Revista Científica
DE LA FACULTAD DE DERECHO
Y CIENCIAS SOCIALES
Y POLÍTICAS - UNNE

Vigilancia digital y derecho: del dispositivo biopolítico al déficit de legitimidad y reconocimiento en la legislación europea

Digital surveillance and law: from the biopolitical apparatus to the deficit of legitimacy and recognition in european

Naím Valerio Yánez Alonso*
Universidad de La Laguna, España
naimvalerioyanezalonso@gmail.com
ORCID: 0009-0009-8908-5111

Recepción: 4 de agosto de 2026
Aceptación: 13 de noviembre de 2026

Resumen

La vigilancia digital ha desbordado las categorías clásicas del derecho de daños y del consentimiento contractual. A partir de Foucault y de su radicalización en Agamben, se sostiene que la vigilancia algorítmica actualiza el dispositivo de captura poblacional y que en ella el derecho opera a la vez como límite y como habilitación del poder de control. Esa genealogía carece, sin embargo, de un criterio normativo para discriminar entre regulaciones legítimas e ilegítimas, déficit que se corrige articulándola con la teoría discursiva del derecho de Habermas y con la teoría del reconocimiento de Honneth. El análisis doctrinal del Reglamento General de Protección de Datos, la Carta de los Derechos Fundamentales, el Reglamento de Inteligencia Artificial y la jurisprudencia del Tribunal de Justicia de

ARTÍCULO CIENTÍFICO

*Naím Valerio Yánez Alonso: Doctor en Filosofía, Universidad de La Laguna (España); Magíster en Investigación en Filosofía, Universidad de La Laguna; Experto en Comunicación Social, Universidad Pontificia de Salamanca (España). Profesor, Departamento de Didáctica e Investigación Educativa, Universidad de La Laguna; integrante del Grupo de Investigación en Bioética y Biopolítica, Universidad de La Laguna.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

la Unión Europea (2014-2025) muestra que incluso el ordenamiento más garantista preserva, en la seguridad nacional, un núcleo de excepción con escrutinio democrático debilitado. Su legitimidad exige, además de procedimientos discursivos, preservar en el diseño de los sistemas de control el estatuto del sujeto vigilado como interlocutor y no como mero objeto de cálculo.

Palabras clave: vigilancia digital, biopolítica, legitimidad democrática, reconocimiento, derecho de la Unión Europea.

Abstract

Digital surveillance has overwhelmed the classical categories of tort law and contractual consent. Drawing on Foucault and on Agamben's radicalization of his work, it is argued that algorithmic surveillance updates the *dispositif* of population capture, and that within it law operates simultaneously as a limit on, and an enabler of, control power. This genealogy lacks, however, a normative criterion to distinguish legitimate from illegitimate regulation, a deficit addressed by articulating it with Habermas's discourse theory of law and Honneth's theory of recognition. A doctrinal analysis of the General Data Protection Regulation, the Charter of Fundamental Rights, the Artificial Intelligence Act, and the case law of the Court of Justice of the European Union (2014-2025) shows that even the most protective legal order preserves, in national security, a core of exception with weakened democratic scrutiny. Its legitimacy requires, beyond discursive procedures, preserving in the design of control systems the status of the surveilled subject as an interlocutor rather than a mere object of computation.

Keywords: digital surveillance, biopolitics, democratic legitimacy, recognition, European Union law.

1. Introducción

El paradigma liberal clásico de la privacidad, edificado sobre la idea de un derecho subjetivo a excluir a terceros de una esfera íntima previamente delimitada, presupone un sujeto capaz de identificar cuándo y por quién es observado, y una interferencia estatal puntual, excepcional y sujeta a control judicial previo. Ese presupuesto ha entrado en una crisis que no es meramente cuantitativa —no se trata solo de que hoy se vigile más—, sino cualitativa: la vigilancia digital contemporánea no interviene episódicamente sobre una esfera privada preexistente, sino que produce continuamente, mediante la datificación de la experiencia cotidiana, un doble algorítmico del sujeto sobre el que se ejercen decisiones jurídicamente relevantes —crediticias, migratorias, laborales, penales— sin

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

que medie, en la mayoría de los casos, un acto de vigilancia identificable (Cohen, 2019; Zuboff, 2020).

Frente a este desplazamiento, la filosofía política contemporánea ofrece, cuando menos, dos tradiciones de análisis irreductibles entre sí. La primera, de raíz foucaultiana y radicalizada por Agamben, describe la vigilancia digital como una forma actualizada del dispositivo biopolítico: un entramado de saber-poder que produce sujetos gobernables mediante la gestión estadística de poblaciones (Foucault, 2006) y que tiende, en su versión más extrema, a reducir al sujeto de derecho a mera nuda vida, sometida a un poder soberano que decide sobre la excepción sin estar él mismo sometido a ley alguna (Agamben, 1998, 2004). Gilles Deleuze había anticipado ya, en su post-scríptum sobre las sociedades de control, que el encierro disciplinario cedería el paso a una modulación continua de las conductas, ejercida menos por instituciones que por códigos y accesos diferenciales a redes de información (Deleuze, 2006).

La segunda tradición, representada por Jürgen Habermas y Axel Honneth como herederos críticos de la Escuela de Fráncfort, no se limita a describir el poder, sino que pregunta por las condiciones normativas de su legitimidad: bajo qué procedimientos discursivos una norma jurídica puede considerarse válida (Habermas, 1998), y bajo qué condiciones de reconocimiento intersubjetivo un sujeto puede desarrollar una relación íntegra consigo mismo (Honneth, 1997). No es casual que Habermas dedicara páginas decisivas a objetar a Foucault lo que denominó su *criptonormativismo*: la genealogía del poder describe con agudeza los mecanismos de sujeción, pero elude la pregunta acerca de los criterios normativos desde los cuales esa misma descripción resulta posible como crítica (Habermas, 1989).

Se defiende aquí la hipótesis de que ambas tradiciones son complementarias y de que su articulación resulta indispensable para pensar un derecho de la vigilancia digital que no se limite a describir la dominación ni a legitimar cualquier captura de datos amparada en una ley formalmente válida. La Unión Europea ofrece un caso de estudio privilegiado —y, hasta donde alcanza nuestro conocimiento, insuficientemente explotado por la doctrina *iushumanista* de lengua española—, pues es el ordenamiento que ha llevado más lejos la institucionalización de garantías frente a la vigilancia y, por ello mismo, el que permite observar con mayor nitidez sus límites estructurales.

2. Enfoque metodológico y criterios de selección de las fuentes

Se adopta un enfoque cualitativo, de naturaleza teórico-dogmática, que combina el análisis *iusfilosófico* de categorías con el estudio doctrinal de fuentes normativas y jurisprudenciales del derecho de la Unión Europea. El objeto es el régimen jurídico de la vigilancia digital y los criterios con que cabe evaluar su legitimidad; las prácticas de vigilancia solo se consideran tal como las describen las resoluciones judiciales o la doctrina.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

Se emplean tres procedimientos. El primero es la reconstrucción genealógica y conceptual de las nociones de dispositivo, excepción, legitimidad discursiva y reificación a partir de las obras de Foucault, Agamben, Habermas y Honneth. El segundo es la interpretación sistemática y teleológica de las normas, atenta a la relación entre derecho primario y derivado y al régimen de limitación de derechos del artículo 52.1 de la Carta. El tercero es el análisis de casos, centrado en la *ratio decidendi* y en el fallo, en el que se separa expresamente lo que el Tribunal declara de la lectura teórica que aquí se propone.

Las fuentes se seleccionaron por pertinencia material, vigencia y autoridad. En el plano normativo se incluyen los artículos 7, 8 y 52 de la Carta, el artículo 4.2 del Tratado de la Unión Europea, la Directiva 2002/58/CE y los Reglamentos (UE) 2016/679 y 2024/1689, además de la Directiva 2006/24/CE, invalidada, como objeto de la jurisprudencia examinada. En el plano jurisprudencial se analizan las sentencias del Tribunal de Justicia de la Unión Europea (TJUE) dictadas entre 2014 y 2025 sobre conservación masiva, transferencia internacional o tratamiento automatizado de datos a la luz de los artículos 7 y 8 de la Carta, a partir de su texto oficial en castellano y de los comunicados de prensa del Tribunal. La doctrina reciente (2021-2025), procedente de revistas con revisión por pares, se localizó mediante búsquedas en las plataformas de las editoriales y en repositorios institucionales con descriptores como conservación de datos, seguridad nacional, supervisión humana y decisiones automatizadas, y cada referencia se verificó en su fuente original. Se excluyen, por delimitación, la jurisprudencia del Tribunal Europeo de Derechos Humanos y el derecho interno de los Estados, salvo para explicar la recepción de una sentencia del TJUE.

3. La vigilancia digital como dispositivo biopolítico

Michel Foucault desarrolla, particularmente en los cursos dictados en el Collège de France entre 1975 y 1979, la noción de biopolítica para dar cuenta de una transformación histórica en el ejercicio del poder: el paso de un poder soberano que se ejercía ante todo como derecho de dar muerte a un poder que administra la vida de las poblaciones mediante mecanismos de regulación estadística, epidemiológica y actuarial (Foucault, 2006). Este poder no opera principalmente por prohibición, sino por producción: produce normas de conducta, tipologías de riesgo, categorías de normalidad y desviación, a través de un entramado que Foucault denomina *dispositivo* —red heterogénea de discursos, instituciones, decisiones reglamentarias, leyes, medidas administrativas, enunciados científicos y proposiciones morales que responde a una urgencia histórica y desempeña una función estratégica dominante.

Giorgio Agamben radicaliza esta genealogía. Sostiene que la política occidental se ha fundado, desde sus orígenes, en la producción de una vida biológica desnuda —la nuda

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

vida— separable de la vida cualificada políticamente, y que el campo de concentración, antes que una anomalía histórica, constituye el paradigma oculto de la modernidad política: el espacio en que la excepción se vuelve regla y el derecho suspende su propia vigencia sin dejar por ello de aplicarse (Agamben, 1998, 2004). El soberano, en esta lectura, es precisamente quien decide sobre el estado de excepción, situándose simultáneamente dentro y fuera del orden jurídico. Lo distintivo de la tesis agambeniana es la afirmación de que esa lógica de excepcionalidad tiende a normalizarse a través de mecanismos administrativos ordinarios, sin necesidad de una declaración formal de emergencia.

¿Puede sostenerse, con el mismo rigor conceptual, que la vigilancia digital contemporánea actualiza esta lógica? La respuesta que aquí se defiende es afirmativa, aunque con matices. A diferencia de la vigilancia disciplinaria clásica —centrada en instituciones de encierro y en la observación directa de cuerpos individualizados—, la vigilancia digital opera mediante la datificación masiva de la experiencia: cada interacción con un dispositivo conectado genera un rastro que es capturado, almacenado, correlacionado y empleado para producir perfiles predictivos de comportamiento. El sujeto ya no es primariamente observado, sino calculado; no se lo disciplina mediante la visibilidad constante de un panóptico arquitectónico (Foucault, 2002), sino mediante la agregación estadística de sus huellas digitales en poblaciones comparables. Byung-Chul Han describe con lucidez esta mutación: el poder disciplinario, coercitivo y prohibitivo, ha sido sustituido por una *psicopolítica* que opera mediante la seducción y la autoexposición voluntaria, en la que el propio sujeto colabora activamente en la producción de los datos que lo gobiernan (Han, 2014).

Esta transformación no diluye, sino que intensifica, la lógica biopolítica: la gestión de poblaciones mediante categorías de riesgo (el perfil crediticio, el índice de peligrosidad, la puntuación de confiabilidad ciudadana) reproduce con medios técnicos más sofisticados la misma operación que Foucault identificaba en la estadística demográfica del siglo XIX, y la excepcionalidad jurídica que habilita determinadas formas de vigilancia estatal —invocando la seguridad nacional, la emergencia sanitaria o la lucha contra el crimen organizado— reproduce la lógica agambeniana de una excepción que, lejos de ser transitoria, tiende a consolidarse *de facto* como régimen jurídico permanente. La vigilancia digital de carácter privado, propia del denominado capitalismo de la vigilancia, añade una capa adicional a este análisis.[1]

1. El llamado capitalismo de la vigilancia» designa, en la formulación de Zuboff (2020), una lógica de acumulación que extrae, mediante la datificación de la experiencia humana, excedentes conductuales destinados a la predicción y modificación del comportamiento. Sus productos —perfiles predictivos, puntuaciones de riesgo, sistemas de reconocimiento— son incorporados por el Estado mediante compras, convenios o requerimientos judiciales, lo que diluye la distinción clásica entre vigilancia pública y privada (Lyon, 2018).

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

4. Ambigüedades del derecho ante la vigilancia digital

El derecho contemporáneo exhibe una ambivalencia estructural frente a la vigilancia digital, en un doble movimiento que la doctrina *iusfilosófica* ha caracterizado como constitutivo y no meramente contingente (Cohen, 2019). Por un lado, numerosos ordenamientos han desarrollado marcos de protección de datos que reconocen derechos de acceso, rectificación, supresión y oposición y principios como la minimización y la limitación de la finalidad. Estos marcos coexisten, sin embargo, con normativas de excepción que habilitan a los organismos de seguridad e inteligencia a acceder a metadatos de comunicaciones, desplegar reconocimiento facial en el espacio público o requerir a las empresas tecnológicas información de sus usuarios bajo estándares de control judicial frecuentemente laxos o diferidos.

Esta ambivalencia no es accidental. Expresa la doble función del derecho en la economía biopolítica del control, simultáneamente limitador y habilitador del poder de vigilancia (Lyon, 2018). El derecho de protección de datos, en tanto reconoce derechos individuales, produce una legitimidad formal que oculta la continuidad de fondo entre vigilancia estatal y vigilancia privada; las cláusulas de excepción por razones de seguridad nacional operan, en la lectura agambeniana, como el punto en que el ordenamiento jurídico se abre a su propia suspensión sin declararla expresamente.

La dimensión privada de la vigilancia digital plantea, además, un desafío específico al análisis jurídico clásico, centrado tradicionalmente en la relación vertical entre el Estado y el ciudadano bajo la lógica del acto administrativo singular. Las plataformas y los proveedores de servicios de datos han desarrollado modelos de negocio fundados en la extracción sistemática de información conductual, cuyo tratamiento jurídico se articula mediante contratos de adhesión, términos de servicio y consentimientos formales cuya asimetría informativa y de poder los vuelve difícilmente equiparables a un consentimiento genuinamente autónomo en el sentido que la teoría contractual clásica presupone; Zuboff (2020) describe esa lógica como la apropiación unilateral de la experiencia humana ajena, tratada como materia prima gratuita.

El derecho, en este terreno, enfrenta la dificultad de que sus categorías clásicas —el contrato, el consentimiento individual, la propiedad sobre el dato como bien disponible— resultan insuficientes para captar una lógica de poder que opera menos mediante la coerción directa que mediante la modulación probabilística de conductas a escala poblacional (Rouvroy y Berns, 2013). La creciente porosidad entre vigilancia estatal y corporativa —convenios de intercambio de información, compras de bases de datos comerciales por agencias de seguridad o delegación de facto de funciones de control migratorio o policial en plataformas privadas— dificulta trazar, dentro del propio ordenamiento, una frontera clara entre lo público y lo privado.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

Un ejemplo paradigmático de esta porosidad se observa en los sistemas de reconocimiento facial desplegados en el espacio urbano bajo convenios de cooperación público-privada: la infraestructura de cámaras y el procesamiento algorítmico suelen ser provistos y operados por empresas privadas, mientras que la decisión de detención o identificación conserva su carácter formalmente estatal. Esta división del trabajo diluye las garantías procesales clásicas —control judicial previo, motivación individualizada, impugnación efectiva— precisamente donde resultarían más necesarias. Evaluar la regulación de la vigilancia digital exige, por ello, examinar la arquitectura institucional en la que el tratamiento tiene lugar, y no solo el catálogo de derechos individuales.

5. El marco legislativo europeo, entre garantismo y excepción

La Unión Europea constituye el caso paradigmático de un ordenamiento que ha desarrollado el sistema más articulado de garantías frente a la vigilancia digital, al elevar la protección de datos personales al rango de derecho fundamental autónomo. La Carta de los Derechos Fundamentales de la Unión Europea distingue, en sus artículos 7 y 8, el derecho al respeto de la vida privada del derecho a la protección de datos personales, exigiendo que todo tratamiento se realice de modo leal, para fines determinados y sobre la base del consentimiento u otro fundamento legítimo, bajo el control de una autoridad independiente (Carta de los Derechos Fundamentales de la Unión Europea [CDFUE], 2016).

Sobre esta base se erige el Reglamento (UE) 2016/679 (RGPD), que instituye principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización, exactitud y limitación del plazo de conservación, junto con derechos exigibles de acceso, rectificación, supresión y oposición, y con evaluaciones de impacto obligatorias cuando el tratamiento entrañe alto riesgo. Su adopción por codecisión, tras una extensa consulta pública, puede leerse como un ejercicio próximo al ideal habermasiano de legitimidad discursiva.

Esta arquitectura convive, sin embargo, con un límite estructural: en virtud del artículo 4.2 del Tratado de la Unión Europea, la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro. El TJUE ha interpretado la cláusula de forma estricta; las normas nacionales que imponen a los operadores de comunicaciones obligaciones de conservación o transmisión de datos con fines de seguridad nacional quedan sometidas a la Directiva 2002/58/CE y a la Carta, y solo las medidas que los poderes públicos ejecutan directamente escapan al derecho de la Unión (TJUE, 2020b; Rojszczak, 2021, pp. 621-622). En ese perímetro, el de mayor opacidad, persiste con más fuerza la lógica de excepción que la genealogía agambeniana identifica como estructural.

La jurisprudencia del TJUE ofrece un mapa privilegiado de esta tensión. En Digital Rights Ireland, la Gran Sala declaró inválida la Directiva 2006/24/CE sobre conservación de datos de tráfico. La invalidez no derivó de una falta de competencia de la Unión, cuya

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

base jurídica el Tribunal había confirmado años antes (Rojszczak, 2021, p. 610), sino de la desproporción de la injerencia en los derechos a la vida privada y a la protección de datos:

> Habida cuenta de todas las consideraciones anteriores, ha de considerarse que, al adoptar la Directiva 2006/24, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7, 8 y 52, apartado 1, de la Carta. (TJUE, 2014a, apdo. 69)

La conservación abarcaba a casi toda la población europea sin exigir relación alguna entre los datos y una amenaza para la seguridad pública, y el acceso de las autoridades no requería control previo independiente (apdos. 56-62). El Tribunal advirtió, además, que conservar y utilizar los datos sin informar al afectado puede generar "el sentimiento de que su vida privada es objeto de una vigilancia constante" (TJUE, 2014a, apdo. 37), observación que un lector de Foucault no puede pasar por alto.

En Schrems I, el Tribunal invalidó la decisión Safe Harbor por la incompatibilidad de los programas de vigilancia masiva estadounidenses con el nivel de protección exigido para las transferencias internacionales de datos (TJUE, 2015), decisión reiterada en Schrems II respecto del Privacy Shield (TJUE, 2020a). En Tele2 Sverige y Watson, el TJUE reafirmó que el derecho de la Unión se opone a la conservación generalizada e indiferenciada de datos de tráfico con fines de lucha contra la delincuencia (TJUE, 2016).

La Quadrature du Net exige separar los criterios del Tribunal de la lectura doctrinal que aquí se propone. El TJUE reiteró que el artículo 15.1 de la Directiva 2002/58/CE, a la luz de la Carta, se opone a la conservación generalizada, indiferenciada y preventiva de datos de tráfico y de localización. Solo la admitió cuando un Estado se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, por un tiempo limitado a lo estrictamente necesario, renovable mientras persista la amenaza y bajo el control efectivo de un órgano jurisdiccional o de una autoridad administrativa independiente con decisión vinculante (TJUE, 2020b, apdos. 135-139). El fallo permite también, con garantías específicas, la conservación selectiva, la de direcciones IP y datos de identidad civil y el análisis automatizado (apdos. 172-182).

La lectura agambeniana pertenece ya al plano doctrinal. El fallo institucionaliza una zona en la que la suspensión de la regla general depende de la constatación de una amenaza; el Tribunal la concibe como excepción temporal y controlada, mientras que Agamben sostiene que tales excepciones tienden a perpetuarse, y la recepción nacional del fallo apunta en esa dirección. Rojszczak (2021) documenta que el Conseil d'État francés dedujo en 2021, de la persistencia de la amenaza terrorista, la licitud de mantener la conservación generalizada con revisiones periódicas, lectura con la que el derecho a la privacidad

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

podría quedar "eliminado de forma permanente del ámbito de los derechos fundamentales" (p. 629, traducción propia); Tzanou y Karyda (2022, p. 124) ven en la sentencia el abandono del enfoque prohibitivo en favor de otro que abre la puerta a diversas formas de vigilancia masiva. La convergencia con Agamben es, pues, una hipótesis interpretativa que la práctica estatal tiende a corroborar, y no una afirmación del Tribunal.

En el terreno de la vigilancia algorítmica y biométrica, el Reglamento (UE) 2024/1689 (Ley de IA) prohíbe la puntuación social, sea cual sea el agente que la practique, y la identificación biométrica remota en tiempo real en espacios de acceso público con fines policiales, salvo excepciones tasadas sujetas a autorización judicial o de autoridad independiente. La negociación de estas excepciones en el trílogo, donde las posiciones más protectoras del Parlamento cedieron ante la insistencia de los Estados, ofrece un caso empírico de asimetría deliberativa en sentido habermasiano. El artículo 2.3 excluye, además, los sistemas destinados exclusivamente a fines militares, de defensa o de seguridad nacional, y Yovan (2025, pp. 3-4) advierte que esta exención puede sustraer el control migratorio a las evaluaciones de impacto y salvaguardias exigidas en otros ámbitos.

En Google Spain, el reconocimiento del llamado derecho al olvido mostró que la lógica de reconocimiento del sujeto como interlocutor no es ajena a la tradición jurídica europea (TJUE, 2014b). En Ligue des droits humains, sobre datos de pasajeros aéreos, la Gran Sala excluyó los sistemas de aprendizaje automático capaces de modificar sin intervención humana los criterios de evaluación, cuya opacidad impide comprender por qué un programa arroja una coincidencia positiva (TJUE, 2022, apdos. 194-195). Esta doble faz, garantismo general y excepción securitaria, es la manifestación más nítida de la tensión estructural examinada.

6. El déficit normativo de la crítica biopolítica

La descripción foucaultiano-agambeniana ofrece herramientas analíticas de notable potencia explicativa. Presenta, sin embargo, la dificultad ya señalada por Habermas (1989): si el derecho mismo es leído como dispositivo de producción de nuda vida, o si la excepción es concebida como estructura originaria y no como desviación patológica del orden jurídico, resulta difícil formular un criterio interno para distinguir entre una norma de vigilancia arbitraria y una norma de vigilancia sometida a control judicial efectivo, proporcionalidad y rendición de cuentas democrática.

Esta dificultad tiene consecuencias prácticas para el diseño institucional. Si toda regulación jurídica de la vigilancia es una manifestación más del mismo dispositivo de captura biopolítica, el derecho pierde su capacidad de operar como instancia de contención del poder, y la crítica corre el riesgo de desembocar en un diagnóstico totalizante, una suerte

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

de nihilismo jurídico que no ofrece orientación alguna para la acción política o jurídica concreta.

La pregunta pertinente no es, entonces, si el derecho produce sujeción —lo cual la genealogía muestra convincentemente que, en efecto, ocurre—, sino bajo qué condiciones normativas una regulación jurídica de la vigilancia puede considerarse más o menos legítima, y qué relación guarda esa legitimidad con la integridad de los sujetos sometidos a vigilancia. Es precisamente en este punto donde la teoría discursiva del derecho y la teoría del reconocimiento realizan su aporte distintivo, no como sustitutos de la genealogía crítica sino como su complemento normativamente necesario.

7. Legitimidad procedimental y esfera pública digital en Habermas

Jürgen Habermas distingue, en su teoría de la acción comunicativa, entre una racionalidad orientada al entendimiento mutuo —propia de la interacción comunicativa cotidiana, en la que los sujetos coordinan su acción mediante pretensiones de validez susceptibles de ser discutidas racionalmente— y una racionalidad estratégica orientada al éxito, propia de los subsistemas económico y administrativo, que operan mediante los medios sistémicos del dinero y el poder (Habermas, 1999). La tesis de la colonización del mundo de la vida sostiene que estos subsistemas tienden a penetrar en las esferas de la interacción comunicativa cotidiana, sustituyendo el entendimiento mutuo por mecanismos de coordinación sistémica que escapan al control democrático de los propios afectados.

La vigilancia digital puede leerse como una forma paradigmática de esta colonización. La extracción sistemática de datos conductuales convierte interacciones que originalmente pertenecían al mundo de la vida —la conversación privada, la relación afectiva, la deliberación política informal— en insumos de un cálculo estratégico orientado a la predicción y modulación del comportamiento, sin que los propios sujetos tengan posibilidad efectiva de deliberar sobre las condiciones de esa extracción. La opacidad algorítmica agrava esta colonización al sustraer del escrutinio público los criterios mismos con los que las decisiones automatizadas clasifican y afectan a los sujetos.

Frente a este diagnóstico, Habermas no concluye que el derecho sea inevitablemente cómplice de la colonización sistémica. Sostiene, en Facticidad y validez, que el derecho moderno cumple una función de bisagra entre sistema y mundo de la vida: puede operar como medio de integración sistémica —cuando se limita a garantizar formalmente la seguridad de las expectativas de comportamiento— pero también puede institucionalizar procedimientos de formación democrática de la voluntad que permiten someter las decisiones sistémicas al escrutinio de una esfera pública deliberativa (Habermas, 1998). La legitimidad de una norma jurídica, en esta perspectiva, no deriva de su mera validez formal, sino de que pueda reconstruirse racionalmente como el resultado posible de un

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

procedimiento discursivo en el que todos los afectados hubieran podido participar en condiciones de simetría argumentativa.

¿Podría la regulación vigente de la vigilancia digital reconstruirse como el resultado de un proceso deliberativo en el que los propios sujetos vigilados hubieran tenido voz efectiva? La respuesta, en la mayoría de los casos, es negativa: los términos de servicio se redactan unilateralmente, la legislación de excepción en materia de seguridad se aprueba frecuentemente con escaso debate público y los criterios de los sistemas algorítmicos permanecen protegidos por secreto comercial o razones de seguridad. El aporte habermasiano no consiste en negar la descripción biopolítica, sino en proporcionar el criterio normativo —la simetría discursiva y la transparencia deliberativa— que permite calificarla como un déficit de legitimidad, y no como un dato ontológico irremediable del poder.

El caso europeo permite calibrar este criterio. El RGPD satisface, en buena medida, el estándar de legitimidad discursiva: fue objeto de un procedimiento legislativo público, con participación de la sociedad civil, y su interpretación queda sometida al control jurisdiccional del TJUE. En la seguridad nacional, tal como la delimitó La Quadrature du Net, esa legitimidad se adelgaza; la apreciación de la amenaza corresponde a los ejecutivos nacionales, el control exigido es jurisdiccional o administrativo y no deliberativo, y la fiscalización parlamentaria de los servicios de inteligencia es con frecuencia débil. La legitimidad procedimental no es, en consecuencia, una propiedad binaria del sistema jurídico, sino una variable que se distribuye de manera desigual entre sus sectores normativos.

8. Reconocimiento y patologías de la vigilancia en Honneth

Axel Honneth desplaza el eje normativo desde la legitimidad procedimental del derecho hacia las condiciones intersubjetivas de la formación de la identidad. En La lucha por el reconocimiento, Honneth distingue tres esferas en las que los sujetos desarrollan una relación práctica consigo mismos: el amor, que funda la autoconfianza mediante vínculos afectivos primarios; el derecho, que funda el autorrespeto mediante el reconocimiento de la igual dignidad y autonomía moral de todo sujeto de derecho; y la solidaridad o estima social, que funda la autoestima mediante el reconocimiento de las capacidades y contribuciones particulares de cada sujeto a la comunidad de valores compartidos (Honneth, 1997).

Las patologías sociales no se explican, en esta perspectiva, primariamente por la distribución desigual de recursos, sino por experiencias de menosprecio —humillación, exclusión de derechos, denigración— que dañan alguna de estas tres dimensiones. En un desarrollo posterior, Honneth (2007) introduce la categoría de reificación o cosificación para describir una patología específica del reconocimiento: el olvido práctico de que el otro es, antes que un objeto de conocimiento o cálculo, un sujeto cuya perspectiva merece ser reconocida empáticamente.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

La vigilancia digital constituye, leída desde esta categoría, un caso paradigmático de cosificación institucionalizada. El sujeto vigilado es sistemáticamente traducido en variables cuantificables —puntuación crediticia, índice de riesgo, categoría de propensión al consumo o a la conducta delictiva— cuya lógica de producción prescinde estructuralmente de su perspectiva en primera persona. A diferencia del daño distributivo, reparable mediante redistribución de recursos, el daño del reconocimiento que produce la vigilancia digital es relacional: consiste en la instauración de una relación asimétrica en la que el sujeto es gestionado por sistemas que no lo reconocen como interlocutor válido, sino como fuente de datos explotable. En el control migratorio, donde esa asimetría se agudiza, Yovan (2025) observa que las personas sometidas a tecnologías de perfilado "no son tratadas como sujetos de derecho, sino como objetos de gestión securitaria" (p. 19). Han añade una vuelta de tuerca: cuando el sujeto se autoexpone voluntariamente, la cosificación se experimenta como una forma perversa de autorrealización (Han, 2014), lo que dificulta reconocerla como daño y repararla jurídicamente.

Este diagnóstico ilumina una dimensión que la crítica exclusivamente procedimental tiende a subestimar: incluso una regulación que satisficiera plenamente los estándares habermasianos podría seguir produciendo cosificación si no preserva el estatuto del sujeto vigilado como interlocutor. El propio derecho europeo ofrece un ensayo de respuesta, aún parcial, cuyo eje es el artículo 22 del RGPD, que reconoce el derecho a no ser objeto de una decisión basada únicamente en tratamiento automatizado con efectos jurídicos o de similar significación y garantiza, en los supuestos exceptuados, la intervención humana, la expresión del propio punto de vista y la impugnación. La jurisprudencia ha ensanchado ese perímetro: en SCHUFA, el TJUE calificó como decisión automatizada la puntuación crediticia de una agencia privada de la que depende de manera determinante la decisión de un tercero, para evitar una "laguna en la protección jurídica" (TJUE, 2023, apdo. 61), y en Dun & Bradstreet Austria reconoció el derecho a una explicación que permita comprender e impugnar la decisión (TJUE, 2025). La Ley de IA añade obligaciones de transparencia y supervisión humana para los sistemas de alto riesgo. En clave honnethiana, estas garantías intentan preservar al sujeto como interlocutor, aunque su eficacia depende de que la intervención humana no se reduzca a una ratificación *pro forma*. Green (2022), tras examinar 41 políticas que exigen supervisión humana de algoritmos públicos, concluye que pueden proporcionar "una falsa sensación de seguridad" (p. 1, traducción propia); Laux (2024) propone, frente a ese riesgo, institucionalizar la desconfianza hacia el propio supervisor mediante exigencias como la justificación, los mandatos periódicos o la justiciabilidad.

9. Hacia una lectura complementaria

La articulación entre la genealogía biopolítica y las teorías normativas de la legitimidad

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

y el reconocimiento no debe entenderse como una síntesis armónica que disuelve las tensiones entre ambas tradiciones, sino como una complementariedad crítica en la que cada perspectiva corrige los puntos ciegos de la otra.

La genealogía foucaultiano-agambeniana previene contra la ingenuidad de suponer que bastan procedimientos deliberativos o derechos formalmente reconocidos para neutralizar las asimetrías de poder que estructuran la vigilancia digital: un proceso legislativo participativo puede estar capturado por actores con recursos desproporcionados, y los derechos de protección de datos pueden coexistir con una cosificación efectiva de los sujetos en la práctica algorítmica cotidiana. Recíprocamente, la teoría de la legitimidad discursiva y la del reconocimiento previenen contra el determinismo distópico de una lectura exclusivamente agambeniana, en la que todo derecho aparece condenado de antemano a producir nuda vida, sin espacio para distinguir entre regulaciones que amplían el control democrático sobre la vigilancia y regulaciones que lo erosionan.

Un derecho de la vigilancia digital normativamente exigente debe satisfacer, en consecuencia, tres condiciones acumulativas —no alternativas—: primero, una condición genealógica, que exige hacer visibles los mecanismos concretos de captura y gestión poblacional que la regulación jurídica habilita o limita; segundo, una condición de legitimidad procedimental, que exige que las normas de vigilancia puedan reconstruirse como resultado de un proceso deliberativo transparente y simétrico; y tercero, una condición de reconocimiento, que exige preservar el estatuto del sujeto vigilado como interlocutor y no como mero objeto de cálculo.

El caso europeo ilustra el valor heurístico de estas tres condiciones combinadas. El ordenamiento de la Unión satisface de modo comparativamente elevado la legitimidad procedimental en la protección general de datos y avanza, aunque de manera incompleta, hacia el reconocimiento mediante el artículo 22 del RGPD y la Ley de IA; la excepción de seguridad nacional, tal como la delimitó La Quadrature du Net, muestra sin embargo que ninguna de estas condiciones se satisface homogéneamente. Coexisten en un mismo sistema jurídico sectores de alta legitimidad democrática y sectores que preservan, bajo el ropaje de la excepción justificada, la lógica de captura que la genealogía identifica como estructural, y esa coexistencia es precisamente el objeto que una teoría crítica del derecho de la vigilancia digital debe poder describir y evaluar.

10. Conclusiones

En primer lugar, la vigilancia digital contemporánea constituye una actualización refinada del dispositivo biopolítico descrito por Foucault y radicalizado por Agamben: organiza la gestión poblacional mediante la datificación masiva de la experiencia y normaliza formas de excepcionalidad jurídica que tienden a consolidarse como régimen permanente.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

Esta descripción genealógica no basta, sin embargo, para orientar el diseño jurídico-institucional, pues carece —tal como objetó Habermas (1989) a Foucault— de un criterio normativo interno capaz de distinguir regulaciones legítimas de ilegítimas.

En segundo lugar, el caso europeo ha permitido someter esta hipótesis a un contraste particularmente exigente. El RGPD, la Carta, la Ley de IA y la jurisprudencia del TJUE entre 2014 y 2025 muestran que incluso este régimen reproduce en su interior la tensión estudiada; una legitimidad discursiva robusta en la regulación general del tratamiento de datos convive con una zona de excepción, admitida por el Tribunal bajo condiciones estrictas de temporalidad y control, cuya aplicación nacional tiende a desbordarlas. Este hallazgo corrobora la hipótesis biopolítica en su núcleo más resistente, siempre que se lea como interpretación doctrinal y no como contenido de los fallos.

En tercer lugar —y esta es la tesis más fuerte que el análisis permite sostener— ningún diseño normativo de la vigilancia digital merece ser calificado de legítimo por haber superado un test de proporcionalidad o haber sido aprobado mediante un procedimiento legislativo formalmente correcto si perpetúa, en su implementación técnica cotidiana, la cosificación del sujeto vigilado. La legitimidad procedimental es condición necesaria, pero no suficiente; la condición de reconocimiento —el derecho efectivo, y no meramente declarativo, a ser tratado como interlocutor por los sistemas que nos gobiernan— constituye su complemento indispensable, y su ausencia explica buena parte del malestar difuso que la vigilancia algorítmica suscita.

Queda como agenda de investigación la exploración empírica de mecanismos institucionales concretos —auditorías algorítmicas participativas, derechos de explicación reforzados, órganos de control parlamentario de los servicios de inteligencia dotados de capacidades técnicas propias y una eventual revisión del alcance de la excepción prevista en el artículo 4.2 del Tratado de la Unión Europea— capaces de traducir en diseño normativo efectivo la articulación teórica aquí propuesta.

Referencias bibliográficas

Agamben, G. (1998). *Homo sacer: El poder soberano y la nuda vida* (A. Gimeno Cuspinera, trad.). Pre-Textos.

Agamben, G. (2004). *Estado de excepción* (F. Costa & I. Costa, trads.). Adriana Hidalgo Editora.

Carta de los Derechos Fundamentales de la Unión Europea. (2016). *Diario Oficial de la Unión Europea*, C 202, de 7 de junio de 2016, 389-405.

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press. https://doi.org/10.1093/oso/9780190246693.001.0001

Deleuze, G. (2006). Post-scríptum sobre las

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

sociedades de control. En *Conversaciones 1972-1990* (J. L. Pardo, trad.). Pre-Textos.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. *Diario Oficial de las Comunidades Europeas*, L 201, de 31 de julio de 2002, 37-47.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. *Diario Oficial de la Unión Europea*, L 105, de 13 de abril de 2006, 54-63.

Foucault, M. (2002). *Vigilar y castigar: Nacimiento de la prisión* (A. Garzón del Camino, trad.). Siglo XXI.

Foucault, M. (2006). *Seguridad, territorio, población: Curso en el Collège de France (1977-1978)* (H. Pons, trad.). Fondo de Cultura Económica.

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, *45*, Article 105681. https://doi.org/10.1016/j.clsr.2022.105681

Habermas, J. (1989). *El discurso filosófico de la modernidad* (M. Jiménez Redondo, trad.). Taurus.

Habermas, J. (1998). *Facticidad y validez: Sobre el derecho y el Estado democrático de derecho en términos de teoría del discurso* (M. Jiménez Redondo, trad.). Trotta.

Habermas, J. (1999). *Teoría de la acción comunicativa* (M. Jiménez Redondo, trad., Vols. 1-2). Taurus.

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

Honneth, A. (1997). *La lucha por el reconocimiento: Por una gramática moral de los conflictos sociales* (M. Ballestero, trad.). Crítica.

Honneth, A. (2007). *Reificación: Un estudio en la teoría del reconocimiento* (G. Calderón, trad.). Katz Editores.

Laux, J. (2024). Institutionalised distrust and human oversight of artificial intelligence: Towards a democratic design of AI governance under the European Union AI Act. *AI & Society*, *39*(6), 2853-2866. https://doi.org/10.1007/s00146-023-01777-z

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, L 119, de 4 de mayo de 2016, 1-88.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial […] (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, L, 2024/1689, de 12 de julio de 2024.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC

Rojszczak, M. (2021). National security and retention of telecommunications data in light of recent case law of the European courts. *European Constitutional Law Review*, *17*(4), 607-635. https://doi.org/10.1017/S1574019621000353

Rouvroy, A., & Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation? *Réseaux*, *177*(1), 163-196. https://doi.org/10.3917/res.177.0163

Tratado de la Unión Europea (versión consolidada). (2016). *Diario Oficial de la Unión Europea*, C 202, de 7 de junio de 2016.

Tribunal de Justicia de la Unión Europea. Gran Sala. *Digital Rights Ireland y Seitlinger y otros*. Asuntos acumulados C-293/12 y C-594/12. Sentencia del 8 de abril de 2014. ECLI:EU:C:2014:238.

Tribunal de Justicia de la Unión Europea. Gran Sala. *Google Spain y Google*. Asunto C-131/12. Sentencia del 13 de mayo de 2014. ECLI:EU:C:2014:317.

Tribunal de Justicia de la Unión Europea. Gran Sala. *Schrems*. Asunto C-362/14. Sentencia del 6 de octubre de 2015. ECLI:EU:C:2015:650.

Tribunal de Justicia de la Unión Europea. Gran Sala. *Tele2 Sverige y Watson y otros*. Asuntos acumulados C-203/15 y C-698/15. Sentencia del 21 de diciembre de 2016. ECLI:EU:C:2016:970.

Tribunal de Justicia de la Unión Europea. Gran Sala. *Facebook Ireland y Schrems*. Asunto C-311/18. Sentencia del 16 de julio de 2020. ECLI:EU:C:2020:559.

Tribunal de Justicia de la Unión Europea. Gran Sala. *La Quadrature du Net y otros*. Asuntos acumulados C-511/18, C-512/18 y C-520/18. Sentencia del 6 de octubre de 2020. ECLI:EU:C:2020:791.

Tribunal de Justicia de la Unión Europea. Gran Sala. *Ligue des droits humains*. Asunto C-817/19. Sentencia del 21 de junio de 2022. ECLI:EU:C:2022:491.

Tribunal de Justicia de la Unión Europea. Sala Primera. *SCHUFA Holding (Scoring)*. Asunto C-634/21. Sentencia del 7 de diciembre de 2023. ECLI:EU:C:2023:957.

Tribunal de Justicia de la Unión Europea. Sala Primera. *Dun & Bradstreet Austria*. Asunto C-203/22. Sentencia del 27 de febrero de 2025. ECLI:EU:C:2025:117.

Tzanou, M., & Karyda, S. (2022). Privacy International and Quadrature du Net: One step forward two steps back in the data retention saga? *European Public Law*, *28*(1), 123-154. https://doi.org/10.54648/euro2022007

Yovan, D. E. (2025). El Reglamento de Inteligencia Artificial de la Unión Europea y su impacto en los derechos de las personas migrantes: Un análisis crítico. *Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE*, *4*(1), 1-22. https://doi.org/10.30972/rcd.418114

Zuboff, S. (2020). *La era del capitalismo de la vigilancia*. Paidós.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 5. Núm.2, 2026. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.529766 - CC BY-NC