

DETECTIVES PRIVADOS

La Inteligencia Invisible. Fuentes, análisis y rigor más allá del mito.

By Martín González y Santiago

Profesor Doctor en Medicina, Seguridad y Derecho. Investigador y Profesor Universitario (PDI). Analista de Inteligencia, Seguridad y Defensa.

INTRODUCCIÓN

El autor es detective privado habilitado por el Ministerio del Interior, director y jefe de seguridad y profesor acreditado. Su trayectoria incorpora también la investigación científica y el análisis de inteligencia, seguridad y defensa.

Desde esta perspectiva interdisciplinar, La inteligencia invisible aborda **la evolución de la profesión de detective privado, sus nuevas posibilidades de especialización y su contribución potencial a la seguridad**, reivindicando el rigor metodológico de una actividad que trasciende los estereotipos tradicionales.

1. Más allá del mito

La imagen popular del detective privado continúa asociada a seguimientos, fotografías, infidelidades y escenas cinematográficas. Sin embargo, **esta representación ofrece una visión parcial de una profesión cuya complejidad permanece, en gran medida, fuera del imaginario colectivo.**

Investigar exige formular preguntas pertinentes, reconstruir secuencias de hechos, contrastar versiones y determinar qué explicaciones encuentran respaldo en la información disponible.

Superar el mito del detective **significa reconocer el rigor intelectual y metodológico de una profesión** cuyo valor reside en la solidez de sus resultados y en la capacidad de fundamentarlos.

2. Una profesión regulada

El ejercicio de la investigación privada en España está sujeto a los requisitos establecidos por **la Ley 5/2014, de 4 de abril, de Seguridad Privada**, y su normativa de desarrollo. Su ejercicio profesional requiere una **formación específica y la correspondiente habilitación.**

El artículo 37 de la Ley 5/2014, de Seguridad Privada, **regula específicamente la figura del detective privado y delimita sus funciones profesionales.** Entre ellas se

Prof. Dr. Martín González y Santiago

Dr. en Medicina, Seguridad y Derecho
Analista de Inteligencia, Seguridad y Defensa

encuentran la ejecución personal de los servicios de investigación, la elaboración de los informes correspondientes y su ratificación ante las autoridades judiciales o policiales cuando sea requerido.

La formación universitaria de detective privado, articulada en programas de **180 créditos ECTS distribuidos en tres cursos académicos**, permite establecer una comparación histórica, por duración y carga lectiva, de equivalencia, con las antiguas diplomaturas o estudios universitarios de grado medio, hoy extinguidos.

Esta preparación constituye la base para una actividad que **exige conocimientos jurídicos, capacidad de investigación y responsabilidad profesional**, y que requiere **actualización continua** ante la evolución tecnológica y la creciente complejidad de las fuentes de información.

3. Del dato a la inteligencia

El valor de una investigación reside en transformar datos dispersos en conclusiones fundamentadas mediante un proceso sistemático de obtención legítima, evaluación de fuentes, corroboración y análisis.

Su rigor exige distinguir entre **dato, hecho documentado, indicio, inferencia, hipótesis y conclusión analítica**.

La calidad del análisis depende, además, de combatir el sesgo de confirmación, contrastar explicaciones alternativas y explicitar las incertidumbres. En este sentido, la *Intelligence Community Directive 203* (ICD 203), de la comunidad de inteligencia estadounidense, constituye una referencia doctrinal útil por sus estándares de rigor analítico, evaluación de fuentes y expresión de la incertidumbre. Aunque no es una norma aplicable a la investigación privada española, sus principios pueden contribuir a fortalecer la objetividad, la trazabilidad y la solidez de los informes profesionales.

La inteligencia consiste en determinar qué se permite afirmar, con qué fundamento y grado de confianza.

4. Fiabilidad de las fuentes y credibilidad de la información

Toda investigación rigurosa debe distinguir entre la fiabilidad de la fuente y la credibilidad de la información que proporciona. La doctrina de inteligencia de la OTAN recoge esta diferenciación mediante el denominado **código del Almirantazgo**, que combina una escala alfabética (A–F) para evaluar la fiabilidad de la fuente y otra numérica (1–6) para valorar la credibilidad del dato (*AJP-2.1, Allied Joint Doctrine for Intelligence Procedures*, edición B, versión 1).

Tabla 1

Matriz de evaluación de la fiabilidad de las fuentes y la credibilidad de la información (código del Almirantazgo)

Código	Evaluación de la fuente	Código	Evaluación de la información
A	Completamente fiable	1	Confirmada por otras fuentes
B	Habitualmente fiable	2	Probablemente cierta
C	Bastante fiable	3	Posiblemente cierta
D	No suele ser fiable	4	Dudosa
E	No fiable	5	Improbable
F	Fiabilidad no evaluable	6	Veracidad no evaluable

Fuente: Elaboración propia a partir de la doctrina de inteligencia de la OTAN, AJP-2.1, Allied Joint Doctrine for Intelligence Procedures, edición B, versión 1.

Ambas dimensiones deben valorarse independientemente. Así, una valoración **B2** indica una fuente habitualmente fiable y una información probablemente cierta. **B4** expresa que la fuente mantiene esa valoración, pero el dato concreto es dudoso.

La matriz constituye una herramienta de apoyo al juicio analítico, no una obligación normativa específica para los detectives privados.

Como complemento, la *Intelligence Community Directive 203 (ICD 203)* establece estándares para explicitar las incertidumbres, distinguir la información de los juicios analíticos y considerar explicaciones alternativas.

5. Fuentes de información y disciplinas de inteligencia aplicadas

La investigación privada puede incorporar metodologías procedentes de distintas disciplinas de inteligencia para obtener, contrastar e interpretar información. **Conviene distinguir entre las fuentes de información, de las que proceden los datos, y las disciplinas y metodologías empleadas para obtenerlos, evaluarlos y analizarlos.**

OSINT (Open Source Intelligence) constituye una de las áreas de mayor aplicación práctica. **Se refiere a la obtención y el análisis de información procedente de fuentes abiertas**, incluidas las publicaciones institucionales, los registros accesibles y las fuentes digitales. En este ámbito resulta fundamental la consulta sistemática del **Boletín Oficial del Estado (BOE)**, el **Boletín Oficial del Registro Mercantil (BORME)**, los boletines oficiales autonómicos (como el **BOC de Canarias**) y los boletines oficiales provinciales (**BOP**), así como los portales de contratación pública.

En los ámbitos mercantil y patrimonial, el **Registro Mercantil** y el **Registro de la Propiedad** permiten consultar, conforme a sus respectivos regímenes de publicidad, información societaria, cargos inscritos, actos registrales y titularidades inmobiliarias.

Las **cuentas anuales depositadas en el Registro Mercantil**, incluidos el balance y la cuenta de pérdidas y ganancias (denominada habitualmente *cuenta de resultados*), aportan información relevante sobre la situación patrimonial y la evolución económica de las sociedades.

HUMINT (*Human Intelligence*) comprende la información obtenida mediante fuentes humanas, como entrevistas, declaraciones y otras actuaciones lícitas. **GEOINT** (*Geospatial Intelligence*) permite interpretar información geográfica, localizaciones y relaciones espaciales. **IMINT** (*Imagery Intelligence*) se centra en la obtención y el análisis de imágenes, atendiendo a su autenticidad, resolución y contexto. **SOCMINT** (*Social Media Intelligence*) aborda la información procedente de redes sociales y suele considerarse una especialización de OSINT, aunque su delimitación terminológica varía. Estas denominaciones identifican disciplinas o enfoques de inteligencia, no fuentes concretas de información.

Otras disciplinas requieren especial cautela. **FININT** (*Financial Intelligence*) permite analizar información financiera legítimamente accesible, sin conferir acceso general a datos bancarios o fiscales protegidos. **CYBINT** (*Cyber Intelligence*) se relaciona con la información del entorno digital. **SIGINT** (*Signals Intelligence*) y **MASINT** (*Measurement and Signature Intelligence*) corresponden a ámbitos especializados de obtención y análisis de señales, mediciones y firmas características.

6. Geolocalización, metadatos e investigación visual

Las imágenes, los vídeos y sus metadatos pueden aportar indicios relevantes para la investigación, pero su valor depende de la autenticidad, la integridad, el contexto y la posibilidad de corroboración.

Los metadatos pueden revelar características del dispositivo, marcas temporales y, cuando se conservan, coordenadas geográficas.

La **geolocalización visual** permite contrastar edificios, señalización, relieve y otros elementos identificativos con cartografía e imágenes de referencia. Asimismo, deben diferenciarse la fecha de captura, la de modificación y la de publicación, al no ser elementos necesariamente coincidentes.

Si la cuestión requiere conocimientos periciales especializados, la interpretación debe distinguirse de una acreditación forense.

7. Integridad y trazabilidad de la evidencia digital

La fiabilidad de la evidencia digital exige documentar su procedencia, obtención, tratamiento y conservación. La **trazabilidad** requiere registrar las actuaciones relevantes,

Prof. Dr. Martín González y Santiago

Dr. en Medicina, Seguridad y Derecho
Analista de Inteligencia, Seguridad y Defensa

sus responsables y su secuencia temporal, preservando el original y trabajando, cuando proceda, sobre copias controladas.

Las funciones *hash* (algoritmos que generan una huella digital única a partir de los datos de un archivo) permiten verificar la integridad de un archivo respecto de una referencia previamente registrada, pero no acreditan su autenticidad ni su procedencia.

La integridad técnica acredita la estabilidad del archivo desde una referencia verificable pero su autenticidad y eficacia probatoria requieren valoraciones adicionales conforme a las circunstancias del caso y al marco procesal aplicable.

El Reglamento (UE) n.º 910/2014 (*eIDAS*), modificado por el Reglamento (UE) 2024/1183, establece el marco europeo de identificación electrónica y servicios de confianza, incluidos los relativos a firmas y sellos electrónicos, sellos de tiempo y archivo electrónico. Su artículo 41 contempla una presunción de exactitud de la fecha y hora e integridad de los datos vinculada a los sellos cualificados de tiempo.

8. Desinformación, contenidos sintéticos y *deepfakes*

La inteligencia artificial generativa permite crear y alterar imágenes, vídeos, audios y documentos con una apariencia de autenticidad cada vez más convincente. Este fenómeno amplía el campo de la investigación privada hacia la detección de suplantaciones, el análisis de contenidos manipulados y la verificación de identidades digitales.

La identificación de *deepfakes* (contenidos audiovisuales sintéticos o manipulados mediante inteligencia artificial para imitar de forma realista la apariencia, la voz o las acciones de personas) y la investigación de fraudes basados en contenidos sintéticos constituyen ámbitos emergentes de especialización, particularmente relevantes en el entorno empresarial, los conflictos comerciales y las controversias judiciales. Su desarrollo exige integrar conocimientos de análisis digital y técnicas de verificación.

9. Ámbitos consolidados de investigación privada

El artículo 48.1 de la Ley 5/2014, de Seguridad Privada, delimita los servicios de investigación privada. Dentro de estos ámbitos se desarrollan distintas modalidades profesionales, cuyo encaje jurídico depende del objeto y las circunstancias de cada encargo:

- ✓ **Investigación empresarial y mercantil:** conflictos societarios, competencia desleal, incumplimientos contractuales e irregularidades comerciales.
- ✓ **Investigación laboral:** averiguación de hechos relacionados con obligaciones profesionales y posibles incumplimientos laborales.

- ✓ **Investigación aseguradora:** comprobación de circunstancias relativas a siniestros, reclamaciones y daños.
- ✓ **Investigación patrimonial y económica:** análisis de información societaria, patrimonial y económica legítimamente accesible.
- ✓ **Investigación personal, familiar y social:** averiguaciones sobre hechos y conductas comprendidos en el artículo 48.1.a), dentro de los límites legales.
- ✓ **Localización de personas y averiguación de paradero:** actuaciones dirigidas a determinar la localización de una persona cuando respondan a un encargo legítimo y su objeto y circunstancias permitan encuadrarlas en los servicios de investigación privada legalmente previstos. Su admisibilidad exige acreditar el interés legítimo del solicitante y respetar los derechos de la persona investigada, así como los principios de necesidad, idoneidad, razonabilidad y proporcionalidad. (No constituye una categoría autónoma expresamente enumerada en el artículo 48.1 ni sustituye las funciones policiales de búsqueda de personas desaparecidas).
- ✓ **Investigaciones vinculadas a actividades en entornos de gran concurrencia:** obtención de información dirigida a garantizar el normal desarrollo de las actividades contempladas en el artículo 48.1.b), incluidos los ámbitos feriales, hoteleros, comerciales y de espectáculos.
- ✓ **Averiguaciones relativas a delitos perseguibles a instancia de parte:** actuaciones comprendidas en el artículo 48.1.c), por encargo de los sujetos legitimados en el proceso penal.

10. Nuevos nichos y especialización profesional

La evolución tecnológica, empresarial y estratégica abre nuevas oportunidades de especialización para la investigación privada, particularmente en el análisis integrado de información, la detección de fraude y la verificación de relaciones económicas y digitales.

10.1. Inteligencia corporativa y análisis de riesgos empresariales

La inteligencia corporativa permite integrar y contextualizar información relevante para identificar riesgos, evaluar relaciones empresariales y fundamentar decisiones estratégicas. Su aplicación a la investigación privada puede contribuir a detectar vulnerabilidades, conflictos de interés e indicios de irregularidades con repercusión sobre los activos y los intereses de las organizaciones. Esta perspectiva se aborda también en el TFM de D. Jorge Hernández Ramírez, El detective privado como actor en la seguridad corporativa: análisis de su papel en la protección de infraestructuras críticas y empresas estratégicas, cuyo desarrollo tuve la oportunidad de acompañar de cerca.

10.2. Fraude digital, suplantación, criptoactivos y contenidos sintéticos

Las identidades digitales falsas, la suplantación de perfiles, los fraudes en plataformas, las estafas relacionadas con criptoactivos y la difusión de contenidos manipulados

Prof. Dr. Martín González y Santiago

Dr. en Medicina, Seguridad y Derecho
Analista de Inteligencia, Seguridad y Defensa

constituyen ámbitos de especialización. La investigación puede combinar fuentes abiertas, verificación de identidades y procedencias, análisis de imágenes y reconstrucción de cronologías para documentar hechos relevantes. En el ámbito de los criptoactivos, puede comprender el análisis de operaciones y movimientos registrados en cadenas de bloques (*blockchain*), la identificación de patrones de transacción y el seguimiento de direcciones públicas.

Cuando el asunto requiera análisis forense de dispositivos, archivos o sistemas, la colaboración con especialistas permite complementar la investigación.

10.3. Comercio electrónico, falsificación y protección de derechos

La comprobación de ofertas, vendedores, canales de distribución y posibles falsificaciones puede aportar información relevante a empresas y titulares de derechos. La documentación de anuncios, productos y relaciones comerciales permite reconstruir operaciones y fundamentar actuaciones posteriores por los cauces correspondientes.

10.4. Integridad de terceros y cadenas de suministro

La verificación de proveedores, intermediarios y relaciones comerciales permite examinar posibles inconsistencias documentales, vinculaciones empresariales relevantes y riesgos asociados a operaciones o cadenas de suministro. Estas investigaciones pueden complementarse con auditorías y procedimientos de cumplimiento normativo, especialmente cuando la evaluación requiera conocimientos técnicos o controles especializados.

10.5. Investigación en entornos sanitarios y asistenciales

Los centros sanitarios y las organizaciones asistenciales pueden requerir investigaciones sobre hechos contractuales, laborales, patrimoniales u organizativos comprendidos en el ámbito legal de la investigación privada. La especialización en estos entornos exige considerar la sensibilidad de la información tratada y delimitar cuidadosamente las actuaciones, en particular cuando puedan verse afectados datos relativos a la salud.

El desarrollo de estas especializaciones puede apoyarse en la colaboración con profesionales jurídicos, auditores, especialistas en informática forense y expertos en fraude o cumplimiento normativo. Su valor diferencial reside en combinar capacidades complementarias para abordar investigaciones de mayor complejidad.

11. Propuesta de reforma legislativa

11.1. Seguridad e inteligencia

La creciente interdependencia de las amenazas físicas, digitales e híbridas refuerza una tesis que he defendido en publicaciones anteriores: la seguridad y la inteligencia constituyen un binomio indisociable. Esta concepción encuentra especial relevancia en la protección de las entidades críticas, cuyo marco europeo de resiliencia establece la Directiva (UE) 2022/2557 (CER).

He desarrollado esta perspectiva en Seguritecnia, en «*Global Blackout*: del “cero energético” al “cero digital”, binomio indisociable» (30 de abril de 2025), y en Delta 13 News, entre otras aportaciones, en «El director de seguridad, en el eje de la protección total» (8 de mayo de 2026).

La inteligencia constituye una dimensión estratégica de su evolución. Esta premisa fundamenta la necesidad de revisar el marco normativo de la seguridad privada para adecuarlo a los riesgos y exigencias de protección contemporáneos.

11.2. Actualización legislativa y renovación del desarrollo reglamentario

La Ley 5/2014, de 4 de abril, de Seguridad Privada, supuso un avance en la ordenación del sector. Sin embargo, continúa conviviendo con disposiciones del Reglamento aprobado por el Real Decreto 2364/1994 que mantienen su vigencia en cuanto no se opongan a la legislación posterior.

Desde mi perspectiva, **resulta aberrante que una actividad de esta relevancia siga apoyándose en un desarrollo reglamentario concebido en 1994**, pese a la profunda transformación tecnológica, funcional y organizativa experimentada desde entonces. **La distancia entre aquella realidad y las necesidades actuales de protección evidencia un desfase que exige una respuesta legislativa decidida.**

Por ello, propongo una revisión integral y ulterior sustitución de la Ley 5/2014, así como la aprobación de un desarrollo reglamentario actualizado, coherente y coetáneo con la ley y adaptado a las nuevas realidades de la seguridad del siglo XXI, considerando todos los riesgos emergentes, así como los de 4ª generación, amenazas híbridas, además del contexto social y geoestratégico actual.

11.3. Rango normativo y garantías constitucionales

Junto con la actualización normativa, mantengo mi propuesta de estudiar la configuración de la regulación mediante ley orgánica, en los términos constitucionalmente procedentes. Esta reivindicación responde a la relevancia de

determinadas actuaciones de seguridad privada y a su posible incidencia sobre derechos fundamentales, entre ellos la intimidad, la libertad personal y la protección de datos.

El artículo 81 de la Constitución Española reserva la ley orgánica a determinadas materias, incluido el desarrollo de los derechos fundamentales y las libertades públicas.

La reforma debería establecer una arquitectura normativa clara, con garantías proporcionadas, competencias delimitadas, responsabilidades definidas y procedimientos de supervisión acordes con las necesidades actuales.

11.4. Integración de la investigación privada y la inteligencia corporativa

El artículo 36.1.i) de la Ley 5/2014 atribuye al director de seguridad la función de realizar las comprobaciones necesarias sobre el personal que, por las funciones encomendadas, necesite acceder a determinadas áreas o informaciones, para garantizar la protección efectiva de la entidad.

La propuesta consiste en **articular la investigación privada y la inteligencia corporativa dentro de la estructura de seguridad de las organizaciones**. Bajo las prioridades de protección definidas por el director de seguridad, los detectives privados habilitados podrían desarrollar las investigaciones propias de su ámbito profesional, mientras que el análisis de inteligencia permitiría contextualizar los resultados y orientar las decisiones.

Esta propuesta debe respetar el régimen de incompatibilidades del artículo 37.3 de la Ley 5/2014, **por lo que su desarrollo exige delimitar, mediante la correspondiente actualización normativa, las funciones, responsabilidades y garantías de una coordinación efectiva entre profesionales diferenciados**.

Esta articulación permitiría vincular la investigación de hechos concretos con la evaluación de riesgos, la detección de vulnerabilidades y la protección de activos estratégicos, **respetando las competencias legalmente atribuidas a cada profesional**.

12. Seguridad Nacional y Protección de Entidades Críticas

La Ley 5/2014, de Seguridad Privada, establece en sus artículos 14 y 37 obligaciones de colaboración de los despachos y detectives privados con las Fuerzas y Cuerpos de Seguridad. Por su parte, el artículo 7 de la Ley 36/2015 contempla la colaboración del sector privado en materia de seguridad nacional.

En la protección de las infraestructuras críticas, el artículo 16 de la Ley 8/2011 exige que el responsable de Seguridad y Enlace del operador crítico disponga de habilitación de director de seguridad. Asimismo, los artículos 13 y 14 de la Directiva (UE) 2022/2557

(CER) contemplan medidas de resiliencia relativas a la protección del personal y los derechos de acceso, incluidas determinadas comprobaciones de antecedentes conforme al ordenamiento aplicable.

13. Producto de Inteligencia, Informe de Investigación y Valor Probatorio

El producto de inteligencia transforma información evaluada y analizada en conocimiento útil para fundamentar decisiones. Su formato depende de la finalidad perseguida, mientras que el informe de investigación constituye una exigencia documental específica de la actividad del detective privado.

Los artículos 49 y 50 de la Ley 5/2014, de Seguridad Privada, regulan el informe de investigación, que debe ajustarse al objeto y la finalidad del encargo, documentar las actuaciones realizadas y respetar los deberes de reserva profesional.

En el ámbito procesal civil, los artículos 265.1.5.º y 380 de la Ley de Enjuiciamiento Civil regulan la aportación del informe y la declaración de su autor cuando los hechos no sean reconocidos como ciertos. En el orden social, la **STS 551/2023, de 12 de septiembre (ECLI:ES:TS:2023:3677)** precisa que el informe del detective ratificado en juicio constituye la plasmación escrita de la prueba testifical sobre los hechos observados por su autor.

PERORATIONES

1. La inteligencia invisible consiste en transformar información dispersa en conocimiento útil y fundamentar decisiones. En esa capacidad reside el potencial de evolución de la investigación privada.
2. La inteligencia corporativa, el fraude digital, la verificación de contenidos sintéticos y la protección de activos estratégicos abren nuevas vías de especialización, mientras que la inteligencia artificial amplía las posibilidades de análisis y las exigencias de verificación.
3. La integración de la investigación privada y la inteligencia corporativa en la protección de las entidades críticas, así como su posible contribución a la seguridad pública y nacional, exige estudiar nuevas formas de articulación normativa.
4. **Todo ello exige una reforma legislativa que abandone la desidia y el desfase que arrastra el sector.**
5. **Resulta difícil justificar que una ley del siglo XXI siga cautiva de un reglamento del siglo XX, concebido en 1994.**

REFERENCIAS

- Constitución Española. Boletín Oficial del Estado, 311, de 29 de diciembre de 1978, 29313–29424. [https://www.boe.es/eli/es/c/1978/12/27/\(1\)/con](https://www.boe.es/eli/es/c/1978/12/27/(1)/con)
- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo. Diario Oficial de la Unión Europea, L 333, de 27 de diciembre de 2022, 164–198. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=es>
- González y Santiago, M. (2025, 30 de abril). *Global Blackout: del «cero energético» al «cero digital», binomio indisociable. La crisis que paralizó a España salvo los archipiélagos. Seguritecnia*. https://www.seguritecnia.es/sectores/proteccion-de-infraestructuras-criticas/global-blackout-del-cero-energetico-al-cero-digital-la-crisis-que-paralizo-a-espana_20250430.html
- Hernández Ramírez, J. (2026). El detective privado como actor en la seguridad corporativa: análisis de su papel en la protección de infraestructuras críticas y empresas estratégicas [Trabajo de fin de máster inédito].
- Intelligence Community Directive 203: Analytic standards. (2015). Office of the Director of National Intelligence. <https://www.dni.gov/files/documents/ICD/ICD-203.pdf>
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Boletín Oficial del Estado, 7, de 8 de enero de 2000. <https://www.boe.es/eli/es/l/2000/01/07/1/con>
- Ley 5/2014, de 4 de abril, de Seguridad Privada. Boletín Oficial del Estado, 83, de 5 de abril de 2014. <https://www.boe.es/eli/es/l/2014/04/04/5/con>
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Boletín Oficial del Estado, 102, de 29 de abril de 2011. <https://www.boe.es/eli/es/l/2011/04/28/8/con>
- Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social. Boletín Oficial del Estado, 245, de 11 de octubre de 2011. <https://www.boe.es/eli/es/l/2011/10/10/36/con>
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Boletín Oficial del Estado, 233, de 29 de septiembre de 2015. <https://www.boe.es/eli/es/l/2015/09/28/36/con>
- NATO Standardization Office. (2016). *Allied joint doctrine for intelligence procedures* (AJP-2.1, Edition B, Version 1). North Atlantic Treaty Organization.
- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada. Boletín Oficial del Estado, 8, de 10 de enero de 1995. <https://www.boe.es/eli/es/rd/1994/12/09/2364>
- Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Diario Oficial de la Unión Europea, L 257, de 28 de agosto de 2014, 73–114. <https://eur-lex.europa.eu/eli/reg/2014/910/oj/spa>
- Tribunal Supremo, Sala de lo Social. (2023, 12 de septiembre). *Sentencia 551/2023* (ECLI:ES:TS:2023:3677). Iberley. <https://www.iberley.es/jurisprudencia/sentencia-social-tribunal-supremo-12-9-23-48534048>