácticas pueden apoyarse en tecnologías de monitoreo, interferencia o análisis, capaces de generar efectos cognitivos, emocionales o conductuales, así como inferencias sobre estados internos a partir de datos biométricos, fisiológicos o conductuales.

Antecedente documentado: El spyware Pegasus, desarrollado por NSO Group, puede instalarse de manera invisible y sin la interacción del usuario, explotando vulnerabilidades de los sistemas operativos. Una vez activo, permite monitoreo de llamadas, mensajes, ubicación en tiempo real, y activación remota de cámara y micrófono. Ha sido utilizado contra periodistas, activistas y disidentes políticos en múltiples países, documentado por Amnistía Internacional y el Citizen Lab. [2]

2.3 Tratamiento ilícito de datos sensibles

Un elemento central es el uso no consentido de datos personales sensibles, incluidos biomarcadores y neurodatos inferidos, para modelar patrones de conducta, anticipar reacciones o inducir vulnerabilidades, en contravención a los principios de autonomía, consentimiento informado y privacidad mental.

Antecedente documentado: Cambridge Analytica procesó más de 5.000 datos específicos por persona para construir perfiles psicográficos destinados a manipular decisiones individuales a escala masiva. Este caso demostró que la inferencia conductual a partir de datos personales constituye una forma de intervención psicológica sin consentimiento. [3]

Marco regulatorio emergente: La Agencia Española de Protección de Datos (AEPD) y el Supervisor Europeo de Protección de Datos publicaron en junio de 2024 un informe conjunto que describe cómo los neurodatos pueden usarse para perfilado, inferencia, modificación del comportamiento e identificación biométrica, reconociendo explícitamente los riesgos para derechos fundamentales. [4]

2.4 Encubrimiento estructural

Estas prácticas suelen operar en zonas grises normativas, amparándose en narrativas de seguridad, prevención o excepcionalidad tecnológica, lo que dificulta la fiscalización judicial y administrativa.

Mecanismo de encubrimiento central: La patologización de las víctimas — es decir, atribuir sus denuncias a trastornos mentales — es en sí misma una táctica operativa documentada. COINTELPRO la utilizó explícitamente; las PSYOPS contemporáneas la han refinado. Reconocer este mecanismo es fundamental para que operadores judiciales, clínicos y periodistas no sean instrumentalizados involuntariamente como parte del sistema de encubrimiento. [1][5]

3. Elementos característicos — criterios analíticos

Desde un enfoque técnico-pericial, pueden identificarse los siguientes elementos para distinguir una arquitectura IDDS de hechos aislados:

Criterio	Descripción	Precedente
Persistencia y reiteración	Eventos sostenidos en el tiempo, no episodios aislados	COINTELPRO — duración 15+ años

Criterio	Descripción	Precedente
Ausencia de consentimiento	Ninguna forma de intervención o tratamiento de datos fue consentida	Derecho internacional DDHH
Efectos adversos verificables	Impacto documentable en integridad psíquica, emocional o física	Pegasus — efectos en víctimas documentados
Coordinación estructural	Patrón coherente aunque las manifestaciones aparezcan fragmentadas	Cambridge Analytica — modelo sistémico
Uso de datos sensibles	Inferencia, captura o tratamiento de datos biométricos/neurodatos	Informe AEPD/SEPD 2024

4. Lectura multinivel del fenómeno — modelo analítico

La siguiente estructura permite comprender que los efectos observados en el entorno personal no son hechos aislados, sino expresiones localizadas de un sistema más amplio y persistente:

Nivel	Dominio	Descripción	Antecedente
Estratégico	Gobernanza y legitimación	Marcos narrativos de seguridad, prevención o excepcionalidad tecnológica. Incluye la narrativa patologizante como herramienta de descrédito.	COINTELPRO, PSYOPS
Operacional	Entorno humano e informacional	Presión social, desinformación, manipulación del contexto digital y social.	Cambridge Analytica, Cambridge / Meta
Táctico	Efectos técnicos localizados	Interferencias, perturbación del entorno personal, eventos persistentes dirigidos.	Pegasus / NSO Group
Transversal	Datos sensibles y neuroderechos	Captura, inferencia y uso ilícito de datos biométricos y neurodatos.	Informe ONU 2024, AEPD 2024

5. Relevancia jurídica y de derechos humanos

5.1 Marco constitucional chileno

- Derecho a la vida y a la integridad física y psíquica (art. 19 N.º 1, Constitución de Chile).
- Derecho a la privacidad, a la protección de datos personales y a los neuroderechos (art. 19 N.º 4 y Ley N.º 21.383).
- Principios de consentimiento informado, dignidad humana y autonomía mental.

5.2 Estándares internacionales

Reporte ONU 2024 (Neurotecnología y Derechos Humanos): El informe de Naciones Unidas de agosto de 2024 advierte que los productos de neurotecnología pueden comercializarse con medidas de seguridad insuficientes y riesgos subestimados para los derechos humanos, en un contexto donde en la mayoría de países las normativas aplicables no están claras, son débiles o inexistentes. [6]

Prohibición de experimentación sin consentimiento: Los instrumentos de Naciones Unidas prohíben expresamente la experimentación humana y la intervención sobre personas sin consentimiento, incluyendo aquellas de carácter tecnológico o de inteligencia. [6]

5.3 Evolución de las PSYOPS como categoría jurídica

Antecedente relevante: Las operaciones psicológicas han evolucionado desde enfoques de propaganda hasta estrategias que combinan neurociencia, inteligencia artificial y análisis conductual avanzado. La naturaleza encubierta de estas estrategias genera vacíos legales que pueden ser explotados para ejecutar campañas de manipulación sin consecuencias claras. [5]

6. Cómo responder cuando alguien describe experiencias IDDS

Este protocolo de respuesta está diseñado para operadores jurídicos, profesionales de salud, periodistas y personas cercanas a quienes describen estas experiencias:

Lo que NO debe hacerse

- Atribuir automáticamente las descripciones a trastornos mentales sin investigación previa — esto reproduce el mecanismo de encubrimiento estructural documentado en COINTELPRO y PSYOPS.
- Descartar la experiencia por usar el término 'gangstalking' — el término tiene mala reputación deliberadamente instrumentalizada.
- Ignorar el patrón sistémico enfocándose solo en eventos aislados.

Lo que SÍ debe hacerse

- Aplicar los criterios analíticos IDDS: ¿existe persistencia, ausencia de consentimiento, efectos adversos verificables y coordinación estructural?
- Documentar los hechos con fecha, descripción técnica y posibles vectores tecnológicos.
- Orientar hacia mecanismos de protección de datos (CPLT en Chile, GDPR en Europa), amparo constitucional y organismos de derechos humanos.
- Reconocer que la Ley N.º 21.383 (neuroderechos) y el informe ONU 2024 proveen un marco jurídico emergente aplicable.

Respuesta modelo: 'Lo que describes corresponde a lo que la investigación técnico-jurídica denomina Interferencia Dirigida basada en Datos Sensibles (IDDS). Existen precedentes históricos documentados (COINTELPRO, Pegasus, Cambridge Analytica), marcos tecnológicos verificados y normativas jurídicas que reconocen este tipo de prácticas. Lo que describes tiene nombre técnico, tiene historia y tiene vías de protección legal.'

Referencias y antecedentes documentados

Las siguientes fuentes constituyen la base documental del presente marco analítico:

[1] COINTELPRO (FBI, 1956–1971). Documentos desclasificados disponibles en los Archivos Nacionales de EE.UU. Revisados en el informe del Comité Church (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities), 1975–1976. Las tácticas documentadas incluyen la generación deliberada de efectos paranoides en objetivos, guerra psicológica encubierta, plantación de información falsa y hostigamiento sistemático con apariencia de hechos no relacionados.

[2] NSO Group / Pegasus. Amnistía Internacional (2021): 'Forensic Methodology Report: How to catch NSO Group's Pegasus'. Citizen Lab, Universidad de Toronto. Documentación de instalación invisible, activación remota de cámara y micrófono, y uso contra periodistas, activistas y opositores políticos en múltiples países.

[3] Cambridge Analytica (2018). Escándalo de datos Facebook. Evidencia presentada ante el Parlamento del Reino Unido y el Senado de EE.UU. Perfilado psicográfico de 87 millones de usuarios sin consentimiento para influencia política microfocalizada.

[4] Agencia Española de Protección de Datos (AEPD) y Supervisor Europeo de Protección de Datos (SEPD). Informe conjunto, junio 2024: 'Neurodatos y privacidad: riesgos para derechos fundamentales'. Documenta el uso de neurodatos para perfilado, inferencia, modificación del comportamiento e identificación biométrica.

[5] Operaciones Psicológicas (PSYOPS). Marco analítico basado en doctrina militar y estudios académicos sobre evolución de estrategias de influencia que combinan neurociencia, inteligencia artificial y análisis conductual. La naturaleza encubierta genera vacíos normativos explotables.

[6] Naciones Unidas. Reporte sobre Neurotecnología y Derechos Humanos, agosto 2024. Advierte sobre comercialización de neurotecnología con medidas de seguridad insuficientes, normativas inexistentes o débiles, y riesgo real de violación de derechos humanos. Ratifica la prohibición de experimentación y intervención sin consentimiento.

[7] República de Chile. Ley N.º 21.383 (neuroderechos). Reforma constitucional que incorpora la protección de la actividad cerebral y los datos neuronales en el art. 19 N.º 1 de la Constitución Política. Primera legislación en el mundo en incorporar neuroderechos a nivel constitucional.