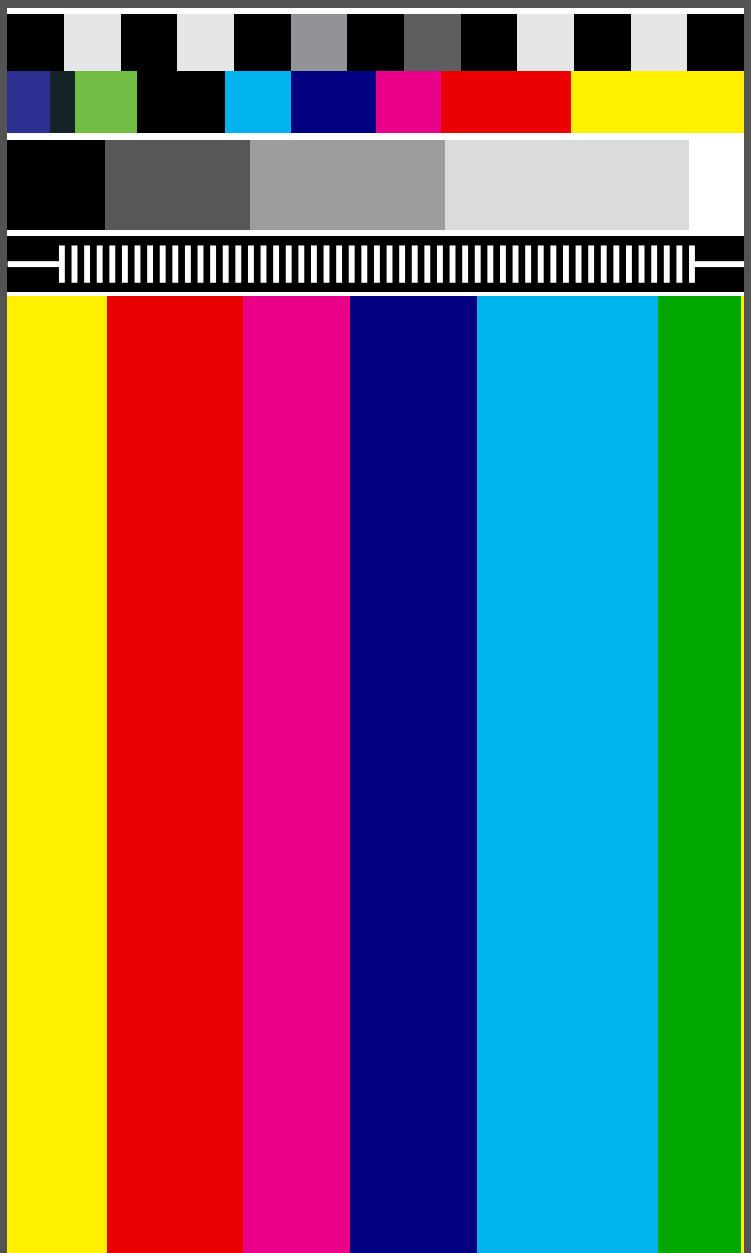
LA CONSTRUCCIÓN DE ESTÁNDARES LEGALES PARA LA VIGILANCIA EN AMÉRICA LATINA

PARTE II: REGLAS COMPARADAS A NIVEL GLOBAL

MARCO CORREA
J. CARLOS LARA
MARÍA PAZ CANALES



DERECHOS DIGITALES
América Latina

LA CONSTRUCCIÓN DE ESTÁNDARES LEGALES PARA LA VIGILANCIA EN AMÉRICA LATINA

PARTE II: REGLAS COMPARADAS A NIVEL GLOBAL

MARCO CORREA
J. CARLOS LARA
MARÍA PAZ CANALES

@ | DERECHOS DIGITALES
América Latina

Portada y diagramación: Javiera Méndez
Correcciones: Vladimir Garay
Septiembre de 2018.

Esta publicación fue posible gracias al apoyo de Global Partners Digital

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción de la libertad de expresión, el acceso a la cultura y la privacidad.

1. Introducción

El propósito de esta investigación es relevar los estándares normativos que se han desarrollado a nivel comparado y en el sistema internacional de protección de los derechos humanos, que permitan identificar los elementos que debieran encontrarse presentes en un marco normativo para el uso de tecnologías de vigilancia en forma respetuosa de los derechos fundamentales. No con un ánimo de recoger y comparar normativas, sino de construir estándares accionables a partir de los cuales iniciar procesos de cambios regulatorios y prácticos en el uso de herramientas de vigilancia.

La metodología del estudio consideró el levantamiento de legislaciones locales, revisión de jurisprudencia y se apoyó en la doctrina sobre cada uno de los puntos expuestos. Lo anterior, acompañado de la referencia a casos de estudio específicos conocidos a partir de hechos noticiosos con el objeto de dar cuenta de algunas hipótesis que subyacen a la investigación. El informe pretende proveer hallazgos sobre los estándares que las normativas comparadas –que han sido objeto de revisión a la fecha– utilizan para regular la vigilancia y constatar si es que estos cumplen o no con los principios que desde Naciones Unidas y el Sistema Interamericano de Derechos Humanos recomiendan para precaver el respeto de los derechos fundamentales en su implementación.

Se han escogido cinco áreas temáticas de estudio: (1) Leyes que contemplan capacidades de inteligencia; (2) Normativa que regula la interceptación de comunicaciones; (3) Normativa que regula la retención de datos y metadatos por proveedores de servicios (ISPs); (4) Normativa que regula la televigilancia; y, (5) Normativa que regula el uso de biometría. Después del análisis, en la Parte I, de la normativa más relevante en América Latina, esta Parte II explorará algunas normas ejemplares de países como Alemania, Australia, Estados Unidos, Nueva Zelanda y Reino Unido.

2. La situación comparada de países fuera de América Latina

2.1. Leyes de inteligencia: organismos de inteligencia y facultades

2.1.1. Reino Unido

Los organismos de inteligencia del Reino Unido son tres; el Servicio Secreto (MI5), que opera al interior del país y depende del Ministerio del Interior; el Servicio de Inteligencia Secreto (SIS o MI6), que opera en el extranjero; y el Cuartel General de Comunicaciones del Gobierno (*Government Communications Headquarters*, GCHQ), dedicado a la inteligencia de señales, siendo estos dos últimos dependientes del Ministerio de Relaciones Exteriores.[1]

Las funciones de los organismos son reguladas por la Ley de Servicios de Inteligencia de 1994 (*Intelligence Services Act*, ISA)[2] y la Ley del Servicio Secreto de 1989 (*Security Service Act*, SSA):[3]

Organismo	Funciones
MI5 (art. 1 SSA)	• Protección de la seguridad nacional y, en particular, su protección contra amenazas de espionaje, terrorismo y sabotaje, de las actividades de agentes extranjeros y de acciones dirigidas a derrocar o socavar la democracia parlamentaria por medios políticos, industriales o violentos. • Salvaguardar el bienestar económico de UK contra amenazas presentadas por acciones o intenciones de personas que estén fuera de las Islas Británicas. • Actuar en apoyo de las actividades de las fuerzas policiales, la Agencia Nacional del Crimen y otras agencias en la prevención y detección de crímenes serios.
MI6 (art. 1(1) ISA)	• Obtener y proveer información relativa a las acciones o intenciones de personas que estén fuera de las Islas Británicas. • Realizar otras tareas relativas a las acciones o intenciones de dichas personas.

1 Feikert-Ahalt, Clare (2016a). Foreign Intelligence Gathering Laws: United Kingdom. Disponible en: <https://www.loc.gov/law/help/intelligence-activities/unitedkingdom.php>

2 Texto disponible en: <https://www.legislation.gov.uk/ukpga/1994/13>

3 Texto disponible en: <https://www.legislation.gov.uk/ukpga/1989/5>

GCHQ (art. 3(1) ISA)	• Monitorear, usar o interferir con las emisiones electromagnéticas, acústicas y otras y cualquier equipo que las produzca, y obtener y proveer información, derivada o relativa de dichas emisiones, equipos o de material cifrado. • Proveer asesoría y asistencia sobre lenguajes, incluyendo terminología usada en materias técnicas, criptografía y otras materias relativas a la protección de la información y otros materiales a las fuerzas armadas, al gobierno o, en casos que se considere apropiado, a otras organizaciones o personas o al público en general.

Tanto el MI6 como el GCHQ podrán ejercer sus funciones solo: (i) en interés de la seguridad nacional, en particular de las políticas internacionales del gobierno; (ii) en el interés del bienestar económico de UK; y (iii) en apoyo a la prevención o detección de crímenes serios.[4]

El artículo 5 ISA establece un régimen de órdenes (*warrants*), emanadas por el ministro competente, para autorizar las acciones de las agencias de inteligencia que interfieran con la propiedad o la comunicación inalámbrica. Según expertos, el régimen de autorización de las agencias de inteligencia es mucho más amplio que el otorgado a otras agencias de vigilancia interna.[5]

La **Ley de Poderes de Investigación** de 2016 (*Investigatory Powers Act*, IPA),[6] también conocida como *Snoopers' Charter*, es una ley que reorganizó sustancialmente la legislación de inteligencia del Reino Unido, ya que modificó la ISA y la **Ley de Regulación de los Poderes de Investigación** de 2000 (*Regulation of Investigatory Powers Act,* RIPA)[7] y derogó la **Ley de Retención de Datos y Poderes Investigativos de 2014** (*Data Retention and Investigatory Powers Act,* DRIPA). Regula la interceptación de comunicaciones, la interferencia de equipos y la adquisición y retención de datos de comunicaciones, bases de datos personales masivos y otros tipos de información.

En el artículo 2 IPA se establecen deberes generales de privacidad. En el ejercicio de vigilancia, la autoridad debe atender a criterios de necesidad y proporcionalidad: (i) si existen métodos menos intrusivos para obtener la información; (ii) si el nivel de protección de la información es mayor por ser un dato particularmente sensible; (iii) al interés público y la integridad y seguridad de las telecomunicaciones y servicios postales; y (iv) otros aspectos de interés público en la protección de la privacidad.

---

4 Cf. art. 1(2), 3(2) ISA. Cabe señalar que, con respecto al GCHQ, en la causal del interés económico se agrega que sus funciones deben ejecutarse "en relación a las acciones o intenciones de personas que estén fuera de las Islas Británicas".

5 Feikert-Ahalt, Clare (2016a). Op. cit.

6 Texto disponible en: < https://www.legislation.gov.uk/ukpga/2016/25>

7 Texto disponible en: <https://www.legislation.gov.uk/ukpga/2000/23>

La **Ley de Derechos Humanos** de 1998 (*Human Rights Act 1998*, HRA)[8] establece limitaciones a los organismos de inteligencia, mediante la consagración de los derechos al respeto de la vida familiar y privada (Anexo 1, art. 8) y la libertad de expresión (Anexo 1, art. 10).[9] Su art. 7 permite a los ciudadanos accionar en contra de las autoridades públicas que contravengan estos derechos frente a un tribunal competente; en el caso de las acciones de vigilancia dicha competencia recae en el *Investigatory Powers Tribunal*, creado por el artículo 65 RIPA.[10]

2.1.2. Estados Unidos

La legislación federal de inteligencia de los Estados Unidos está contenida fundamentalmente en las leyes que regulan sus servicios de inteligencia, el Decreto 12333 y la Ley de Vigilancia de la Inteligencia Extranjera y sus posteriores enmiendas.[11]

Existe una amplia red de **organismos de inteligencia** en los Estados Unidos, la cual está compuesta por 17 agencias y departamentos que se agrupan en la Comunidad de Inteligencia (*Intelligence Community*, IC). De estas, las principales instituciones son la Agencia Central de Inteligencia (*Central Intelligence Agency*, CIA), creada por la *National Security Act* de 1947,[12] y la Agencia de Seguridad Nacional (*National Security Agency*, NSA), creada por la *National Security Agency Act* de 1959,[13] además de algunos departamentos del Buró Federal de Investigaciones (*Federal Bureau of Investigation*, FBI).

Las funciones de esos organismos de inteligencia están contenidas en el Decreto 12333 (*Executive Order 12333*), emitido por el presidente Ronald Reagan en 1981, y modificado por los Decretos 13284 de 2003, 13355 de 2004 y 13470 de 2008:[14]

---

8 Texto disponible en: <https://www.legislation.gov.uk/ukpga/1998/42>

9 Human Rights Act 1998. The Investigatory Powers Tribunal. Disponible en: <http://www.ipt-uk.com/content.asp?id=17>

10 General Overview and Background. The Investigatory Powers Tribunal. Disponible en: <http://www.ipt-uk.com/content.asp?id=10>

11 NSA (2013). The National Security Agency: Missions, Authorities, Oversight and Partnerships. Disponible en: <https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml>

12 Título 50 Capítulo 44 del U.S. Code. Texto disponible en: <https://www.law.cornell.edu/uscode/text/50/chapter-44>

13 Título 50 Capítulo 47 del U.S. Code. Texto disponible en: < https://www.law.cornell.edu/uscode/text/50/chapter-47>

14 Texto disponible en: <https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf>

Organismo	Funciones
CIA (art. 1.7(a))	• Recolectar (incluso a través de medios clandestinos), analizar, producir y diseminar inteligencia y contrainteligencia extranjera. • Llevar a cabo actividades de contrainteligencia sin asumir o realizar ninguna función de seguridad interna dentro de los Estados Unidos. • Llevar a cabo actividades de apoyo administrativo y técnico dentro y fuera de los Estados Unidos según sea necesario para la cobertura y los acuerdos de propiedad. • Llevar a cabo actividades de acción encubierta aprobadas por el presidente. • Llevar a cabo relaciones de enlace de inteligencia extranjera con inteligencia o servicios de seguridad de gobiernos extranjeros u organizaciones internacionales. • Coordinar la implementación de las relaciones de inteligencia y contrainteligencia entre elementos de la IC y los servicios de inteligencia o seguridad de gobiernos u organizaciones internacionales. • Realizar otras funciones y deberes relacionados con la inteligencia.
NSA (art. 1.7(c))	• Recolectar (incluso a través de medios clandestinos), procesar, analizar, producir y difundir información y datos de inteligencia de señales para propósitos de inteligencia y contrainteligencia extranjera, para apoyar misiones nacionales y departamentales. • Establecer y operar una organización efectiva unificada para las actividades de inteligencia de señales. • Controlar las actividades de recopilación y procesamiento de inteligencia de señales. • Llevar a cabo actividades de apoyo administrativo y técnico dentro y fuera de los Estados Unidos, según sea necesario para los arreglos de cobertura. • Proporcionar apoyo de señales de inteligencia para los requisitos nacionales y departamentales, y para la realización de operaciones militares. • Actuar como Gerente Nacional de Sistemas de Seguridad Nacional. • Prescribir las normas de seguridad que cubren las prácticas operativas, incluida la transmisión, manejo y distribución de señales de seguridad y material de seguridad de las comunicaciones. • Llevar a cabo relaciones extranjeras de enlace criptológico.
FBI (art. 1.7(g))	• Recolectar (incluso a través de medios clandestinos), analizar, producir y difundir inteligencia y contrainteligencia extranjera para apoyar las misiones nacionales y departamentales. • Realizar actividades de contrainteligencia. • Llevar a cabo inteligencia y contrainteligencia extranjera.

La **Ley de Vigilancia de la Inteligencia Extranjera** de 1978 (*Foreign Intelligence Surveillance Act*, FISA)[15] fue la respuesta al poder sin contrapesos que tenía el presidente de los Estados Unidos desde la Segunda Guerra Mundial para realizar actividades de vigilancia, y que culminó con el famoso escándalo conocido como *Watergate* (1972).[16] FISA tiene como principal objetivo regular la autorización de la vigilancia electrónica para obtener información de inteligencia desde el extranjero.

Ha sido modificada en numerosas oportunidades desde los ataques terroristas de 2001: ***PATRIOT Act*** (2001), ***Protect America Act*** (2007), ***USA Freedom Act*** (2015) y la ***FISA Amendments Act*** de 2008 (FAA).[17] Paradójicamente, esta última ley terminó por otorgar a la NSA el poder prácticamente sin restricciones de monitorear la actividad en línea de los ciudadanos estadounidenses (mediante llamadas internacionales, mensajes de texto y correos electrónicos) con el pretexto de investigar a extranjeros fuera del país.[18] Los efectos de la FAA fueron renovados por la *FISA Amendments Reauthorization Act* de 2017.[19]

Además, las actividades de vigilancia están limitadas por la Cuarta Enmienda a la Constitución de los Estados Unidos, que establece: "el derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".[20] Esta norma es la base para establecer que la vigilancia electrónica, al constituir un tipo de pesquisa, debe estar sujeta a una orden de búsqueda (*warrant*).[21]

2.1.3. Alemania

La legislación federal de inteligencia de Alemania está contenida fundamentalmente en las leyes que regulan sus servicios de inteligencia y la Ley que Restringe el Secreto Epistolar, Postal y de Telecomunicaciones (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*), también conocida como Ley del Artículo 10 (*Artikel 10-Gesetz*).[22]

Existen tres organismos de inteligencia en Alemania: la Oficina Federal para la Protección de la Constitución (*Bundesamt für Verfassungsschutz*, BfV), el Servicio de Contrainteligencia Militar (*Militärischer Abschirmdienst*, MAD), que se especializan en inteligencia interior

15 Texto disponible en: <https://www.law.cornell.edu/uscode/text/50/chapter-36>

16 The Foreign Intelligence Surveillance Act: Legislating a Judicial Role in National Security Surveillance. Michigan Law Review, vol. 78, no. 7. Disponible en: <https://www.jstor.org/stable/1288093>

17 Texto disponible en: <https://www.congress.gov/bill/110th-congress/house-bill/6304/text>

18 <https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance>

19 Texto disponible en: <https://www.congress.gov/bill/115th-congress/house-bill/4478/text>

20 La Carta de Derechos. National Archives. Disponible en: <https://www.archives.gov/espanol/declaracion-de-derechos.html>

21 Jurkowski, Stephanie (2017). Electronic Surveillance. Disponible en: <https://www.law.cornell.edu/wex/electronic_surveillance>

22 Deutscher Bundestag (2010). Op. Cit.

o doméstica, y el Servicio Federal de Inteligencia (*Bundesnachrichtendienst*, BND), especializado en inteligencia extranjera.

Las funciones de estos servicios están estrictamente separadas de las facultades de las policías y otras agencias de cumplimiento de la ley, para evitar la acumulación de poderes como ocurrió con la Gestapo de la Alemania Nazi.[23] Estas están reguladas por las leyes específicas de dichos organismos: la Ley de la Oficina Federal para la Protección de la Constitución (BVerfSchG),[24] la Ley del Servicio de Contrainteligencia Militar (MADG)[25] y la Ley del Servicio Federal de Inteligencia (BNDG):[26]

Organismo	**Funciones**[27]
BfV (art. 3(1) BVerfSchG).	• Protección de los organismos constitucionales de la Federación y los Estados federales mediante la recopilación y análisis de la información, especialmente de la relacionada a personas involucradas en: 1. Esfuerzos dirigidos contra el orden básico libre y democrático, la existencia o la seguridad de la Federación o de uno de sus Estados o destinados a obstaculizar ilícitamente los órganos constitucionales de la Federación o uno de sus Estados o sus miembros en el desempeño de sus funciones. 2. Actividades que amenacen las actividades de seguridad o de inteligencia llevadas a cabo en nombre de un poder extranjero. 3. Esfuerzos que ponen en peligro las preocupaciones en el extranjero de Alemania mediante el uso o la preparación de la violencia. 4. Esfuerzos dirigidos contra la idea de entendimiento internacional, especialmente contra la coexistencia pacífica de los pueblos.

23 Gesley, Jenny (2016a). Foreign Intelligence Gathering Laws: Germany. Disponible en: <https://www.loc.gov/law/help/intelligence-activities/germany.php>

24 Texto disponible en: <https://www.gesetze-im-internet.de/bverfschg/>

25 Texto disponible en: <http://www.gesetze-im-internet.de/madg/index.html>

26 Texto disponible en: <http://www.gesetze-im-internet.de/bndg/BJNR029790990.html>

27 Deutscher Bundestag (2010). German Laws governing Parliamentary Control of Intelligence Activities. Disponible en: <http://www.ennir.be/sites/default/files/pictures/GermanLawsgoverningParliamentaryControlofIntelligenceActivities.pdf>

MAD (art. 1(1) MADG)	• Recopilación y análisis de información, específicamente de datos personales y pertinentes, inteligencia y documentos relativos a (i) esfuerzos dirigidos contra el orden libre y democrático, la existencia o seguridad del gobierno federal o uno de los estados federales, o (ii) actividades dentro del ámbito de este acto que supongan una amenaza para la seguridad nacional o actividades de espionaje en nombre de una potencia extranjera, siempre que estas actividades o esfuerzos estén dirigidos al personal, agencias o instalaciones bajo responsabilidad del Ministerio Federal de Defensa y se lleven a cabo por personas que son miembros o empleados del ministerio y sus agencias o que son sospechosas de tales acciones.
BND (arts. 1(2), 2(1) BNDG)	• Recopilación y análisis de la información requerida para obtener información de inteligencia extranjera, que sea importante para la política exterior y de seguridad de Alemania. • Recopilación, procesamiento y uso de la información requerida, en la medida en que esto no entre en conflicto con la Ley Federal de Protección de Datos, para: 1. Protección de los miembros de su personal, instalaciones, objetos y fuentes contra actividades sensibles o de inteligencia. 2. Control de seguridad de las personas que trabajan o van a trabajar para ello. 3. Verificación de la información obtenida, que sea necesaria para la realización de sus funciones. 4. Sobre eventos en el extranjero que sean importantes para la política exterior y de seguridad de Alemania, si tal información puede obtenerse solo de esta manera y ninguna otra autoridad es responsable de su recopilación.

La Ley Fundamental de Alemania[28] consagra en su artículo 10 la inviolabilidad del secreto epistolar, postal y de telecomunicaciones, garantía fundamental que solo puede ser restringida en virtud de una ley, como la Ley del Artículo 10.Todos los organismos públicos (y privados) están obligados a cumplir con las reglas de la Ley Federal de Protección de Datos (*Bundesdatenschutzgesetz*, BDSG),[29] cuya última versión fue promulgada en 2017, para cumplir con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. De este modo, su artículo 47 establece que el tratamiento de los datos personales en general debe ser:

28 Texto disponible en: <https://www.btg-bestellservice.de/pdf/80206000.pdf>

29 Texto disponible en: <https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf>

(i) legal y justo;

(ii) recogido por propósitos específicos, explícitos y legítimos, y que no sea tratado de una forma que sea incompatible con esos propósitos;

(iii) adecuado, relevante y no excesivo en relación con dichos propósitos;

(iv) exacto y, cuando sea necesario, actualizado, y deben tomarse los pasos necesarios para que si esos datos no sean exactos se borren sin retraso;

(v) conservado en una forma que permita la identificación de los interesados por un período no superior al necesario para sus fines;

(vi) sean tratados de una forma que asegure la necesidad apropiada a los datos personales.

2.1.4. Australia

Las organizaciones de inteligencia del país son la Organización Australiana de Inteligencia de Seguridad (*Australian Security Intelligence Organization*, ASIO), encargada principalmente de la inteligencia doméstica; el Servicio Australiano de Inteligencia Secreta (*Australian Secret Intelligence Service*, ASIS), encargado de la inteligencia extranjera; y la Dirección Australiana de Señales (*Australian Signals Directorate*, ASD), dedicada a la inteligencia de señales.

Las funciones de las tres organizaciones están reguladas por la **Ley de la Organización Australiana de Inteligencia de Seguridad** de 1979 (*Australian Security Intelligence Organisation Act*, ley ASIO)[30] y la **Ley de Servicios de Inteligencia** de 2001 (*Intelligence Services Act*, ISA)[31]:

Organismo	**Funciones**[32]
ASIO (art. 17(1) ley ASIO)	• Obtener, correlacionar y evaluar inteligencia relevante para la seguridad. • Comunicar información para fines relacionados con la seguridad, de la manera que sea apropiada para esos fines. • Asesorar a los ministros y autoridades del Commonwealth con respecto a cuestiones relacionadas con la seguridad. • Proporcionar evaluaciones de seguridad a un Estado o a una autoridad de un Estado. • Obtener inteligencia extranjera dentro de Australia en conformidad con la ley. • Cooperar con agencias de inteligencia y policías.

30 Texto disponible en: <https://www.legislation.gov.au/Details/C2018C00174>

31 Texto disponible en: <https://www.legislation.gov.au/Details/C2018C00160>

32 Datos obtenidos de una traducción en inglés no oficial de extractos de las leyes acá presentadas, disponible en: <http://www.ennir.be/sites/default/files/pictures/GermanLawsgoverningParliamentaryControlofIntelligenceActivities.pdf>

ASIS (art. 6(1) ISA)	• Obtener, de conformidad con los requisitos del Gobierno, información sobre las capacidades, intenciones o actividades de personas u organizaciones fuera de Australia. • Comunicar, de conformidad con los requisitos del Gobierno, dicha inteligencia. • Proporcionar asistencia a la Fuerza de Defensa en apoyo de operaciones militares y cooperar con la Fuerza de Defensa en cuestiones de inteligencia. • Realizar actividades de contrainteligencia. • Servir de enlace con los servicios de inteligencia o seguridad u otras autoridades de otros países. • Cooperar con agencias de inteligencia y policías. • Emprender actividades fuera de Australia según establece la ley.
ASD (art. 7 ISA)	• Obtener información sobre las capacidades, intenciones o actividades de personas u organizaciones fuera de Australia en forma de energía electromagnética, ya sea guiada o no, o ambas, o en forma de energía eléctrica, magnética o acústica. • Comunicar, de conformidad con los requisitos del Gobierno, dicha inteligencia. • Proporcionar material, asesoramiento y otra asistencia a las autoridades de la Commonwealth y estatales sobre asuntos relacionados con la seguridad y la integridad de la información que se procesa, almacena o comunica por medios electrónicos o similares. • Proporcionar asistencia a la Fuerza de Defensa en apoyo de operaciones militares y cooperar con la Fuerza de Defensa en cuestiones de inteligencia. • Proporcionar asistencia a las autoridades estatales y estatales en relación con: 1. Criptografía y tecnologías de comunicación e informática. 2. Otras tecnologías especializadas adquiridas en relación con el desempeño de sus otras funciones. 3. El desempeño de esas autoridades de las funciones de búsqueda y rescate. • Cooperar con agencias de inteligencia y policías.

Las leyes antes señaladas están siendo objeto de una revisión que culminará con la proposición de un nuevo marco normativo para la inteligencia australiana.[33]

---

33 Westcott, Ben (2018). Australia's intelligence laws face most significant review in 40 years. CNN. Disponible en: <https://edition.cnn.com/2018/05/31/asia/australia-intelligence-review-china-intl/index.html>

La **Ley de Privacidad** de 1988 (*Privacy Act*, PA)[34] regula el tratamiento de datos personales realizado por organismos públicos y privados.

2.1.5. Nueva Zelanda

Las organizaciones de inteligencia del país son el Servicio de Inteligencia de Seguridad (*New Zealand Security Intelligence Service*, NZSIS), encargado de la inteligencia (y contrainteligencia) doméstica y extranjera; el Buró de Seguridad de las Comunicaciones Gubernamentales (*Government Communications Security Bureau*, GCSB), dedicado a la inteligencia de señales; y el Buró de Evaluaciones Nacionales (*National Assessments Bureau*, NAB), responsable de la evaluación de información extranjera.

Tanto el NZSIS como el GCSB, que son las instituciones que realizan recolección de inteligencia, están gobernadas por la **Ley de Inteligencia y Seguridad** de 2017 (*Intelligence and Security Act*, ISA),[35] que reemplazó a los cuatro cuerpos legales que hasta entonces regulaban la inteligencia neozelandesa: *New Zealand Security Intelligence Service Act* (1969), *Government Communications Security Bureau Act* (2003), *Intelligence and Security Committee Act* (1996) y la *Inspector-General of Intelligence and Security Act* (1996).[36]

De acuerdo con ISA, los objetivos de las agencias de inteligencia son la protección de: (i) la seguridad nacional de Nueva Zelanda; (ii) las relaciones y el bienestar internacional de Nueva Zelanda; y (iii) el bienestar económico de Nueva Zelanda (art. 9). Sus funciones son:

(i) Recolección y análisis de inteligencia (art. 10).

(ii) Servicios, asesoría y asistencia de protección de la seguridad (art. 11).

(iii) Actividades de aseguramiento de la información y ciberseguridad (art. 12).

(iv) Cooperación con otras autoridades públicas (policías y defensa) para facilitar sus funciones (art. 13).

(v) Cooperación con otras entidades para responder a una amenaza inminente (art. 14).

La Ley de Privacidad de 1993 (*Privacy Act*, PA)[37] establece principios con respecto a la recopilación, uso y divulgación, por parte de las agencias del sector público y privado, de datos personales, y el acceso de cada persona a la información que dichas agencias tienen.

---

34 Texto disponible en: <https://www.legislation.gov.au/Details/C2018C00034>

35 Texto disponible en: <http://www.legislation.govt.nz/act/public/2017/0010/latest/DLM6920823.html>

36 DPMC. Intelligence and Security Act 2017. Disponible en: <https://www.dpmc.govt.nz/our-programmes/national-security-and-intelligence/intelligence-and-security-act-2017>

37 Texto disponible en: <http://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html>

2.2. Interceptación de comunicaciones

2.2.1. Reino Unido

RIPA unificó la regulación de la intercepción de las comunicaciones y del tratamiento de los datos de dichas comunicaciones. La ley demostró ser funcional a las autoridades de Reino Unido, pues fue invocada en la realización de más de 20.000 interceptaciones durante su primera década de vigencia.[38]

A pesar de su extensivo uso, dicho marco jurídico comenzó a ser verdaderamente cuestionado solamente a partir de las revelaciones de Edward Snowden en 2013. Por ello se constituyó un panel llamado *Independent Surveillance Review* (ISR), que en 2015 emitió un informe donde se concluye que la normativa británica de vigilancia era poco clara y debía ser reemplazada por una norma comprensiva.[39]

En 2016 IPA introdujo una nueva regulación de interceptación. Sin embargo, y muy por el contrario de lo que de varias organizaciones no gubernamentales y expertos esperaban de la nueva ley, la IPA tuvo como principal efecto expandir los poderes de vigilancia electrónica de la policía y los organismos de inteligencia.[40] El mismo Snowden la calificó como "[la ley] de vigilancia más extrema en la historia de la democracia occidental. Va más lejos que muchas autocracias".[41] Ello quedó en evidencia cuando, en abril de 2018, la Corte Suprema falló que IPA vulneraba la regulación europea, otorgando al gobierno de Theresa May un plazo de seis meses para realizar los cambios pertinentes a la ley.[42]

Tanto RIPA (parte I, cap. I) como IPA (partes 1 y 2) configuran el marco jurídico para la interceptación de comunicaciones. Según ambas leyes, interceptación puede definirse como la realización de un acto relevante –ya sea la modificación o interferencia de un sistema o su operación, el monitoreo por medios del sistema o por comunicación inalámbrica desde o hacia un aparato del sistema– que tenga el efecto de hacer disponible cualquiera de los contenidos de esa comunicación, mientras son transmitidos en un tiempo relevante, a una persona distinta al emisor o a quien están supuestamente destinados.[43]

---

38 Justice (2011). Freedom from Suspicion Surveillance Reform for a Digital Age. Disponible en: <http://www.statewatch.org/news/2011/nov/uk-ripa-justice-freedom-from-suspicion.pdf>

39 RUSI (2015). A Democratic Licence to Operate. Disponible en: <https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf>

40 Griffin, Andrew (2016). Investigatory Powers Act goes into force, putting UK citizens under intense new spying regime. The Independent. Disponible en: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html>

41 Disponible en: <https://twitter.com/snowden/status/799371508808302596>

42 Cobain, Ian (2018). UK has six months to rewrite snooper's charter, high court rules. Disponible en: <https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules>

43 Cf. art. 2(2) RIPA, art. 4(1)(2) IPA. Cabe señalar que por "tiempo relevante" se entiende (i) mientras la comunicación sea transmitida, (ii) cuando la comunicación sea almacenada (art. 4(4) IPA).

Interceptación ilegal. Será considerada delito la intercepción de comunicaciones realizada, dentro del Reino Unido y de manera intencional, durante su transmisión mediante un sistema público o privado de telecomunicaciones o un servicio postal público, por una persona que no tenga la autoridad legal para realizarla.[44]

Se exime de responsabilidad penal a la interceptación de comunicaciones transmitidas por un sistema de telecomunicaciones privado si la persona tiene derecho a controlar la operación o uso del sistema o lo realiza con el consentimiento de esta.[45]

Interceptación legal. La autoridad legal para realizar interceptaciones está dada por:[46]

Causal	**Tipos**	
Órdenes de interceptación	i)	Interceptación dirigida (*targeted interception warrant*).
	ii)	Asistencia mutua (*mutual assistance warrant*).
	iii)	Interceptación masiva (*bulk interception warrant*).
Autorización o facultad otorgada por ley (pt. I cap. II IPA)	i)	Consentimiento del emisor o del receptor (art. 44).
	ii)	Motivos administrativos o de cumplimiento de la ley (art. 45-48).
	iii)	Realizadas por ciertas instituciones especiales, como prisiones, hospitales psiquiátricos o unidades de detención de inmigrantes (art. 49-51).
	iv)	Solicitudes por autoridades de país extranjero (art. 52).
Casos de comunicación almacenada	i)	Orden de interferencia de equipos focalizada (*targeted equipment interference warrant*).
	ii)	Poder estatutario que se ejecuta por el propósito de obtener información o de obtener un documento ajeno.
	iii)	Orden judicial.

Las órdenes de interceptación pueden ser de examinación dirigida o de asistencia mutua (art. 15(1) IPA). En la pt. 1 cap. 1 IPA se regulan las causales para emitir dichas órdenes y la aprobación por Comisionado Judicial.

Las **órdenes de interceptación dirigida** autorizan u obligan a realizar: (i) intercepción postal o de telecomunicaciones; (ii) obtención de datos secundarios por dichos medios; (iii) divulgación de lo obtenido a la persona a la cual la orden está dirigida o a su representante (art. 15(2) IPA).

---

44 Cf. art. 1(1)(1A)(2) RIPA, art. 3(1) IPA.

45 Cf. art. 1(6) RIPA, 3(2) IPA.

46 Cf. art. 1(5) RIPA, 6(1) IPA.

Las órdenes de examinación dirigida autorizan a realizar la sección de contenidos relevantes para su examinación que infrinjan la prohibición de buscar o identificar comunicaciones de individuos dentro de las Islas Británicas (art. 15(3) IPA).

Las **órdenes de asistencia mutua** autorizan u obligan a realizar: (i) solicitud de una interceptación de comunicaciones en virtud de un instrumento de la EU o acuerdo internacional de asistencia mutua; (ii) autorización de una intercepción de comunicaciones realizada por autoridades extranjeras en virtud de esos instrumentos o acuerdos; (iii) divulgación de lo obtenido a la persona a la cual la orden está dirigida o a su representante (art. 15(4) IPA).

Dichas órdenes pueden ser requeridas por una "autoridad interceptora",[47] y deben ser emitidas por el ministro del Interior (art. 19), previa autorización del Comisionado Judicial (art. 23), salvo que se trate de casos urgentes, donde la revisión es posterior (art. 24). Ambas autoridades deben velar por que se cumplan los requisitos de necesidad y proporcionalidad. La necesidad debe seguir los motivos de (a) interés de seguridad nacional; (b) prevenir o detectar crímenes serios; (c) salvaguardar el bienestar económico de UK; (d) dar efecto a instrumentos o acuerdos de asistencia mutua en situaciones similares a la de prevenir o detectar crímenes serios. Además, el ministerio deberá verificar si se realizaron los arreglos satisfactorios (salvaguardias).

Luego, las **órdenes de interceptación masiva** son reguladas por la parte 6 capítulo 1. Su propósito principal es la intercepción de comunicaciones internacionales (emitida o recibida por persona fuera del país) o los datos secundarios de estas. Autorizan a realizar alguna de las siguientes actividades: (i) interceptación de comunicaciones en el curso de su transmisión en un sistema de telecomunicaciones; (ii) obtención de datos secundarios transmitidos por esos medios; (iii) selección de examinación de los contenidos interceptados u obtenidos; (iv) divulgación de lo obtenido a la persona a la cual la orden está dirigida o a su representante (art. 136).

El ministro de Estado puede emitir estas órdenes siguiendo el requisito de necesidad por: (i) interés de la seguridad nacional; o sobre la base de: (ii) prevención de crímenes serios; (iii) interés económico de UK, siempre que sea relevante para los intereses de la seguridad nacional (art. 138); y debe ser aprobada por comisionado judicial (art. 140).

Una de estas formas de intercepción masiva es el uso de *IMSI-catchers*,[48] también llamados *stingrays* ("mantarrayas"). En 2016 se reveló que la policía británica estaba utilizando este tipo de tecnología en Londres y otras siete ciudades, con el objetivo de investigar delitos de alta complejidad.[49]

---

47 Autoridades interceptoras (art. 18): (i) jefe de un servicio de inteligencia (MI5, MI6 o GCHQ); (ii) director general de la National Crime Agency; (iii) comisionado de la Policía de la Metrópolis (Londres); (iv) jefes de las policías de Irlanda del Norte y Escocia; (v) comisionado del HM Revenue and Customs (impuestos); (vi) jefe de la Inteligencia de Defensa; (vii) autoridades extranjeras autorizadas por asistencia mutua.

48 IMSI es el acrónimo para International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil). Es un código único incorporado a las tarjetas SIM de los teléfonos móviles, que permiten la geolocalización de los dispositivos.

49 Pegg, David; Evans, Rod (2016). Controversial snooping technology 'used by at least seven police forces'. The Guardian. Disponible en: <https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces>

La parte 3 RIPA regula las causales y el procedimiento para obtener la **revelación de datos electrónicos cifrados** o "descifrado forzoso".[50] El artículo 49(2) establece los requisitos para que cualquier persona con el permiso apropiado pueda imponer un requerimiento de revelación (*disclosure requirement*) a una persona que tenga la clave para acceder a la información protegida. Estos son:

(i) La llave para acceder a la información está en poder de una persona.

(ii) Es necesaria la imposición de un requerimiento de revelación:

   a. por los motivos razonables de interés nacional, prevenir o detectar crimen o interés del bienestar económico de UK, o

   b. para el propósito de asegurar el ejercicio efectivo o el rendimiento adecuado de poder o deber estatutario por cualquier autoridad.

(iii) Proporcionalidad.

(iv) La obtención de la información protegida en una forma inteligible no es razonablemente practicable sin este procedimiento.

La persona que sea requerida para revelar datos cifrados que no cumpla con ello (art. 53), o que no cumpla con la confidencialidad de la medida en ciertos casos (art. 54), puede ser penalmente responsable.

La solicitud de descifrado ha sido utilizada en varias oportunidades por las autoridades británicas, la primera de ellas a activistas por los derechos animales en 2007.[51] Los primeros detenidos por negarse a otorgar las claves de descifrado fueron una persona que padecía de esquizofrenia, acusada del porte de un explosivo RDX en 2009,[52] y un joven de 19 años, en medio de una investigación por imágenes de pedofilia.[53] Se ha criticado que los requisitos que establece la ley son excesivamente amplios y que la aplicación de la norma por parte de la policía ha sido generalmente desproporcionada en razón del crimen que se investiga.[54]

El 23 de febrero de 2017, el Ministerio del Interior inició una consulta pública sobre los cinco proyectos de códigos de prácticas que tiene previsto publicar en virtud de IPA (sobre interceptación de comunicaciones, interferencia de equipos, adquisición de datos de comunicaciones a granel, retención y uso de datos personales masivos) que establecerán los procesos y salvaguardas que regirán las facultades de investigación por parte de las autoridades públicas. Ofrecerán detalles sobre cómo deberán ejercerse las competencias pertinentes,

---

50 Feikert-Ahalt, Clare (2016b). Government Access to Encrypted Communications: United Kingdom. Disponible en: <https://www.loc.gov/law/help/encrypted-communications/united-kingdom.php>

51 Ward, Mark (2007). Campaigners hit by decryption law. BBC. Disponible en: <http://news.bbc.co.uk/2/hi/technology/7102180.stm>

52 Williams, Christopher (2009). UK jails schizophrenic for refusal to decrypt files. The Register. Disponible en: <http://www.theregister.co.uk/2009/11/24/ripa_jfl/>

53 Oates, John (2010). Youth jailed for not handing over encryption password. The Register. Disponible en: <https://www.theregister.co.uk/2010/10/06/jail_password_ripa/>

54 Cox, Joseph (2014). How Refusing to Hand Over Your Passwords Can Land You in Jail. Motherboard. Disponible en: <https://motherboard.vice.com/en_us/article/wnjgdq/how-refusing-to-hand-over-your-passwords-can-land-you-in-jail>

incluidos ejemplos de mejores prácticas. Están destinados a proporcionar claridad adicional y garantizar los más altos estándares de profesionalismo y cumplimiento de la legislación pertinente. Tras el cierre de la consulta el 6 de abril de 2017, los proyectos de códigos se enmendaron ulteriormente y los reglamentos que los pondrán en vigor se presentarán y debatirán en el Parlamento. Solo entrarán en vigor cuando se hayan debatido en ambas cámaras del Parlamento y hayan sido aprobadas mediante una resolución en ambas cámaras.[55]

2.2.2. Estados Unidos

La interceptación de telecomunicaciones está regulada fundamentalmente en dos leyes: FISA, para la vigilancia extranjera, y la **Ley de Privacidad de las Comunicaciones Electrónicas** (Electronic Communications Privacy Act, ECPA), para la vigilancia interna.

FISA regula la vigilancia electrónica en su subcapítulo 1 (arts. 1801-1813). En su art. 1801(f) define vigilancia electrónica como:

(i) Adquisición mediante un dispositivo electrónico, mecánico u otro dispositivo de vigilancia del contenido de cualquier comunicación:

1. Cable o radio: enviada por o destinada a ser recibida por una persona particular, conocida en EEUU que se encuentre en ese país, si los contenidos son adquiridos para dirigirse intencionalmente contra esa persona, en circunstancias en las que dicha persona tiene una expectativa razonable de privacidad y se requerirá una orden para fines policiales.
2. Cable: enviada o recibida por una persona en EEUU, sin el consentimiento de cualquiera de las partes, si tal adquisición ocurre en ese país, pero no incluye la adquisición de aquellas comunicaciones de intrusos informáticos.
3. Radio: realizada intencionalmente, en circunstancias en las cuales una persona tiene una expectativa razonable de privacidad y se requeriría una orden para fines policiales, y si tanto el remitente como todos los posibles destinatarios se encuentran dentro de EEUU.

(ii) Instalación o uso de un dispositivo electrónico, mecánico u otro dispositivo de vigilancia en EEUU para supervisar la adquisición de información, que no sea por cable o radio, en circunstancias en que una persona tiene una expectativa razonable de privacidad y se requeriría una orden judicial para fines policiales.

Interceptación sin orden judicial. Establece la facultad del presidente, a través del fiscal general, de obtener información de inteligencia extranjera sin una orden judicial, siempre que:

(i) La vigilancia esté únicamente dirigida a: (a) la adquisición de contenidos de las comunicaciones transmitidas entre gobiernos extranjeros, o (b) la adquisición de inteligencia técnica bajo el control abierto y exclusivo de un gobierno extranjero.

---

55 Sentencia de la Corte Europea de Derechos Humanos , Caso "Big Brother Watch and others v. United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15), 13 de septiembre de 2018, párrafo 201.

(ii) No haya una probabilidad sustancial de que la vigilancia adquiera el contenido de las comunicaciones en las que se involucre una persona de los Estados Unidos.

(iii) El procedimiento cumpla con las reglas de minimización.

El fiscal general debe certificar el cumplimiento de esas condiciones ante las comisiones de inteligencia de la Cámara y el Senado y enviar una certificación al Tribunal de Vigilancia de la Inteligencia Extranjera (*Foreign Intelligence Surveillance Court*, FISC) (art. 1802).

Excepcionalmente, el fiscal general podrá autorizar órdenes de vigilancia electrónica sin órdenes judiciales por un periodo de 15 días tras una declaración de guerra (art. 1811).

Interceptación con orden judicial. Las demás actividades de vigilancia electrónica deberán someterse a la autorización judicial. El juez emitirá una orden *ex parte* si:

(i) La solicitud del agente federal fue aprobada por el fiscal (cf. art. 1804).

(ii) Hay una causa probable para creer que: (a) el objetivo de la vigilancia es un gobierno o agente extranjero y (b) está dirigida a instalaciones o lugares utilizados por ese gobierno o agente extranjero.

(iii) Cumple con los procedimientos de minimización.

(iv) Contiene las declaraciones y certificaciones necesarias.

Sin embargo, también otorga la facultad de realizar vigilancia electrónica en casos de emergencia o cuando una persona no estadounidense realiza una amenaza de muerte o serio daño corporal a cualquier persona (art. 1805).

Resguardos. Establece una "moción para suprimir" evidencias en juicios por personas que hayan sido afectadas por la vigilancia electrónica en dos causales: (i) información adquirida ilegalmente; (ii) vigilancia no fue hecha en conformidad a una orden de autorización o aprobación (art. 1806).

Consagra la obligación al fiscal general de generar un reporte anual con la cantidad de aplicaciones y órdenes de vigilancia electrónica y de individuos vigilados (art. 1807).

Interceptación dirigida en el extranjero. El art. 1881a (conocido como la "sección 702 FISA") –introducida por la *FISA Amendments Act* de 2008 (FAA)– establece procedimientos para realizar interceptación de comunicaciones (como correos electrónicos o llamadas telefónicas) dirigida a ciertas personas fuera de los Estados Unidos que no sean estadounidenses. Según el Comité Permanente de Inteligencia de la Cámara de Representantes, esta norma se justificaría fundamentalmente en que ha sido una de las principales facultades legales que ha permitido identificar y eliminar a objetivos ligados al terrorismo, como Hajji Imam, líder de Dáesh.[56]

Sin embargo, la sección 702 ha sido la base para que la NSA desarrolle el programa de vigilancia PRISM, que ha realizado una interceptación masiva de comunicaciones, incluyendo las de ciudadanos estadounidenses (sin tener la autorización para realizar ambas

---

56 HPSCI Majority. FISA Section 702 Debate. Disponible en: <https://intelligence.house.gov/uploadedfiles/2017_section_702_fact_sheet.pdf>

cosas), realizadas mediante nueve proveedores estadounidenses: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube y Apple.[57]

ECPA en su Título I (arts. 2510-2522 del título 18 U.S.C.) complementa la **Ley de Escuchas** o *Wiretap Act*,[58] para regular la interceptación de comunicaciones orales, por cable y electrónicas. Sus normas se aplican al correo electrónico, las conversaciones telefónicas y los datos almacenados electrónicamente.[59]

Define comunicación electrónica como cualquier transferencia de signos, señales, escritura, imágenes, sonidos, datos o inteligencia de cualquier naturaleza, transmitida, en todo o en parte, por un sistema de cable, radio, electromagnético, fotoelectrónico o fotoóptico que afecte el comercio interestatal o extranjero (art. 2510(12)).

Interceptación ilegal. El art. 2511 prohíbe en general la interceptación intencional, intento de interceptar o procurar que otra persona intercepte o intente interceptar dichas comunicaciones, y la divulgación y uso del contenido obtenido mediante una interceptación prohibida.

También prohíbe el uso de dispositivos para interceptar comunicaciones orales en determinadas condiciones.[60] Así mismo, prohíbe la divulgación intencional o intentada del contenido de comunicaciones por cable, oral o electrónica que, habiendo sido interceptada por medios autorizados por la ley, está relacionada a una investigación criminal, y se obtuvo con la intención de obstruir, impedir o interferir indebidamente con dicha investigación.

Interceptación autorizada. El art. 2516 establece que el FBI o las agencias federales o estatales que tengan responsabilidad en la investigación de delitos, con la autorización del fiscal general o estatal, podrán solicitar la interceptación de comunicaciones a un juez competente, para obtener evidencia para la investigación de alguno de los delitos enumerados en una lista de delitos taxativa pero prácticamente omnicomprensiva.

También permite a los oficiales de cumplimiento de la ley el uso y divulgación a otro oficial del contenido de dichas interceptaciones en la medida en que sea apropiado para el desempeño apropiado de sus deberes (art. 2517(1-2)). También puede divulgar dichos contenidos a cualquier otro oficial federal de seguridad, inteligencia, protección,

---

57 Gellman, Barton y Poitras, Laura (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post. Disponible en: <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>

58 Texto disponible en: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119>

59 Justice information Sharing (2013). Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22. Disponible en: <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>

60 El art. 2511(1)(b) establece que se prohíbe el uso intencional o intentado, o el encargo a otra persona de usar o intente usar un dispositivo electrónico, mecánico u otro para interceptar cualquier comunicación oral si: (i) dicho dispositivo está fijado o transmite una señal a través de un cable u otra conexión similar utilizada en la comunicación por cable; o (ii) dicho dispositivo transmite comunicaciones por radio o interfiere con la transmisión de dicha comunicación; o (iii) dicha persona sepa, o tenga motivos para saber, que dicho dispositivo o cualquier componente del mismo ha sido enviado por correo o transportado en comercio interestatal o extranjero; o (iv) dicho uso o intento de uso tenga lugar en las instalaciones de cualquier empresa u otro establecimiento comercial cuyas operaciones afecten el comercio interestatal o extranjero; u obtenga o busque obtener información relacionada con las operaciones de cualquier negocio u otro establecimiento comercial cuyas operaciones afecten el comercio interestatal o extranjero; o (v) dicha persona actúa en el Distrito de Columbia, el Estado Libre Asociado de Puerto Rico o cualquier territorio o posesión de los Estados Unidos.

inmigración, defensa nacional o seguridad nacional, a un agente de cumplimiento de la ley extranjero o a un funcionario de gobierno en casos específicos (art. 2517(6-8)).

El juez también podrá emitir una orden *ex parte* si (art. 2518(3)):

(i) Hay una causa probable para creer que un individuo está cometiendo, ha cometido o está a punto de cometer un delito particular enumerado en el art. 2516.

(ii) Existe una causa probable para creer que las comunicaciones particulares concernientes a dicho delito se obtendrán a través de dicha intercepción.

(iii) Se han intentado procedimientos de investigación normales y han fracasado, o parece ser poco probable que tengan éxito si se intenta o es demasiado peligroso.

(iv) Existe una causa probable para creer que el lugar de las instalaciones donde se hace o intercepta la comunicación es utilizado para la comisión de tal ofensa, o son comúnmente utilizados por la persona que comete el delito.

Resguardos. Los jueces que hayan emitido órdenes *ex parte* o los fiscales federales o estatales que hayan autorizado intercepciones deberán generar un informe anual sobre dichas acciones (art. 2519). Los afectados por las interceptaciones ilegales podrán accionar civilmente (art. 2520).

Además, la **Ley de Asistencia en las Telecomunicaciones para el Cumplimiento de la Ley** (*Communications Assistance for Law Enforcement Act*, CALEA)[61], contenida en los art. 1001-1010 del título 47 U.S.C., impone obligaciones a las compañías operadoras de telecomunicaciones con respecto a la interceptación de las comunicaciones de sus suscriptores.

De acuerdo con el art. 1002, los ISP tienen el deber de asegurarse que sus equipos, instalaciones y servicios permiten:

(i) Interceptar comunicaciones y acceder a información de llamadas requeridas por orden judicial u otra autorización legal.

(ii) Entregar dichas interceptaciones e informaciones al gobierno.

(iii) Facilitar dichas interceptaciones con un mínimo de interferencia a los suscriptores, protegiendo la privacidad y seguridad de las telecomunicaciones para las que no se ha autorizado intercepción, y protegiendo la información sobre la intercepción del gobierno.

El art. 1004 establece el deber de las operadoras de asegurarse que las interceptaciones realizadas en sus dependencias están autorizadas por orden judicial o por ley.

También obliga a las empresas de manufactura de equipos y de servicios de soporte de telecomunicaciones a recibir las consultas y colaborar, respectivamente, con el cumplimiento de dichas interceptaciones (art. 1005).

El fiscal general deberá realizar un reporte anual de los montos pagados a las operadoras por las interceptaciones realizadas, y el inspector general del Departamento de Justicia

---

61 Texto disponible en: <https://www.law.cornell.edu/uscode/text/47/chapter-9/subchapter-I>

deberá realizar un reporte anual sobre los equipos, instalaciones y servicios utilizados en las interceptaciones y la efectividad de estas (art. 1010).

En la legislación federal de Estados Unidos no existen normas referidas al descifrado de las comunicaciones, por lo que esta materia ha sido entregada a la jurisprudencia. A pesar de que existen casos en que se ha invocado la Quinta Enmienda a la Constitución (derecho a la no autoincriminación), eventualmente el gobierno podría solicitar el descifrado mediante la doctrina de la conclusión previsible (*foregone conclusion*), donde se argumenta que existe el conocimiento de que la computadora cifrada tiene una versión no cifrada a la cual se requiere acceso.[62]

2.2.3. Alemania

La interceptación de las telecomunicaciones está regulada por dos legislaciones: la Ley del Art. 10, que está dirigida a los organismos de inteligencia (BfV, MAD y BND), y el Código de Procedimiento Penal, que está dirigido a las policías.[63]

La Ley del Artículo 10 autoriza a los organismos de inteligencia a realizar medidas que restringen el secreto epistolar y de las telecomunicaciones.

Interceptación autorizada. La ley autoriza a monitorear y registrar las telecomunicaciones por motivos de: (i) daño inminente al orden básico libre y democrático o a la existencia o seguridad de la federación y sus estados o (ii) por funciones del BND establecidas en su ley orgánica (art. 1).

Para acogerse a la primera causal debe haber indicaciones concretas que den lugar a la sospecha de que una persona: (i) está planeando, cometiendo o ha cometido alguno de los delitos enumerados en el art. 3(1);[64] (ii) es miembro de una organización cuyo propósito o actividades están enfocadas en cometer delitos contra el orden básico libre y democrático o a la existencia o seguridad de la federación y sus estados.

Dichas medidas no serán permitidas cuando las indicaciones concretas justifiquen la suposición de que, como resultado de estas, solo se adquirirá información sobre el área central de la esfera privada (art. 3a).

Procedimiento. Las interceptaciones deberán ser solicitadas por el oficial competente de cada agencia (art. 9) y serán expedidas por la autoridad superior de cada Estado o en un ministro federal designado por el canciller (art. 10).

Las medidas realizadas por autoridades federales serán supervisadas por el Panel de Control Parlamentario y por una comisión especial ("Comisión G10") (art. 1), mientras que, en el caso de las autoridades federales, estas son supervisadas por el parlamento federal correspondiente (art. 16).

---

62 Terzian, Dan (2015). Forced Decryption as a Foregone Conclusion. California Law Review Circuit, vol. 6. Disponible en: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1069&context=clrcircuit>

63 Gesley, Jenny (2016a). Op. cit.

64 Entre los delitos enumerados están: crímenes contra la paz o alta traición, crímenes contra el estado democrático de derecho, traición que ponga en peligro la seguridad exterior, crímenes contra la defensa nacional, contra la seguridad de las tropas de la OTAN en territorio alemán.

La agencia que recopila los datos verificará en intervalos de no más de seis meses si los datos personales recopilados son, por sí mismos o en conjunto con otros datos, necesarios en relación con sus funciones. Si no lo son, deberán ser borrados bajo la supervisión de un funcionario calificado para ocupar un cargo judicial (art. 4).

Obligaciones a los proveedores de telecomunicaciones. La ley también obliga a los proveedores de telecomunicaciones a proporcionar a la agencia autorizada información detallada sobre las telecomunicaciones efectuadas después de que la orden entre en vigencia, enviar las comunicaciones para su transmisión utilizando instalaciones de telecomunicaciones y habilitar el monitoreo y registro de telecomunicaciones (art. 2).

Se prohíbe que quienes estén involucrados en proveer servicios de telecomunicaciones divulguen el hecho de que dichas comunicaciones están siendo monitoreadas (art. 17), conducta que es constitutiva de delito y tiene una pena de prisión efectiva de hasta 2 años o multa (art. 18).

El **Código de Procedimiento Penal** (StPO)[65] dedica su Capítulo VIII a la incautación, interceptación de telecomunicaciones, búsqueda asistida por computadora, uso de dispositivos técnicos, uso de investigadores de bajo contenido y búsqueda.

El art. 100a establece que las telecomunicaciones pueden ser interceptadas y grabadas, incluso sin el conocimiento de las personas afectadas, si:

(i) Ciertos factores dan lugar a la sospecha de que una persona ha cometido un delito serio, ya sea como autor, instigador o cómplice, o en casos donde se ha intentado la comisión de un delito que otorgue responsabilidad penal por dicho intento o lo ha preparado mediante la comisión de otro delito.

(ii) El delito es uno de particular gravedad en el caso individual; el mismo artículo establece una extensa lista con los delitos que tienen esta consideración.

(iii) Otros medios de establecer los hechos o determinar el paradero del acusado son mucho más difíciles o no ofrecen expectativas de éxito.

La orden para realizar dicha interceptación debe ser solicitada por el ministerio público y aprobada judicialmente dentro de un plazo de 3 días hábiles. Dicha orden estará limitada a no más de tres meses, siempre y cuando las condiciones por las que se solicitó se mantengan (art. 100b).

En los casos de interceptación de conversaciones privadas en lugares privados, a los requisitos del artículo 100a se agrega que, sobre la base de indicios concretos, se puede asumir que la vigilancia resultará en la grabación de declaraciones realizadas por el acusado que podrían ser de importancia para el establecimiento de los hechos o determinando su paradero, o el de un coacusado, y debe realizarse solo si los otros medios para lograr lo anterior fueran desproporcionadamente más difíciles (art. 100c). Como medida de transparencia, el gobierno federal deberá informar anualmente al Parlamento sobre las medidas tomadas en relación con el art. 100c (art. 100e).

---

65 Texto disponible en: <https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html>

El art. 100i también regula el uso de *IMSI-catchers* o mantarrayas, en las siguientes circunstancias:

(i) Casos en que ciertos hechos den lugar a la sospecha de que una persona ha cometido un delito de significancia sustancial, ya sea como autor, instigador o cómplice: (a) siendo uno de los del art. 100a o (b) en casos donde se ha intentado la comisión de un delito que otorgue responsabilidad penal por dicho intento o lo ha preparado mediante la comisión de otro delito.

(ii) Dicha técnica pueda ser usada para determinar: (i) la identificación del dispositivo de una terminal móvil o el número de la tarjeta que usa, así como (ii) la ubicación de la terminal móvil; ambos casos, cuando sea necesario para establecer los hechos o determinar el paradero del acusado.

En 2017 fue aprobada la **Ley para un diseño más eficaz y viable de los procedimientos penales** (*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*),[66] que modifica el StPO, otorgando facultades a las policías para realizar búsquedas en línea y la vigilancia de fuentes de telecomunicaciones mediante *malware* (acciones conocidas como "troyanos estatales").[67] Antes de esta nueva ley, este tipo de *malware* solo podía ser utilizado por la Oficina de la Policía Federal en casos de terrorismo.[68]

Tanto la Ley del Art. 10 como el StPO no hacen distinción en cuanto a las comunicaciones cifradas o no cifradas, por lo cual se ha entendido que las agencias de inteligencia y policiales pueden realizar el descifrado para los fines de interceptación. Sin embargo, hay debate sobre la facultad legal de dichas agencias de obligar a la persona que tiene la llave a que la entregue para descifrar la información, pues al igual que en los Estados Unidos, sería posible invocar el principio de no autoincriminación (*nemo tenetur*) derivado de la Ley Fundamental.[69]

2.2.4. Australia

La interceptación está regulada por la **Ley de Telecomunicaciones (Interceptación y Acceso) de 1979** (*Telecommunications (Interception and Access) Act*, ley TIA).[70]

Interceptación legal. El art. 7 establece como regla general la prohibición de la interceptación o de la autorización a otra persona para interceptar una comunicación transmitida por un sistema de telecomunicaciones, excepto si se realiza en una de estas circunstancias:

---

66 Texto disponible en: <https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3202.pdf>

67 Gesley, Jenny (2017). Germany: Expanded Telecommunications Surveillance and Online Search Powers. Disponible en: <http://www.loc.gov/law/foreign-news/article/germany-expanded-telecommunications-surveillance-and-online-search-powers/>

68 German government to use Trojan spyware to monitor citizens. Deutsche Welle. Disponible en <http://www.dw.com/en/german-government-to-use-trojan-spyware-to-monitor-citizens/a-19066629>

69 Gesley, Jenny (2016b). Government Access to Encrypted Communications: Germany. Disponible en: <https://www.loc.gov/law/help/encrypted-communications/germany.php>

70 Texto disponible en: <https://www.legislation.gov.au/Details/C2018C00201>

(i) Instalación, operación y mantenimiento de las telecomunicaciones realizadas por un empleado de un ISP en el ejercicio de sus funciones, o por un empleado de ASIO para la detección de un dispositivo de escucha.

(ii) Autorización por una orden (*warrant*).

(iii) Policía pueda rastrear la ubicación de las personas que llaman por emergencias relativas a la muerte o herida grave de una persona (art. 30).

(iv) Desarrollo y prueba de capacidades de intercepción autorizadas por el fiscal general (art. 31A).

Interceptación con orden del fiscal general. La interceptación de un servicio de telecomunicaciones realizada por la Organización Australiana de Inteligencia de Seguridad (ASIO) puede ser solicitada por el director general de Seguridad al fiscal general, quien deberá verificar que (i) el servicio de telecomunicaciones es usado o probablemente lo sea por una persona involucrada en actividades que atentan contra la seguridad para dichas actividades; (ii) la interceptación de las comunicaciones ayudará o probablemente ayudará a ASIO a llevar a cabo su función de obtener información de inteligencia relacionada con la seguridad (art. 9).

También pueden emitirse órdenes de interceptación con respecto a las comunicaciones de una persona en particular, en el caso que la orden de interceptación de un servicio de telecomunicaciones no sea efectiva (art. 9A).

Ambas órdenes de interceptación de un servicio de telecomunicaciones (incluso de uno extranjero), o con respecto a una persona, pueden emitirse con el propósito de recolectar inteligencia internacional (arts. 11A-11C), en interés de: (i) la seguridad nacional de Australia; (ii) las relaciones exteriores de Australia; o (iii) el bienestar económico de Australia.

En todos estos casos, el director general de Seguridad deberá reportar de los resultados de la interceptación al fiscal general dentro de un plazo de 3 meses desde que se realizó (art. 17).

Interceptación con orden judicial. Todas las demás agencias autorizadas por ley para realizar interceptaciones de servicio de telecomunicaciones o respecto de una persona deberán solicitarlo a un juez elegible o al miembro nominado del Tribunal Administrativo de Apelaciones (ATT) (art. 39) por escrito, o en el caso de urgencias, por teléfono.

El juez o miembro del ATT podrá emitir a su discreción una orden de interceptación de un servicio de telecomunicaciones, siempre que se cumplan las siguientes condiciones (art. 46):

(i) Si se ha cumplido el procedimiento para solicitar la orden.

(ii) Si la solicitud fue telefónica, si era necesario realizarla por esa vía (urgencia).

(iii) Si hay motivos razonables para sospechar que una persona en particular está usando, o es probable que use, el servicio.

(iv) La información que probablemente se obtendría mediante la interceptación podría ayudar en relación con la investigación de un delito grave donde está involucrada la persona o esta se está comunicando con la persona involucrada.

En el caso de la orden con respecto a la persona, se considera si hay motivos razonables para sospechar que una persona está utilizando más de un servicio de telecomunicaciones (art. 46A).

Tanto en el art. 25A de la **Ley de la Organización Australiana de Inteligencia de Seguridad** (ley ASIO) como en los artículos 3L-3LB de la **Ley de Crímenes de 1916** (*Crimes Act*)[71] se establece la posibilidad de otorgar órdenes para el acceso a computadoras, tanto para recopilación de inteligencia por la ASIO como para recabar evidencia en la investigación de delitos por parte de la policía, respectivamente.

Cifrado. En el caso de la Ley de Crímenes, el artículo 3LA establece la posibilidad de obtener una orden judicial para que una persona con conocimientos sobre un equipo o un sistema computacional pueda proveer de cualquier información o ayuda que sea razonable y necesaria para el acceso a dicho equipo o sistema. A pesar de que la norma no hace referencia expresa al bloqueo o cifrado, se ha interpretado que otorga la base legal para exigir tanto el desbloqueo de una computadora como el descifrado del contenido almacenado en ella.[72]

2.2.5. Nueva Zelanda

La interceptación de telecomunicaciones está contenida en dos leyes: ISA, que regula a los organismos de inteligencia, y la **Ley de Búsqueda y Vigilancia de 2012** (*Search and Surveillance Act*, SSA), que regula a las policías.

ISA autoriza a las agencias de inteligencia a realizar actividades de vigilancia que de otra forma serían ilegales, mediante una orden de inteligencia (*intelligence warrant*), que puede ser de dos tipos:

Orden	**Tipo 1**	**Tipo 2**
Objetivo	Recolectar información referente a una persona o un grupo de personas ciudadanas o residentes permanentes de Nueva Zelanda (art. 53).	Casos donde la orden del tipo 1 no es necesaria (art. 54).
Solicitud	Director general de la agencia.	Director general de la agencia.
Autorización (art. 55)	Ministro autorizante y el Comisionado Jefe de Órdenes de Inteligencia.	Ministro autorizante.

71 Texto disponible en: <https://www.legislation.gov.au/Details/C2018C00200>

72 Buchanan, Kelly (2016). Government Access to Encrypted Communications: Australia. Disponible en: <https://www.loc.gov/law/help/encrypted-communications/australia.php>

Causales	(i) Protección de la seguridad nacional (art. 58). (ii) Contribuir a las relaciones internacionales o al bienestar económico de NZ (art. 59).	(i) Protección de la seguridad nacional. (ii) Contribuir a las relaciones internacionales o al bienestar económico de NZ.

Una de las actividades autorizadas por las órdenes de inteligencia es la interceptación de cualquier comunicación privada (art. 67). Dentro de los poderes otorgados tanto a la NZSIS como a la GCSB está la instalación, uso o remoción de un dispositivo de intercepción (arts. 68-69).

SSA[73] establece en su artículo 45 la prohibición a los oficiales de policía de utilizar un dispositivo de interceptación, salvo con el objetivo de obtener material de evidencia para la investigación de ciertos delitos (condenas de 7 años o más, delitos específicos de la ley de armas y de la ley de sustancias psicoactivas).

Interceptación con orden. La interceptación de comunicaciones privadas debe realizarse mediante una orden de dispositivo de vigilancia (*surveillance device warrant*) (art. 46).[74] Esta puede ser solicitada por:

(i) Oficial policial (art. 49), orden que será aprobada por juez (art. 53).

(ii) Otras agencias específicas de cumplimiento de la ley distintas a la policía –*New Zealand Customs Service* o el *Department of Internal Affairs*– en los casos de vigilancia intrusiva o dispositivos de interceptación, mediante una recomendación del gobernador general al ministro de Justicia (art. 50).

Establece la obligación de reportar al juez que expidió la orden dentro del plazo de 1 mes tras el fin del periodo de vigencia de dicha orden (art. 59). Además, el Comisionado de Privacidad emitirá un reporte anual de la vigilancia utilizada (art. 170).

Interceptación sin orden. Permite realizar vigilancia sin una orden, en ciertos casos: (i) autorización o consentimiento (art. 47) y situaciones de emergencia o urgencia (art. 48). En este último caso, el oficial deberá informar a un juez dentro del plazo de un mes tras el último día, dentro del periodo de 48 horas o menos, en que fue usado el dispositivo (art. 60).

Establece el deber de las personas con conocimiento de sistemas informáticos u otros dispositivos de almacenamiento de datos o sitio de internet de ayudar al acceso de una persona que ejerce un poder de registro (art. 130).

La **Ley de Interceptación de Telecomunicaciones de 2013** (*Telecommunications (Interception Capability and Security Act,* TICSA) impone ciertas obligaciones a los

73 Texto disponible en: <http://www.legislation.govt.nz/act/public/2012/0024/latest/DLM2136536.html>

74 Otras actividades de vigilancia intrusiva son autorizadas por esta norma, véase sección 4.d.5.

operadores de red para la interceptación de las telecomunicaciones requeridas por una orden o una autoridad legal.

En su artículo 9 obliga a los operadores a asegurarse de que cada red pública de telecomunicaciones que el operador posea, controle u opere, y cada servicio de telecomunicaciones que el operador proporciona en Nueva Zelanda, tenga una capacidad de interceptación completa.

Cifrado. El artículo 24 de la ley establece el deber de las operadoras de asistir a la agencia que realiza la interceptación. Entre las acciones de asistencia está el descifrado de las telecomunicaciones cuando la persona que asiste es quien realizó el cifrado. Sin embargo, el numeral (4) de la misma norma establece de manera explícita que la persona no está obligada a:

(i) Descifrar cualquier telecomunicación en la red pública o servicio de telecomunicaciones, si el cifrado ha sido proporcionado por medio de un producto que fue (a) suministrado por la persona como agente de ese producto; o (b) suministrado por otra persona y está disponible para el público.

(ii) Asegurar que la agencia de vigilancia tenga la capacidad de descifrar cualquier telecomunicación.

El mismo artículo también establece que el operador de red o proveedor de servicios debe consultar con la agencia de vigilancia que ejecuta la orden o la autoridad legal, con respecto a la forma más eficiente de llevar a cabo el descifrado (art. 24(5)).

2.3. Retención de data y metadatos por ISPs

2.3.1. Reino Unido

La retención de datos de comunicaciones fue regulada originalmente por lDRIPA, ley que fue declarada ilegal por tribunales británicos y por el Tribunal de Justicia de la Unión Europea,[75] por lo cual fue repelida.

En 2016 fue introducida una nueva regulación sobre retención de datos en la parte 4 de IPA. Como se señaló anteriormente, la aplicación de gran parte de esta ley fue suspendida en 2018 por transgredir la normativa europea.[76]

De acuerdo con las normas de IPA, el Ministerio del Interior podrá emitir un aviso de retención (*retention notice*), el cual debe ser racional o proporcionado para una o más de una de las causales del art. 61(7) (que repite las causales contenidas originalmente en 22(2) de RIPA) y debe ser aprobado por un comisionado judicial. Dicha retención no puede durar más de 12 meses desde la fecha de la comunicación o desde que el operador tuvo conocimiento de esta (art. 87).

---

75 Tribunal de Justicia de la Unión Europea (2016). Sentencia ECLI:EU:C:2016:970. Disponible en: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=ES>

76 Cobain, Ian (2018). Op. cit.

El art. 61(7) fija las causales para la obtención de datos de comunicaciones, que son también aplicables a la retención de dichos datos:

(a) Interés de seguridad nacional.

(b) Prevenir o detectar crimen o prevenir desorden.

(c) Interés del bienestar económico del UK, siempre que sea relevante para los intereses de la seguridad nacional.

(d) Interés de seguridad pública.

(e) Proteger la salud pública.

(f) Tasar o recolectar impuestos u otras imposiciones o pagos a instituciones gubernamentales.

(g) Prevenir la muerte, lesiones o cualquier daño a la salud física o mental de una persona, o mitigar cualquier lesión o daño físico o mental a la salud física o mental.

(h) Ayudar en las investigaciones de supuestos errores judiciales involuntarios.

(i) Identificar a una persona muerta o imposible de identificar u obtener información sobre personas cercanas o sobre su muerte o condición.

(j) Funciones relacionadas a la regulación de servicios y mercados financieros o de estabilidad financiera.

Antes de otorgar un aviso de retención, el Ministerio del Interior debe considerar (art. 88):

(i) Beneficios probables del aviso.

(ii) Número probable de usuarios (si se conoce) de cualquier servicio de telecomunicaciones al que se refiere el aviso.

(iii) Viabilidad técnica de su cumplimiento.

(iv) Costo probable del cumplimiento del aviso.

(v) Cualquier otro efecto del aviso en el operador de telecomunicaciones.

Los operadores de telecomunicaciones que retienen datos deben (art. 92):

(i) Garantizar que los datos son de la misma integridad y están sujetos, al menos, a la misma seguridad y protección que los datos de cualquier sistema del que se deriva.

(ii) Asegurar, mediante las medidas técnicas y organizativas apropiadas, que los datos solo pueden ser accedidos por personal especialmente autorizado.

(iii) Proteger a los datos, mediante las medidas técnicas y organizativas apropiadas, contra la destrucción accidental o ilegal, la pérdida o alteración accidental, o la retención, procesamiento, acceso o divulgación no autorizada o ilegal.

Así mismo, los datos deben destruirse si la retención de los datos deja de estar autorizada por la ley.

La adquisición y divulgación de datos de comunicaciones es adicionalmente regulada por el Código de Práctica, dictado bajo la autorización del art. 71 de RIPA que fue actualizado por última vez en 2015. En este se aborda, entre otros, los criterios para determinar la necesidad y la proporcionalidad, que deben ser comunicados a todos aquellos que participan en la adquisición y divulgación de datos de comunicaciones (párrafo 2.36).

Respecto de la necesidad (párrafos 2.37 y 2.38) como mínimo se deben cubrir tres puntos principales para demostrar que la comunicación es necesaria para el propósito legal especificado: (i) naturaleza del evento bajo investigación (como un crimen o persona desaparecida vulnerable); (ii) vinculación de la persona con el hecho (sospechoso, testigo o persona desaparecida); y, (iii) los datos de comunicación, (número de teléfono o una dirección IP) deben estar relacionados con la persona y el evento.

En cuanto a la proporcionalidad (párrafos 2.39 a 2.45), las solicitudes deben incluir un resumen de cómo la obtención de los datos beneficiará la investigación u operación. El nivel de intrusión debe justificarse cuando se toma en consideración el beneficio que los datos proporcionarán a la investigación. Esta justificación debe incluir la confirmación de que, siempre que sea posible, ya se han llevado a cabo investigaciones pertinentes menos intrusivas. También se debe explicar la relevancia de cualquier período de tiempo solicitado, delineando cómo estos períodos son proporcionales al evento bajo investigación. El examen de proporcionalidad debe incluir, en particular, una consideración de los derechos (particularmente a la privacidad y, en los casos pertinentes, la libertad de expresión) de la persona y un equilibrio de estos derechos con el beneficio de la investigación. Por último, las consideraciones de proporcionalidad debe abarcar la referencia al riesgo de intrusión de colateral si este existe (riesgo de cubrir a personas no investigadas) u otras consecuencias no deseadas (por ejemplo, impacto en profesiones con deberes de confidencialidad).

2.3.2. Estados Unidos

No existe una obligación legal de retención de datos a nivel federal.[77] Durante la administración de George W. Bush hubo varias propuestas por introducir una norma de este tipo.[78] La idea fue revivida en 2009 por congresistas del Partido Republicano, como parte del proyecto de ley llamado *Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act*, o "*Internet Safety Act*",[79] que no se convirtió en ley. El art. 5 introducía un artículo en ECPA que obligaría a un proveedor de servicios de comunicación electrónica o de servicios de computación remota a retener, durante al menos dos años, todos los registros u otra información perteneciente a la identidad de un usuario al que se le asigne una dirección IP.

---

77 EFF. United States. Disponible en: <https://www.eff.org/issues/mandatory-data-retention/us>

78 McCullagh, Declan (2005). Your ISP as Net watchdog. CNet. Disponible en: <https://www.cnet.com/news/your-isp-as-net-watchdog/>; Broache, Anne (2006). U.S. attorney general calls for 'reasonable' data retention. CNet. Disponible en: <https://www.cnet.com/U.S.-attorney-general-calls-for-reasonable-data-retention/2100-1030_3-6063185.html>; McCullagh, Declan (2005). FBI, politicos renew push for ISP data retention laws. CNet. Disponible en: < https://www.cnet.com/news/fbi-politicos-renew-push-for-isp-data-retention-laws/>.

79 Texto disponible en: <https://www.govtrack.us/congress/bills/111/hr1076/text>

Entre las normas vigentes que son citadas como ejemplos de retención de comunicaciones por parte de los proveedores de telecomunicaciones está el título II de ECPA (18 U.S.C., arts. 2701-2712).[80] El art. 2703 fija el requerimiento, a petición de una agencia gubernamental, para preservar registros de telecomunicaciones con el objeto de que constituyan evidencia para una investigación. Dicha retención deberá mantenerse por 90 días, lo cual podría extenderse por un periodo adicional de 90 días, en el caso de una renovación de dicho requerimiento.

2.3.3. Alemania

En Alemania se han realizado dos intentos por introducir una ley de retención de datos de comunicaciones obligatoria. El primero de ellos fue en 2007, cuando se promulgó la **Ley para la Enmienda de la Vigilancia de Telecomunicaciones** (*Gesetz zur Neuregelung der Telekommunikationsüberwachung*) que adoptó la Directiva 2006/24/CE de la Unión Europea sobre retención de datos.[81] Dicha norma modificó la Ley de Telecomunicaciones y el StPO, exigiendo a las compañías de telecomunicaciones la retención de los datos de sus usuarios por un mínimo de seis meses y un máximo de dos años, los cuales debían mantenerse disponibles en el caso de delitos graves. Fue declarada inconstitucional por el Tribunal Constitucional alemán, debido a que violaba el secreto de las comunicaciones consagrado en el art. 10 de la Ley Fundamental.[82]

A pesar de que la Directiva 2006/24/CE fue declarada nula por el Tribunal de Justicia de la Unión Europea en 2014,[83] al año siguiente el gobierno alemán promovió la **Ley de retención de datos de telecomunicaciones** (VerkdHSpFruSpPflEG),[84] que modifica al StPO en términos similares a la ley anterior. La vigencia de la ley comenzaba el 1 de julio de 2017, sin embargo, su aplicación fue suspendida porque el Tribunal Administrativo Superior del estado de Renania del Norte-Westfalia determinó que la ley contraviene la legislación de la Unión Europea.[85]

2.3.4. Australia

La retención de datos de telecomunicaciones está regulada por la parte 5-1ª de la **Ley de Telecomunicaciones (Interceptación y Acceso) de 1979** (Ley TIA), que fue introducida por la Ley de Retención de Datos de 2015 (*Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*).[86]

---

80 Texto disponible en: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>

81 Texto disponible en: <http://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP16/T/telekUeberw.html>

82 Tribunal Constitucional de Alemania (2010). Data retention unconstitutional in its present form. Disponible en: <http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html>

83 Tribunal de Justicia de la Unión Europea (2014). Sentencia ECLI:EU:C:2014:238. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62012CJ0293>

84 Texto disponible en: <https://www.gesetze-im-internet.de/verkdhspfrusppfleg/BJNR221800015.html>

85 Chase, Jefferson (2017). Things to know about Germany's recent surveillance laws. Deutsche Welle. Disponible en: <http://www.dw.com/en/things-to-know-about-germanys-recent-surveillance-laws/a-39421060>

86 Texto disponible en: <https://www.legislation.gov.au/Details/C2015A00039>

El art. 187A de la ley establece la obligación de los proveedores de servicios de mantener cierta información y documentos que contengan dichos datos, en relación con cualquier comunicación realizada mediante sus servicios. Dicha retención debe realizarse durante dos años (art. 187C).

El art. 187A establece los tipos de información –fundamentalmente metadatos–[87] que deben retenerse:

(i) Información sobre el nombre, dirección o identificación del usuario y sus cuentas, servicios contratados y dispositivos de telecomunicaciones.

(ii) Identificadores del origen (emisor) de una comunicación.

(iii) Identificadores del destino (receptor) de una comunicación.

(iv) Fecha, hora y duración de una comunicación (inicio y fin) o de su conexión (y desconexión) a un servicio.

(v) Tipo de comunicación (ej. voz, SMS, email, chat, redes sociales) o de servicio (ej. ADSL, WiFi, VoIP, cable, etc.) usado, y de las características de este (ej. espera y reenvío de llamada, uso de datos).

(vi) Ubicación de un equipo o línea utilizada en conexión con una comunicación (ej. torres de celular, puntos de acceso a WiFi).

Los proveedores no están obligados a retener los contenidos de dicha comunicación, el historial de navegación web de sus usuarios o la ubicación del dispositivo mediante el cual se conecta el usuario (art. 187A(4)).

Cabe señalar que la policía australiana ha utilizado la técnica del *IMSI-catcher* para obtener metadatos sobre las comunicaciones móviles desde 2014,[88] antes que se introdujera la regulación de retención de datos.

2.3.5. Nueva Zelanda

La retención de datos obtenidos por vigilancia (tanto por interceptación de telecomunicaciones como por televigilancia) está regulada en lSSA. El art. 63(1) permite la retención de datos no procesados de vigilancia obtenida por la agencia policial en las siguientes circunstancias:

(i) Hasta la conclusión de un proceso penal en relación con un delito respecto del cual se recogieron datos, ya sea la conclusión del procedimiento de apelación o la expiración del plazo para interponer dicho recurso.

(ii) Hasta el anterior por un período máximo de 3 años, o cualquier otro período en

---

87 Galperin, Eva (2015). Data Retention Law Passes in Australia, but the Fight Isn't Over. EFF. Disponible en: <https://www.eff.org/deeplinks/2015/04/data-retention-law-passes-australia-fight-isnt-over>

88 Ben Grubb, Ben y Partridge, Emma (2014). Police scoop up data on thousands in mobile phone 'tower dumps' to track down criminals. The Sydney Morning Herald. Disponible en: <https://www.smh.com.au/technology/police-scoop-up-data-on-thousands-in-mobile-phone-tower-dumps-to-track-down-criminals-20140704-zsvtf.html>

que un juez haya extendido dicho periodo por no más de 2 años,[89] si:

1. No se ha iniciado ningún proceso penal en relación con ningún delito respecto del cual se recopilaron datos.
2. Los datos son necesarios para una investigación en curso por parte de la agencia.

2.4. Televigilancia

2.4.1. Reino Unido

El Reino Unido es uno de los países de Europa y del mundo con la mayor cantidad de cámaras de vigilancia. Según la *British Security Industry Association* (BSIA) en 2013 había alrededor de 6 millones de cámaras, lo cual ha sido caracterizado por el Comisionado de Cámaras de Vigilancia británico como preocupante, ya que "los europeos miran con asombro la cantidad de cámaras que nuestra sociedad tolera".[90]

La televigilancia está regulada por el cap. 1 pt. 2 de la **Ley de Protección de las Libertades de 2012** (*Protection of Freedoms Act*, POFA).[91] La ley obliga al Ministerio del Interior (art. 29-30) a crear y publicar un código de buenas prácticas para guiar el uso y desarrollo de sistemas de cámaras de vigilancia y el uso o procesamiento de las imágenes u otra información obtenida por dichos sistemas, que debe ser presentado al Parlamento junto con el reglamento que le da fuerza.

Dicho código de buenas prácticas debe incluir: (i) consideraciones sobre cómo usar circuitos cerrados de televisión (CCTV); (ii) tipos de sistemas o aparatos; (iii) estándares técnicos; (iv) ubicaciones para esos sistemas o aparatos; (v) publicación de información; (vi) estándares aplicables a personas usando o manteniendo dichos sistemas o aparatos; (vii) estándares aplicables a personas usando o procesando información obtenida por esos sistemas; (viii) acceso o divulgación a dicha información; (ix) procedimientos para reclamos o consultas.

El Ministerio del Interior publicó el *Surveillance Camera Code of Practice* ("código POFA") en junio de 2013. Sus normas están dirigidas a las autoridades pertinentes (incluyendo a la policía) de Inglaterra y Gales que operan sistemas de cámaras de vigilancia, otorgando directrices para cumplir con la ley.

Además, el art. 34 POFA establece que el Ministerio del Interior deberá designar un Comisionado de Cámaras de Vigilancia (*Surveillance Camera Commissioner*, SCC), cuyas funciones son: (i) fomentar el cumplimiento del "código POFA"; (ii) revisar el funcionamiento del código; y (iii) proporcionar asesoría sobre el código (incluyendo

---

89 El art. 63(2) establece las condiciones para una prórroga: (i) debe ser solicitada por la agencia antes de que expire el periodo inicial de 3 años; y (ii) el juez debe estar conforme con la investigación.

90 BBC (2015) CCTV: Too many cameras useless, warns surveillance watchdog Tony Porter. Disponible en: <https://www.bbc.com/news/uk-30978995>

91 Texto disponible en: <https://www.legislation.gov.uk/ukpga/2012/9/contents>

información sobre cambios o incumplimientos de este). El Comisionado también deberá realizar un informe anual sobre sus funciones (art. 35).

La regulación de televigilancia también ha sido entregado a otros códigos de buenas prácticas. Uno de ellos es el publicado por el Comisionado de Información (*Information Commissioner's Office Code of Practice*, "Código ICO"),[92] que está dirigido a personas u organizaciones que operan sistemas de CCTV para usos privados o comerciales, otorgando recomendaciones para cumplir con los requisitos de la DPA. Esta regulación es aplicable a los drones (*unmanned aircraft systems*, UAS) que utilizan cámaras para grabar imágenes.[93]

Otro ejemplo es el de la ciudad de Glasgow, en Escocia, que cuenta con el *Public Space CCTV Code of Practice*,[94] el que expresa que las autoridades y organizaciones que hagan uso de CCTV deben regirse por las obligaciones impuestas por la HRA, la DPA y las reglas para autorizar la vigilancia de RIPA. En su sec. 4 replica los principios de protección de datos personales de la DPA, mientras que en su sec. 5 fija los criterios para que el uso de CCTV en espacios públicos cumpla con las reglas de la RIPA sobre vigilancia dirigida y cubierta.

Las autoridades de Glasgow justifican el uso de CCTV por ser una herramienta necesaria, proporcionada y apropiada para ayudar a reducir el crimen, la victimización y mejorar la seguridad pública. En particular, establece los objetivos para su uso: (i) ayudar al aumento de la captura y enjuiciamiento de delincuentes; (ii) gestión de riesgos y problemas ambientales; (iii) aumento de la seguridad y tranquilidad pública; (iv) reducción de la victimización.

2.4.2. Estados Unidos

A pesar del extenso uso de cámaras de video en espacios públicos en los Estados Unidos,[95] no existen leyes federales que regulen el uso de estas tecnologías de vigilancia, ya sea por privados o por las agencias de cumplimiento de la ley.[96]

Se ha invocado la Cuarta Enmienda de la Constitución en casos donde el uso de televigilancia ha afectado la privacidad de personas. Sin embargo, ningún tribunal superior ha declarado que el uso policial de CCTV como una "pesquisa arbitraria". Incluso algunos tribunales ordinarios han establecido que no hay expectativa de privacidad en espacios públicos.[97]

---

92 ICO (2017). In the picture: A data protection code of practice for surveillance cameras and personal information. Disponible en: <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

93 Feikert-Ahalt, Clara (2016c). Regulation of Drones: United Kingdom. Disponible en: <https://www.loc.gov/law/help/regulation-of-drones/united-kingdom.php>

94 Community Safety Glasgow. Public Space CCTV Code of Practice. Disponible en: <http://www.communitysafetyglasgow.org/wp/wp-content/uploads/2014/12/GOC-Code-of-Practice.pdf>

95 Dailey, Kate (2013). The rise of CCTV surveillance in the US. BBC. Disponible en: <https://www.bbc.com/news/magazine-22274770>

96 ACLU. What's Wrong with Public Video Surveillance? Disponible en: <https://www.aclu.org/other/whats-wrong-public-video-surveillance>

97 The Constitution Project (2006). Guidelines for Public Video Surveillance. Disponible en: <https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf>

Uno de los precedentes más importantes está en el caso *United States v. Jones* (2012),[98] donde la Corte Suprema debió pronunciarse sobre un caso de vigilancia por GPS a un condenado por tráfico de drogas.[99] Los abogados de Jones consideraban que se había violado la razonable expectativa de privacidad del demandado consagrada en la Cuarta Enmienda de la Constitución, cuestión que fue acogida por la Corte de Apelaciones. La Corte Suprema, en opinión mayoritaria redactada por el juez Antonin Scalia, estableció que la instalación y uso del dispositivo de GPS en el vehículo por parte del gobierno constituía una "pesquisa" en términos de la Cuarta Enmienda, adhiriendo al argumento de la defensa.

Otras leyes tampoco son aplicables para proteger la privacidad ante el uso de CCTV. ECPA se refiere únicamente a las comunicaciones auditivas.

A pesar de no ser vinculantes, los principios de mejores prácticas en el uso de información (*Fair Information Practice Principles*, FIPPS) establecen recomendaciones a las entidades gubernamentales para el tratamiento de datos personales, en base a los siguientes derechos por parte de los afectados:[100]

(i) Aviso y conocimiento del propósito de la recopilación de datos y cómo se usa dicha información.

(ii) Consentimiento para la recopilación de información personal y elección sobre cómo se usa.

(iii) Acceso y participación en el proceso de recopilación y uso de datos, incluido el derecho de corrección de los errores.

(iv) Integridad y seguridad adecuadas para proteger la información contra pérdida o uso indebido.

(v) Reparación y responsabilidad por lesiones resultantes de pérdida o mal uso de información personal.

El Departamento de Seguridad Nacional de los Estados Unidos ha publicado un documento con las conclusiones de la discusión sobre cómo el uso de CCTV puede ser compatible con dichos principios.[101]

A nivel estatal, existen varias regulaciones que se refieren a este tipo de tecnologías, incluyendo algunas conocidas como las "leyes Peeping Tom", que se refieren a los delitos de intrusión de la privacidad por voyerismo. Trece estados consideran ilegal la instalación o

---

98 United States v. Jones, 132 S.Ct. 945 (2012). Disponible en: <https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>

99 La policía instaló un dispositivo de seguimiento por GPS en el vehículo registrado a nombre de la cónyuge del sospechoso, amparado en una orden de registro. Sin embargo, el seguimiento excedió lo permitido por dicha orden, tanto geográfica como temporalmente. Los datos obtenidos en la residencia de Jones fueron descartados, pero los demás fueron utilizados en el juicio que lo condenó a cadena perpetua, pues no habría expectativa de privacidad en lugares públicos.

100 The Constitution Project (2006). Op. cit.

101 Homeland Security Department (2007). CCTV: Developing Privacy Best Practices. Disponible en: <https://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf>

uso de dispositivos de fotografiado, observación o escucha de eventos o sonidos en un lugar privado sin el consentimiento de la persona grabada.[102]

2.4.3. Alemania

El art. 4(1) de la **Ley Federal de Protección de Datos** (BDSG) permite el monitoreo de áreas de acceso público con dispositivos ópticos-electrónicos solo en la medida en que sea necesaria para (i) cumplir las tareas de los organismos públicos; (ii) ejercer el derecho de admisión; (iii) perseguir intereses legítimos para propósitos definidos con precisión. En todos los casos, siempre que no haya indicios de que prevalezcan los intereses legítimos de los afectados.

La ley agrega que, en el caso de grandes instalaciones (deportivas, entretenimiento, centros comerciales, estacionamientos) o vehículos de transporte masivo, se considerará especialmente importante la protección de la vida, la salud y la libertad de los asistentes/pasajeros.[103] Esta norma fue introducida por la **Ley de mejoramiento de la videovigilancia de 2017** (*Videoüberwachungsverbesserungsgesetz*, VideoÜVG),[104] que fue una de las leyes que reforzó la vigilancia aprobadas tras el atentado terrorista ocurrido en Berlín en diciembre de 2016. De acuerdo con la prensa alemana, esta disposición también permitiría a la policía el uso de cámaras corporales (*bodycams*).[105]

El art. 4(2) BDSG establece que se deben tomar los medios apropiados para informar sobre la vigilancia, el nombre del operador y los detalles de contacto, lo más temprano posible. Según la interpretación de los expertos, esto significa que el aviso debe ubicarse antes de la entrada de la zona vigilada.[106]

Esta normativa es aplicable a los drones equipados con cámaras de video, salvo que se use con fines recreativos.[107]

2.4.4. Australia

La regulación de televigilancia en Australia está fundamentalmente contenida en la **Ley de Dispositivos de Vigilancia de 2004** (*Surveillance Devices Act*, SDA),[108] la cual solo se

---

102 Dichos Estados son: Alabama, Arkansas, California, Delaware, Georgia, Hawaii, Kansas, Maine, Michigan, Minnesota, New Hampshire, South Dakota and Utah. Véase: RCFP. Introduction: Recording - State hidden camera statutes. Disponible en: <https://www.rcfp.org/first-amendment-handbook/introduction-recording-state-hidden-camera-statutes>

103 Bertermann, Nikolaus (ed.) (2017). The New German Federal Data Protection Act. Disponible en: <https://www.skwschwarz.de/fileadmin/user_upload/Artikel_Dokumente/BDSG-neu_2017-06-07_EN.pdf>

104 Texto disponible en: <http://dip21.bundestag.de/dip21/btd/18/109/1810941.pdf>

105 AFP (2017). German Bundestag greenlights further surveillance measures. Deutsche Welle. Disponible en <http://www.dw.com/en/german-bundestag-greenlights-further-surveillance-measures/a-37878350>

106 Bertermann, Nikolaus (ed.) (2017). Op. cit.

107 Gesley, Jenny (2016c). Regulation of Drones: Germany. Disponible en: <https://www.loc.gov/law/help/regulation-of-drones/germany.php>

108 Texto disponible en: <https://www.legislation.gov.au/Details/C2018C00188>

refiere a la autorización para la instalación y uso de este tipo de tecnologías por las agencias gubernamentales y policiales. No existen leyes que regulen el uso de televigilancia en privados; en el caso de establecimientos comerciales podría invocarse la Ley de Privacidad u otras leyes estatales.[109]

Televigilancia autorizada. La principal forma de autorizar su uso es mediante la obtención de órdenes (*warrant*) que deben ser aprobadas judicialmente: (i) de dispositivo de vigilancia y (ii) de recuperación de dichos dispositivos (art. 10). Ambas deberán ser otorgadas por un juez elegible o un miembro nominado del Tribunal Administrativo de Apelaciones (ATT) (art. 11).

Otra de las formas es obtener una autorización de emergencia, por las siguientes causales: (i) riesgo serio a personas y propiedades; (ii) circunstancias urgentes relacionadas a una orden de recuperación; (iii) riesgo o pérdida de evidencia (arts. 28-30).

En todos los casos, debe emitirse un informe por cada uso de dispositivos de vigilancia a la autoridad competente (fiscal general) y notificar de las órdenes emitidas al Ombudsman (art. 49, 49A). Además, el oficial en jefe de la policía realizará reportes anuales (art. 50).

Órdenes de dispositivos de vigilancia. Pueden solicitarse por las siguientes causales (art. 14):

(i) Un agente policial sospecha por motivos razonables que: (a) uno o más delitos relevantes han sido, están siendo, están a punto de ser, o probablemente sean cometidos; (b) una investigación sobre esos delitos está siendo, será o probablemente será conducida; (c) el uso de un dispositivo de vigilancia es necesario en el curso de esa investigación con el fin de permitir que se obtenga evidencia de la comisión de los delitos pertinentes o la identidad o ubicación de los delincuentes.

(ii) Un agente policial la solicita en virtud de una orden de recuperación de un menor, y sospecha por motivos razonables que el uso de un dispositivo de vigilancia puede ayudar en la ubicación y recuperación segura del niño al que se refiere dicha orden.

(iii) Un agente policial es autorizado por orden de asistencia mutua; sospecha, por motivos razonables, que el uso de un dispositivo de vigilancia es necesario en el curso de la investigación o del procedimiento de investigación, para obtener pruebas de: (a) la comisión del delito al que se refiere la orden; o (b) la identidad o ubicación de las personas sospechosas de cometer el delito.

(iv) Un agente federal sospecha, por motivos razonables, que el uso de un dispositivo de vigilancia ayudará a la realización de una operación de integridad autorizada en relación con una ofensa que se sospecha ha sido, es o será probable que sea cometida por un miembro del personal de una agencia objetivo; para: (a) registrar o monitorear la operación; y (b) permitir que se obtenga evidencia relacionada con la comisión del delito o la integridad, ubicación o identidad de cualquier miembro del personal de la agencia objetivo.

---

109 OAIC. Surveillance and monitoring. Disponible en: <https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/what-can-i-do-about-my-neighbour-s-security-camera>

(v) Un agente policial sospecha, por motivos razonables, que el uso de un dispositivo de vigilancia ayude sustancialmente a obtener información relacionada con una persona relacionada a una orden de control para: (a) proteger al público de un acto terrorista; (b) prevenir la entrega de apoyo o la facilitación de un acto; (c) prevenir la entrega de apoyo o la facilitación de una actividad hostil en un país extranjero; o (d) determinar si la orden de control, o cualquiera posterior, se ha cumplido o se está cumpliendo.

Televigilancia sin orden de autorización. La ley también contempla excepciones para el uso de ciertos tipos de vigilancia sin órdenes que las autoricen: (i) dispositivos de vigilancia ópticos por oficiales de policía en el ejercicio de sus funciones, siempre y cuando su uso no involucre el ingreso en propiedades o la interferencia en vehículos o cosas sin el permiso correspondiente (art. 37); (ii) escucha o grabación de voz por oficiales de policía en el ejercicio de sus funciones, siempre que quien habla sea oficial de policía u otra persona quien sepa o debería saber que está siendo escuchado, o que haya consentimiento expreso o implícito del hablante (art. 38); (iii) uso de dispositivos de rastreo en la investigación de un delito de importancia (art. 39).

2.4.5. Nueva Zelanda

Los sistemas de órdenes de inteligencia y vigilancia contenidos en ISA y en la SAA, que fueron previamente analizadas en relación con la interceptación de telecomunicaciones, son también aplicables a la televigilancia.[110]

ISA permite realizar, mediante una orden de inteligencia (*intelligence warrant*), la conducción de vigilancia respecto de personas, lugares o cosas (art. 67). Dentro de los poderes otorgados a la NZSIS podrán usar, mantener o remover un dispositivo de vigilancia visual (art. 68), mientras que a la GCSB se le permite la misma acción, aunque con el requisito de mantener la seguridad operacional de cualquier actividad autorizada que se lleve a cabo (art. 69).

De acuerdo con SSA las conductas que requieren una orden de dispositivo de vigilancia (*surveillance device warrant*) de acuerdo con el artículo 46, además de la interceptación, son:

(i) Dispositivo de rastreo, excepto cuando este sea instalado con el único propósito de asegurarse de cuándo una cosa ha sido abierta, manipulada o tratada de alguna otra manera, y la instalación de dicho dispositivo no involucra la violación de propiedad o bienes.

(ii) Observación de actividades privadas en recintos privados, y cualquier grabación de dicha observación, realizada mediante un dispositivo de televigilancia.

(iii) Uso de un dispositivo de vigilancia que implique la violación de propiedad o bienes.

(iv) Observación de actividades privadas en los alrededores de recintos privados,

---

110 Esta sección solo se referirá a las menciones específicas en ambas leyes de uso de televigilancia. Para mayor información sobre los procedimientos para obtener órdenes de inteligencia y de vigilancia, véase la sección 4.b.5.

y cualquier grabación de dicha observación, si cualquier parte de dicha observación ha sido realizada mediante un dispositivo de televigilancia, por los propósitos de una o varias investigaciones conectadas, y la duración de la observación exceda de: (a) 3 horas en cualquier período de 24 horas; o (b) 8 horas en total.

Como se ha dicho anteriormente, este tipo de órdenes puede ser solicitada por un oficial de policía y autorizada por juez, o, en el caso de otras agencias específicas, debe contar con la autorización del ministro de Justicia, previa recomendación del gobernador general.

Para los demás usos de las tecnologías de televigilancia, llevados a cabo por organizaciones tanto públicas como privadas y por individuos, aplican las normas de la Ley de Privacidad. Dicha ley creó el Comisionado de la Privacidad (art. 12), que tiene entre sus funciones la promoción, mediante educación y publicidad, de la comprensión y aceptación de los principios de privacidad consagrados por la ley (art. 13).

En 2009 el Comisionado publicó un documento con **directrices para el uso de CCTV** dirigido a comercios, agencias y organizaciones, con el propósito que dichas entidades puedan entender, mediante términos simples, cómo se cumple con la Ley de Privacidad.[111] Entre las principales directrices están:

(i) Responsabilidad: hay una persona encargada de operar el sistema de CCTV.

(ii) Equipamiento: las cámaras son adecuadas para el propósito elegido.

(iii) Ubicación no intrusiva de las cámaras.

(iv) Signos adecuados que indiquen la televigilancia.

(v) Límites de tiempo para la operación de las cámaras.

(vi) Uso y divulgación de las imágenes grabadas: solo para el propósito del sistema.

(vii) Seguridad en la transmisión y almacenamiento de las imágenes grabadas.

(viii) Retención de las imágenes grabadas por períodos limitados.

(ix) Registro de acceso al sistema: incluye accesos por individuos y la policía.

(x) Revisión periódica del funcionamiento del sistema.

2.5. Biometría

2.5.1. Reino Unido

El Reino Unido cuenta una **base de datos nacional de ADN** (*National DNA Database*, NDNAD) que es, de acuerdo con el supervisor europeo de Protección de Datos, "la base

111 Privacy Commissioner (2009). Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations. Disponible en: <https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf>

de datos más desarrollada de Europa (y del mundo)",[112] y actualmente cuenta con más de 6 millones de entradas, correspondientes a un total de 5,3 millones de individuos.[113]

El tratamiento de material biométrico como prueba en investigaciones penales está regulado por la **Ley de Evidencia Policial y Criminal de 1984** (*Police and Criminal Evidence Act*, PACE).[114] Esta ley fue sustancialmente modificada por la POFA, que en su parte 1 capítulo 1 regula la destrucción, retención y uso de material probatorio.

Toma de muestras. Se establece en general que el material biométrico no puede ser tomado sin el consentimiento apropiado, salvo que se cumpla con los requisitos de la ley; en el caso de huellas dactilares o de su pisada, la persona debe estar detenida tras su arresto por un delito, y sus huellas no han sido tomadas en el curso de la investigación por la policía (arts. 61-61A PACE).

La POFA regula en su parte 1 capítulo 2 la protección de la información biométrica de los niños en las escuelas y otros lugares. Establece el requisito de notificar y obtener el consentimiento de al menos uno de los padres antes de procesar la información biométrica (art. 26 POFA), y también regula las excepciones a dicha regla: (i) no se puede encontrar a uno de los padres; (ii) incapacidad de estos; (iii) protección del menor impide contactarlos; (iv) no es practicable notificarlo u obtener su consentimiento (art. 27 POFA).

Retención y uso. Por regla general, la ley permite la retención de las muestras hasta el fin de la investigación penal, o hasta la conclusión de los procedimientos contra la persona que se inicien tras dicha investigación (art. 63E PACE). Además, la ley establece otros casos excepcionales para la retención: investigaciones pendientes, reincidencia, consentimiento del comisionado, seguridad nacional, entrega voluntaria, entre otras (arts. 63F-63O PACE).

Los requisitos para usar el material retenido son: (i) interés de seguridad nacional; (ii) propósitos de investigación terrorista; (iii) prevención o detección de crimen, investigación de un delito o la conducción de una persecución penal; (iv) identificación de persona fallecida o de la persona de la que proviene el material (art. 63T PACE).

Destrucción. Las muestras biométricas deben ser destruidas si el oficial jefe de la policía considera que: (i) la toma de las muestras fue ilegal; (ii) la toma de las muestras fue realizada a una persona durante un arresto que fue ilegal o se basó en una identidad equivocada; (iii) cualquier otro caso donde no haya una autorización para retener dicho material. En general, las muestras deben ser destruidas, a más tardar, tras el transcurso de 6 meses desde que fueron tomadas (arts. 63D, 63R PACE).

La POFA creó dos **instituciones supervisoras** del tratamiento de material biométrico. El principal es el Comisionado para la retención y el uso de material biométrico, que tiene como objetivo revisar las determinaciones de seguridad realizadas en virtud de

---

112 Supervisor Europeo de Protección de Datos (2007). Dictamen 2007/C 169/02. Diario Oficial de la Unión Europea. Disponible en: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:169:0002:0014:ES:PDF>

113 National DNA Database statistics, Q4 2017 to 2018. Disponible en: <https://www.gov.uk/government/statistics/national-dna-database-statistics>

114 Texto disponible en: <https://www.legislation.gov.uk/ukpga/1984/60>

distintas leyes y regular los usos a los que se aplica el material retenido en virtud de una determinación de seguridad nacional (art. 20 POFA). El Comisionado deberá realizar un reporte anual al Ministerio del Interior sobre el ejercicio de sus funciones (art. 21 POFA).

Además, la NDNAD está supervisada por un Panel de Estrategia, que debe guiar al organismo en el cumplimiento de la ley respecto a la destrucción y retención de los perfiles de ADN, quien deberá consultar sus lineamientos con el Comisionado para la retención y el uso de material biométrico (art. 63AB PACE).

El uso de **reconocimiento facial** no ha sido regulado en el Reino Unido. En 2018, organismos de derechos humanos han denunciado que la policía ha utilizado estas tecnologías en una veintena de eventos de alta convocatoria desde mayo de 2017,[115] incluyendo la final de la Champions League 2017 en Cardiff, donde dos mil personas fueron erróneamente identificadas como potenciales criminales.[116]

2.5.2. Estados Unidos

Al igual que en el caso de la televigilancia, no existe una ley federal que regule el uso de material biométrico. Por ello, ciertos Estados han tomado la iniciativa de establecer regulaciones para proteger la privacidad de sus ciudadanos.[117]

La **Ley de Privacidad de Información Biométrica de Illinois** (*Biometric Information Privacy Act*)[118] obliga a las organizaciones privadas que estén en posesión de identificadores biométricos o información biométrica, a desarrollar una política escrita, puesta a disposición del público, donde se establezca un cronograma de retención y pautas para destruir permanentemente dicha información, cuando el propósito inicial de recopilar u obtenerla ha sido satisfecha o dentro de los 3 años posteriores a la última interacción de la persona con la entidad, lo que ocurra primero (art. 15(a)).

También establece que ninguna entidad privada puede recopilar, capturar, comprar, recibir a través del comercio u obtener de otra manera el identificador biométrico o la información biométrica de una persona o del cliente, a menos que (art. 15(b)):

(i) Informe por escrito al sujeto o a su representante legal que se está recolectando o almacenando un identificador biométrico o información biométrica.

(ii) Informe por escrito al sujeto o a su representante legal sobre el propósito específico y la duración del término para el cual se está recopilando, almacenando y utilizando un identificador biométrico o información biométrica; y

---

115 Bowcott, Owen (2018). Police face legal action over use of facial recognition cameras. The Guardian. Disponible en: <https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras>

116 Telegraph Reporters (2017). Police defend facial recognition technology that wrongly identified 2,000 people as potential criminals. Disponible en: <https://www.telegraph.co.uk/news/2018/05/05/police-defend-facial-recognition-technology-wrongly-identified>

117 McCray, Niya T. (2017). The Face of the Future: Developments in Biometric Privacy Law and Litigation. Data and Security Dispatch, vol. 3, issue 3. Disponible en: <http://portal.criticalimpact.com/newsletter/newslettershow5.cfm?contentonly=1&content=358691&id=21791>

118 Texto disponible en: <http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004>

(iii) Reciba una autorización escrita para hacerlo, firmada por el sujeto o su representante legal.

Además, dicha entidad podrá divulgar dicha información siempre y cuando (art. 15(d)):

(i) Consentimiento por el sujeto o su representante legal.

(ii) La divulgación completa una transacción financiera solicitada o autorizada por el sujeto o su representante legal.

(iii) La divulgación es requerida por una ley estatal o federal o una ordenanza municipal.

(iv) La divulgación se requiere de conformidad con una orden o citación válida emitida por un tribunal de jurisdicción competente.

La **Ley de Identificadores Biométricos de Texas** (*Biometric Identifier Statute*), replicada en el art. 503.001 del Código de Comercio,[119] establece que una persona no puede capturar un identificador biométrico de un individuo para un propósito comercial a menos que la persona (i) informe al individuo antes de capturar el identificador biométrico; y (ii) reciba el consentimiento de este para capturarlo.

La persona que posee un identificador biométrico de un individuo que es capturado para un propósito comercial no puede venderlo, arrendarlo o divulgarlo a otra persona a menos que:

(i) Consentimiento del individuo para fines de identificación en caso de desaparición o muerte de la persona.

(ii) La divulgación complete una transacción financiera que el individuo solicitó o autorizó.

(iii) Sea requerida o permitida por un estatuto federal o estatal.

(iv) Sea hecha por una agencia policial con el propósito de hacer cumplir la ley en respuesta a una orden judicial.

La **Ley de Privacidad Biométrica de Washington** (*Biometric Privacy Act*, HB1493)[120] regula los identificadores biométricos en términos análogos al estatuto de Texas.

2.5.3. Alemania

La BDSG establece una regulación especial para el tratamiento de categorías especiales de datos personales (datos sensibles), entre los cuales incluye la información sobre datos genéticos y datos biométricos para el propósito de identificar a una persona natural (art. 46(14)). También define ambos conceptos:

(i) **Datos genéticos** (art. 46(11)): datos personales relativos a las características genéticas heredadas o adquiridas de una persona natural que proporcionen información única sobre la fisiología o la salud de esa persona y que se

---

119 Texto disponible en: <https://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503-001.html>

120 Texto disponible en: <http://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true>

obtienen, en particular, del análisis de una muestra biológica de la persona física en cuestión.

(ii) **Datos biométricos** (art. 46(12)): datos personales resultantes de un procesamiento técnico específico relacionado con las características físicas, fisiológicas o de comportamiento de una persona natural que permitan o confirmen la identificación única de esa persona física, en particular imágenes faciales o datos dactiloscópicos.

Tratamiento permitido. Los arts. 22-24 establecen las causales donde se permite el tratamiento de dichas categorías especiales de datos personales, según se trate de organismos públicos o privados:

Organismo(s)	**Causales**
Públicos y privados (art. 21)	(i) Necesario para ejercer los derechos derivados del derecho a la seguridad social y la protección social; (ii) Necesario para los fines de la medicina preventiva, evaluación de la capacidad laboral del empleado, diagnóstico médico, entrega de atención, tratamiento o manejo de los sistemas de salud o asistencia social; (iii) Razones de interés público en el ámbito de la salud pública, como la protección contra amenazas transfronterizas graves para la salud o la garantía de altos estándares de calidad y seguridad de la asistencia sanitaria y de medicamentos o dispositivos médicos. En estos casos se deberá tomar las medidas para el secreto profesional.

Públicos (art. 21)	(i) Necesidad urgente por razones de interés público sustancial. (ii) Prevención de una amenaza sustancial a la seguridad pública. (iii) Necesidad urgente para evitar daños sustanciales al bien común o salvaguardar preocupaciones sustanciales del bien común. (iv) Razones urgentes de defensa o para cumplir obligaciones supra o intergubernamentales en el ámbito de la gestión de crisis o la prevención de conflictos, o para medidas humanitarias; en estos casos, el interés del controlador supera los intereses del interesado.
	Otros casos donde es necesario para ejercer su función (art. 23): 1. Si interesa al interesado y no hay ninguna razón para suponer que el sujeto de datos rechazaría el consentimiento si conociera el otro propósito. 2. Si es necesario verificar la información proporcionada por el interesado porque hay motivos para creer que esta información es incorrecta. 3. Si es necesario para evitar daños sustanciales al bien común o una amenaza para la seguridad pública, la defensa o la seguridad nacional; para salvaguardar preocupaciones sustanciales del bien común; o para asegurar los ingresos fiscales y aduaneros. 4. Si es necesario para el proceso de delitos o faltas administrativas, para llevar a cabo o hacer cumplir las penas o medidas penales o multas. 5. Si es necesario para evitar daños graves a los derechos de otra persona. 6. Si es necesario para ejercer los poderes de supervisión y monitoreo, para llevar a cabo auditorías o análisis organizacionales del controlador.
Privados (art. 24)	Necesario para (i) prevenir amenazas a la seguridad pública o estatal o para enjuiciar delitos; o (ii) el establecimiento, ejercicio o defensa de reclamaciones legales, a menos que el interesado tenga un interés primordial en que no se procesen los datos.

2.5.4. Australia

La Ley de Privacidad establece una regulación especial para el tratamiento de información sensible, entre los cuales incluye: (i) información genética sobre un individuo que no sea información de salud; (ii) información biométrica que será usada para el propósito de verificación biométrica automática o identificación biométrica; y (iii) plantillas biométricas (art. 6.1).

Dichos tipos de información sensible sobre un individuo no podrán ser recolectados por una organización pública o privada, a menos que se verifique una de estas circunstancias (arts. 3.3 y 3.4):

(i) Haya consentimiento del individuo, y la información esté directamente relacionada con los fines o actividades de la organización recolectora.

(ii) Aplique una de las siguientes condiciones:

1. La recolección es requerida o autorizada por ley u orden judicial.
2. La recolección es parte de una situación generalmente permitida.
3. La recolección es realizada por una organización de salud a la que se permite recolectar información de ese tipo.
4. La recolección es realizada por un cuerpo policial, y se cree razonablemente que dicha actividad es necesaria o directamente relacionada con sus funciones.
5. La recolección es realizada por una organización sin fines de lucro, y la información se relaciona con las actividades de la organización, y se circunscribe solo a sus miembros o contactos regulares en razón de sus actividades.

La **Ley de Migración de 1995** (*Migration Act*)[121] regula la obtención de datos biométricos para los detenidos por inmigración. El art. 261AA establece que las personas que no sea ciudadanas australianas deben proporcionar a un funcionario autorizado uno o más de los siguientes identificadores personales:

(i) Huellas dactilares o huellas de las manos de la persona (incluidas las tomadas con papel y tinta o tecnologías digitales).

(ii) Medidas de la altura y el peso de la persona.

(iii) Fotografía u otra imagen de la cara y los hombros de la persona.

(iv) Firma de la persona.

(v) Otros que permita la ley.

La ley también regula la realización de exámenes y procedimientos a la persona detenida para obtener dichos identificadores (art. 261AB), los cuales no pueden realizarse de una manera cruel, inhumana o degradante (art. 261AF), y deben ser ejecutados por un oficial autorizado del mismo sexo que la persona (art. 261AH).

2.5.5. Nueva Zelanda

La regulación de la información biométrica fue introducida por la **Ley de mejora de la legislación de verificación de identidad y procesos fronterizos de 2017** (*Enhancing Identity Verification and Border Processes Legislation Act*),[122] que reformó varios cuerpos legales, entre ellos, la Ley de Privacidad y la Ley de Inmigración.

La Ley de Privacidad establece una regulación especial para el tratamiento de datos sensibles ("información de identidad", *identity information*), entre los que se incluyen: (i) información

---

121 Texto disponible en: <https://www.legislation.gov.au/Details/C2018C00173>

122 Texto disponible en: <http://www.legislation.govt.nz/act/public/2017/0042/latest/DLM6887824.html>

biométrica de un individuo; (ii) fotografía o imagen visual del individuo; (iii) detalles de cualquier característica distintiva (incluyendo tatuajes y marcas de nacimiento) (art. 109C).

Se define información biométrica como:

(i) Uno o más de los siguientes tipos de información personal:

(a) una fotografía de todo o parte de la cabeza y los hombros de la persona;

(b) impresiones de las huellas dactilares de la persona; o

(c) un escaneo de los iris de la persona.

(ii) Registro electrónico de la información personal que pueda usarse para la correspondencia biométrica.

El art. 109D establece que ciertas agencias expresamente señaladas por la misma ley pueden tener acceso a estos datos sensibles, manejados por otras agencias titulares, por causales también específicas.

La **Ley de Inmigración de 2009** (*Inmigration Act*)[123] regula el uso que se le da a la información biométrica para los procesos de inmigración.

El art. 30 establece que la información biométrica puede ser utilizada para (i) establecer un registro de la identidad de una persona; (ii) establecer o verificar la identidad de una persona; y (iii) asistir en los procesos de toma de decisiones (visas, ciudadanía). Dicha información puede ser recogida, mediante sistemas automáticos u otros, por un oficial de inmigración o un oficial de refugiados y protección, y deben respetarse las normas de la Ley de privacidad (art. 31).

También puede requerirse la recolección de información biométrica a un pasajero que abordará un avión con destino a Nueva Zelanda, o ya en el área de inmigración del país. Si se opone a la medida, podrá exponerse a no poder abordar el avión o no poder acceder al país (arts. 100, 111). Incluso se le puede exigir la recolección de información biométrica a un pasajero que no sea ciudadana neozelandesa que está dejando el país (art. 120).

El art. 287 establece una categoría de información biométrica especial que puede ser requerida para el ingreso y el tránsito en Nueva Zelanda: (i) impresiones de las palmas de las manos; (ii) impresiones de la pisada; (iii) medidas de la persona entera; (iv) fotografías de la persona entera. Este tipo de información especial puede solicitarse a una persona sujeta a deportación (art. 288). Si esa persona se opone a dicha medida, el oficial de inmigración podrá solicitar una orden judicial para obtener dicha información (art. 289-290).

---

123 Texto disponible en: <http://www.legislation.govt.nz/act/public/2009/0051/latest/DLM1440303.html>

3. Criterios jurídicos del sistema europeo aplicables a la implementación de tecnología de vigilancia

El marco jurídico que regula las tecnologías de vigilancia está conformado por dos tipos de instrumentos: tratados multilaterales, los cuales incluyen a los convenios adoptados por el Consejo de Europa, y las normas de derecho comunitario, como los reglamentos y directivas, que materializan los objetivos de los tratados. Finalmente el Supervisor Europeo de Protección de Datos también realiza recomendaciones específicas en asuntos que tocan el uso de tecnología con fines de vigilancia.

a. Tratados que consagran los derechos a la privacidad y a los datos personales

En primer lugar, están los tratados que consagran los derechos a la privacidad y a los datos personales. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, mejor conocido como la Convención Europea de Derechos Humanos, consagra el derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. De acuerdo a su inciso 2°, las afectaciones al ejercicio de este derecho por parte de los Estados miembros deberán estar establecidas por ley, siempre que constituyan "una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".[124]

El artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE)[125] consagra el derecho a la protección de los datos personales. El inciso 2° mandata al Parlamento Europeo y al Consejo a establecer las normas comunitarias sobre la protección del tratamiento de datos personales realizado por las instituciones europeas y los Estados, y sobre la libre circulación de estos datos.

b. Reglamentos referidos a la protección de datos personales

En segundo lugar, está la normativa referida específicamente a la protección de datos personales.[126] Uno de los instrumentos más relevantes en esta materia es el Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (RGPD),[127] que vino a reemplazar a la anterior normativa (Directiva 95/46/CE). El RGPD establece seis principios que están enunciados en su art. 5:

---

124 Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Disponible en: <https://www.echr.coe.int/Documents/Convention_SPA.pdf>

125 Texto disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:12012E/TXT>

126 Entre los instrumentos que han regulado el tratamiento de datos personales están: Directiva 95/46/CE de 24 de octubre de 1995, relativa al tratamiento de los datos personales y a su libre circulación; Directiva 97/66/CE de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones; Directiva 2000/31/CE de 8 de junio de 2000 sobre comercio electrónico; Reglamento (CE) 45/2001 de 18 de diciembre de 2000, relativo Al tratamiento de datos personales por las instituciones y los organismos comunitarios y a su libre circulación.

127 Texto disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679>

1) Licitud, lealtad y transparencia.
2) Limitación de la finalidad.
3) Minimización de datos.
4) Exactitud.
5) Limitación del plazo de conservación.
6) Integridad y confidencialidad.

El reglamento otorga al interesado los siguientes derechos: acceso (art. 15), rectificación (art. 16), supresión u "olvido" (art. 17), limitación del tratamiento (art. 18), portabilidad de los datos (art. 20), y oposición (art. 21). También otorga el derecho a no ser sujeto de decisiones basadas solamente en tratamiento automatizado (art. 22), junto a un derecho de explicación (Considerando 71).

Las obligaciones y derechos que establece el RGDP pueden ser limitadas siempre que se respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar (art. 23):

1) Seguridad del Estado.
2) Defensa.
3) Seguridad pública.
4) Prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.
5) Otros objetivos importantes de interés público general, en particular un interés económico o financiero, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social.
6) Protección de la independencia judicial y de los procedimientos judiciales.
7) Prevención, investigación, detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas.
8) Función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos de seguridad del Estado, otros objetivos importantes y normas deontológicas.
9) Protección del interesado o de los derechos y libertades de otros.
10) Ejecución de demandas civiles.

c. Las Directrices de videovigilancia del Supervisor Europeo de Protección de Datos

Las Directrices de videovigilancia presentadas en 2010 por el Supervisor Europeo de Protección de Datos, son un instrumento dirigido a los órganos de la Unión, a través del cual se intenta conciliar la protección de los derechos fundamentales con el uso de tecnología para

asegurar la seguridad pública. Para ello, las directrices proponen una aproximación pragmática que se base en la selectividad y la proporcionalidad de los sistemas de videovigilancia.

Las cámaras debieran ser usadas en tal forma que solo se dirijan a cubrir problemas de seguridad previamente identificados y evitar la colección de imágenes irrelevantes. Lo anterior con el fin de minimizar las intrusiones a la privacidad y, a la vez, ayudar a un uso más dirigido y eficiente de la videovigilancia.[128]

Entre las recomendaciones generales que resultan más llamativas de las Directrices se encuentra la de adopción de sistemas de vigilancia que incorporen la privacidad por diseño, además de recomendar una evaluación de impacto en el derecho a la privacidad previo a la adquisición e implementación de este tipo de sistemas.[129]

---

128 Supervisor Europeo de Protección de Datos, "Directrices de videovigilancia", 17 de marzo de 2010, Disponible en: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf, p. 4

129 Ibid, p. 10-12.

4. Iniciativas internacionales para el desarrollo de principios

Además de los principios sobre vigilancia emanados del marco jurídico del sistema europeo, también existen otras iniciativas de carácter internacional que aportan criterios para que los gobiernos utilicen las tecnologías de vigilancia con respeto a la privacidad.

El documento más conocido de este tipo es el de Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,[130] un texto suscrito por varias organizaciones no gubernamentales en 2013, cuyo objetivo es establecer directrices para que las leyes, políticas y prácticas de vigilancia de las comunicaciones adhieran a los tratados y estándares internacionales de derechos humanos, específicamente en lo relativo a los derechos a la privacidad y a la libertad de expresión.

Los 13 principios que contiene dicho documento son:

(i) Legalidad: las limitaciones a los derechos humanos deben ser fijadas por ley.

(ii) Objetivo legítimo: la vigilancia debe ser realizada por autoridades específicas para proteger un interés jurídico relevante y sin incurrir en una discriminación arbitraria.

(iii) Necesidad: la vigilancia debe ser el único medio para alcanzar el objetivo legítimo, o el menos propenso a vulnerar los derechos humanos de los que estén disponibles.

(iv) Idoneidad: los casos de vigilancia autorizados por ley deben ser apropiados para cumplir el objetivo legítimo específico identificado.

(v) Proporcionalidad: dado que la vigilancia es un acto altamente intrusivo que interfiere con los derechos humanos, y lo siguiente debe ser comprobado judicialmente:

a. Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo.

b. Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito grave o una amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la información protegida.

c. Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica.

d. La información a la que se accederá estará limitada a lo relevante y material para el delito grave o la amenaza específica al fin legítimo alegado.

---

130 Necessary and Proportionate Coalition (2014). Necesarios & Proporcionados. Disponible en: <https://necessaryandproportionate.org/es/necesarios-proporcionados>

e. Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud.

f. La información será accedida solo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización.

g. Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

(vi) Autoridad judicial competente: la toma de decisiones sobre vigilancia debe ser tomada por autoridad judicial imparcial e independiente, y debe:

a. Estar separada y ser independiente de las autoridades que ejercen vigilancia.

b. Estar capacitada en materias relacionadas y ser competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las comunicaciones, las tecnologías utilizadas y los derechos humanos.

c. Tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

(vii) Debido proceso: los procedimientos legales de vigilancia estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general.[131]

(viii) Notificación del usuario: la decisión de autorizar la vigilancia debe ser notificada con el tiempo y la información, salvo que:

a. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana.

b. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia.

c. El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.

(viii) Transparencia: publicar información suficiente sobre el uso de la normativa de vigilancia para que las personas puedan comprender plenamente su alcance.

(ix) Supervisión pública: Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la

131 Necessary and Proportionate Coalition (2014). Necesarios & Proporcionados. Disponible en: <https://necessaryandproportionate.org/es/necesarios-proporcionados>

rendición de cuentas de la vigilancia.

(x) Integridad de las comunicaciones y sistemas: los Estados no deben obligar a los proveedores de servicios o de hardware o software a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de vigilancia.

(xii) Garantías para la cooperación internacional: los tratados de asistencia judicial recíproca deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la vigilancia de las comunicaciones, se adopte el estándar disponible con el mayor nivel de protección para las personas.

(xiii) Garantías contra el acceso ilegítimo y derecho al recurso efectivo: promulgar leyes que penalicen la vigilancia ilegal de las Comunicaciones por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los *whistleblowers* y medios de reparación a las personas afectadas.

Un grupo de empresas de tecnología, entre las que se incluyen Apple, Google, Microsoft y Facebook, conformaron la coalición ***Reform Government Surveillance*** (RGS), la cual publicó una declaración de principios para la regulación de la vigilancia. Estos principios son:[132]

1) Limitación de la autoridad de los gobiernos para recopilar información de los usuarios de los proveedores de servicios, equilibrando la necesidad de obtener datos en circunstancias limitadas, las expectativas razonables de privacidad de los usuarios y el impacto en la confianza en internet.

2) Supervisión y responsabilidad: debe existir un marco legal claro en el que el poder ejecutivo esté sujeto a fuertes controles y equilibrios, por tribunales independientes.

3) Transparencia en las solicitudes del gobierno: permitir que las empresas publiquen el número y la naturaleza de las solicitudes gubernamentales de información.

4) Respetar el libre flujo de la información: no debe inhibirse el acceso de compañías o individuos a información legalmente disponible que esté almacenada fuera del país.

5) Evitar conflictos entre gobiernos: promover un marco que rija las solicitudes legales de datos en todas las jurisdicciones, para evitar leyes contradictorias.

6) Garantizar la seguridad y la privacidad a través de un cifrado fuerte: no exigir que las compañías de tecnología diseñen vulnerabilidades en sus productos y servicios.

---

132 RGS. Putting Principles in Action. Disponible en: <http://www.reformgovernmentsurveillance.com/principles/>

5. Conclusiones

Un examen sucinto sobre los países estudiados, muestra que, en general, cuentan con legislaciones que regulan de forma detallada la vigilancia, aun si no es idéntica entre ellas la sistematización de las reglas para el uso de tecnologías en actividades de vigilancia.

A diferencia del caso de las legislaciones latinoamericanas estudiadas, existe un nivel de dispersión normativa sobre uso de tecnologías de vigilancia por parte de agentes estatales, donde es más patente la aplicación de principios jurídicos comunes, tales como los principios de legalidad y proporcionalidad. A nivel internacional, además de los instrumentos propios del sistema internacional de protección de los derechos humanos, aparecen instrumentos regionales como la CEDH, que entregan un nivel adicional de obligatoriedad a los principios.

A nivel legal, los principios de legalidad y proporcionalidad aparecen en general como reconocidos en la normativa, sin perjuicio de la amplitud para el ejercicio de vigilancia en el ámbito de la interceptación de comunicaciones. De este modo, esa forma de interferencia respeta formalmente el principio de legalidad, a pesar de la dispar situación del control judicial o de las existencia de deberes de transparencia o reglas de rendición de cuentas.

En otro contraste con las reglas en América Latina, varios de los países estudiados cuentan con reglas expresas para el tratamiento y el acceso a ciertos datos, tales como los datos biométricos, los datos y metadatos retenidos por ISP, y la información obtenida mediante uso de televigilancia. Se encuentran asimismo instancias de control permanente sobre la televigilancia, específicamente en relación con el uso de videocámaras en el espacio público.

Como punto en común con las legislaciones que justifican ciertas interferencias del Estado vigilante en América Latina, además de las finalidades de prevención y persecución de delitos de cierta gravedad, aparece la seguridad nacional como justificación. Dada la prevalencia del concepto a nivel global, parece altamente necesario mantener condiciones óptimas de control, transparencia y rendición de cuentas para prevenir abusos en función del concepto.

Finalmente, cabe destacar el esfuerzo por la formulación de principios de alto nivel, basados tanto en las preocupaciones de la industria y la sociedad civil, como también basados en un desarrollo más avanzado de los derechos ya existentes dentro del derecho internacional de los derechos humanos. Tales principios, y en particular los principios necesarios y proporcionados, constituyen hoy por hoy las mejores guías a seguir al momento de regular y administrar las capacidades de vigilancia por los Estados.

Existen aspectos locales y regionales dentro de las normativas de vigilancia que no pueden obviarse. Además de las diferencias en lenguaje, en instituciones y en sistemas normativos, deben considerarse seriamente las correlaciones entre normativas propias de la actividad de vigilancia y aquellas regulaciones institucionales que le impactan de forma indirecta, o que condicionan la acción de las autoridades. Esto obliga a la revisión de las normas internacionales vigentes, de la normativa orgánica relevante y de la existencia de esquemas de políticas públicas que afecten a las tecnologías de vigilancia, tales como normas de seguridad nacional, de transparencia, de compras públicas, de ciberseguridad.

Antes de utilizar regulaciones extranjeras como modelo, deben considerarse también las críticas formuladas desde las distintas partes interesadas a los esquemas hoy vigentes. Es decir, es necesario considerar los cuestionamientos públicos a las prácticas de agencias de inteligencia o a procesos de modificación legal de reglas de vigilancia en algunos de los países aquí estudiados. La elaboración de estándares debe estar pendiente de mantener ese equilibrio.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina