



Universidad Miguel Hernández
Facultad de Ciencias Sociales y Jurídicas de Elche

Grado en Seguridad Pública y Privada SEPP

TRABAJO DE FIN DE GRADO

Curso 2023-2024

**VULNERACIÓN DE LA INTIMIDAD EN ARAS DE
LA SEGURIDAD**

Tutora: Carolina Maestre Muñoz

Alumno: Pedro José Clemente Manzanera

Índice

Resumen	3
Abstract	4
Palabras clave	5
Keywords	5
Introducción	5
Metodología	7
1. Marco Teórico	7
2. Marco Legal	14
3. El equilibrio entre seguridad y privacidad	18
4. Sentencias Judiciales relacionadas:	19
4.1. Análisis de STS 141 de 13 de mayo de 2020	19
4.2. Análisis de STS 329 de 20 de abril de 2016	24
5. Medidas de seguridad en la actualidad	28
6. Impacto social, psicológico y medidas de protección.....	38
7. Conclusiones	43
Bibliografía.....	46
Otras fuentes	48

Resumen

La seguridad en sentido amplio ha sido una de las claves para el desarrollo de la humanidad, a lo largo de la historia la sociedad en general ha sufrido diferentes guerras, conflictos de todo tipo entre diferentes culturas, terrorismo, hambruna, crisis humanitarias, crisis sanitarias y otros eventos a nivel mundial que han repercutido negativamente en ese desarrollo, también la seguridad es un factor muy importante en la protección de la integridad física o incluso la vida.

En la sociedad moderna en la que vivimos, con el aumento del desarrollo de nuevas tecnologías en todos los ámbitos los gobiernos también han aplicado ese aumento de la tecnología y han integrado dentro de su estrategia la vigilancia para mantener unos niveles de seguridad adecuados, pero esa estrategia puede generar diferentes opiniones en la sociedad sobre la pérdida de la privacidad de las personas en aras de mantener dicha seguridad. La cuestión es: ¿Cuáles son los límites en la vigilancia y el control de las personas por parte del gobierno para mantener la seguridad, con la consiguiente pérdida del derecho a la intimidad de la sociedad?

En este trabajo se exploran las medidas de mantenimiento de la seguridad llevadas a cabo por algunos gobiernos modernos y democráticos, como la vigilancia masiva, el uso de reconocimiento facial, el Big Data y la inteligencia artificial entre otras, que pueden estar poniendo en peligro la privacidad de las personas permitiendo a los gobiernos y algunas empresas de seguridad recopilar y analizar datos personales, lo que plantea dudas éticas y legales. ¿Se están cruzando los límites de la privacidad en nombre de la seguridad?

El estudio analiza cómo estas prácticas afectan la confianza de la ciudadanía en las instituciones y cómo un exceso de vigilancia puede erosionar la democracia y los derechos fundamentales. Si el gobierno tiene demasiado control, las personas pueden sentir que viven en un estado autoritario, donde la libertad de expresión y otros derechos están en riesgo.

El objetivo principal es analizar la situación actual y encontrar estrategias para un equilibrio entre la seguridad, la privacidad y el derecho a la intimidad, sugerir métodos y soluciones para proteger la intimidad sin comprometer la seguridad. En un mundo en constante evolución es importante debatir este tema para mantener un equilibrio justo y

adaptar las necesidades en cuanto a la seguridad manteniendo una protección adecuada de los derechos de los ciudadanos.

Abstract

Security has been a key factor in the development of humanity. Throughout history, society has faced various wars, conflicts between different cultures, terrorism, famine, humanitarian crises, health crises, and other global events that have negatively impacted that development. Moreover, security is the most important factor in protecting physical integrity and even life.

In the modern society we live in, with the increased development of new technologies in all fields, governments have also applied this technological advancement to enhance their strategies, increasing surveillance to maintain adequate levels of security. However, this strategy can generate differing opinions in society about the loss of individual privacy in the name of maintaining security. The question is: What are the limits of government surveillance and control of individuals to maintain security at the expense of society's right to privacy?

This work explores the security measures implemented by some modern and democratic governments, such as mass surveillance, facial recognition, Big Data, and artificial intelligence, among others, and how these measures are endangering personal privacy. These practices allow governments and some security companies to collect and analyze personal data, raising ethical and legal concerns. Are the boundaries of privacy being crossed in the name of security?

The study examines how these practices affect public trust in institutions and how excessive surveillance can erode democracy and fundamental rights. If the government has too much control, people may feel they are living in an authoritarian state where freedom of expression and other rights are at risk.

The main objective is to analyze the current situation and find strategies to balance security with privacy and the right to intimacy. It aims to suggest methods and solutions to protect privacy without compromising security. In a constantly evolving world, it is crucial to discuss this issue to maintain a fair balance and adapt security requirements with adequate protection of rights.

Palabras clave

Seguridad, privacidad, Intimidad, vigilancia y tecnología.

Keywords

Security, privacy, intimacy, surveillance and technology.

Introducción

La seguridad siempre ha ocupado un lugar importante en la humanidad, desde tiempos de civilizaciones antiguas hasta el momento actual con sociedades modernas, la cuestión de la seguridad siempre ha estado en un lugar privilegiado de las funciones políticas y la sociedad a nivel global. Si bien es cierto que en las últimas décadas algunos efectos negativos de la globalización han llevado a los gobiernos a implementar medidas de seguridad más rigurosas y a ampliar su capacidad de vigilancia y control, estas acciones también han suscitado preocupaciones respecto a la privacidad y la intimidad de los ciudadanos y ha generado un debate sobre hasta qué punto el mantenimiento de la seguridad puede justificar la vulneración de estos derechos fundamentales ya que las medidas implementadas para garantizar esta seguridad pueden chocar con los derechos individuales de privacidad e intimidad de las personas generando conflictos éticos o legales.

En el presente trabajo se debatirá sobre el complejo equilibrio entre la seguridad y el derecho a la intimidad en el contexto moderno y se analizarán algunas de las medidas de seguridad actuales empleadas por los Gobiernos, que puedan comprometer la privacidad de las personas en aras de la seguridad, como la vigilancia masiva, el acceso gubernamental a datos personales y el uso de tecnologías como el reconocimiento facial y el Big Data refiriéndose éste a la recopilación masiva de datos, la inteligencia artificial y el análisis predictivo que permiten a los Gobiernos y a algunas empresas de seguridad vinculadas tener un control sobre las personas tan poderoso como abrumador. Este crecimiento tecnológico tan positivo en algunos aspectos plantea también nuevos desafíos para la privacidad y exige un análisis cuidadoso para evitar la creación de un entorno donde el derecho a la intimidad sea prácticamente inexistente o se vea seriamente perjudicado.

Además, se explorarán las implicaciones legales incluyendo la revisión de algunas sentencias al respecto y se someterá a juicio ético estas prácticas, así como el impacto que tienen en la sociedad y en la confianza que depositan los ciudadanos en las instituciones.

El objetivo de este estudio es identificar y evaluar los límites entre seguridad y privacidad, así como proponer estrategias que permitan proteger la intimidad de las personas sin comprometer la seguridad.

El equilibrio entre seguridad e intimidad es un tema crítico y contemporáneo, con repercusiones significativas para la sociedad, la ley y los derechos humanos. Abordar este tema es importante por influir tan significativamente en la vulneración de la intimidad de la sociedad ya que en algunas ocasiones la seguridad se antepone a la privacidad dejando en un segundo lugar los efectos que puedan llegar a causar en la sociedad moderna, como el detrimento en derecho a la intimidad y la privacidad que están consagrados como derechos fundamentales en nuestra Constitución y Tratados Internacionales.

La utilización de métodos de vigilancia de los Gobiernos respecto a la población con el fin de detectar posibles riesgos para la seguridad han evolucionado en los últimos tiempos debido a un aumento significativo de las tecnologías referidas anteriormente, sin olvidar el desarrollo de las comunicaciones, tanto es así, que se pueden rastrear datos y personas de forma extraordinaria, este control de movimientos de las personas plantea preguntas sobre la legitimidad de las actuaciones de los Estados para llevar a cabo este control en aras de la seguridad.

Otra cuestión importante que lleva consigo el ámbito de este estudio es la confianza o, mejor dicho, la pérdida o disminución de la confianza que los ciudadanos depositan en las instituciones, ya que la sociedad puede sentirse demasiado observada y esto puede provocar animadversión y escepticismo hacia los dirigentes del Estado, además de estrés, ansiedad y pérdida de autonomía que afectaría sin duda al bienestar de las personas y a la calidad de las relaciones sociales.

No podemos olvidar que existe un riesgo mayor, si cabe al de la pérdida de la seguridad, se trata del riesgo a intercambiar un Estado social y democrático de derecho como el nuestro por otro en el que un exceso en la vigilancia dé lugar a abusos por parte del Gobierno, a la discriminación y persecución de minorías sociales, al detrimento o pérdida

de otros derechos como la libertad de expresión, de manifestación o reunión, Justicia e igualdad ante la ley, etc. en definitiva, el peligro de convertir un Estado social y democrático en un estado autoritario. En un mundo cada vez más interconectado, es importante reflexionar sobre los límites de la seguridad respecto a la intimidad. ¿Estamos dispuestos a sacrificar nuestra intimidad en aras de la seguridad colectiva? Este trabajo invita a explorar esta pregunta desde diferentes perspectivas, con el objetivo último de promover un equilibrio justo entre ambos valores fundamentales de la sociedad contemporánea.

Metodología

El método utilizado para el siguiente estudio se basa en la búsqueda, recopilación y análisis crítico de documentos y referencias bibliográficas, así como, en la exploración meticulosa de diversas fuentes documentales, como investigaciones científicas, leyes, artículos, entre otros. Se describen los hallazgos obtenidos, lo que permite desarrollar el cuerpo teórico relacionado con el tema de estudio.

1. Marco Teórico

Es importante abordar la definición de privacidad e intimidad, así como la definición de seguridad y el marco legal que regula estos conceptos para el desarrollo del presente estudio con el fin de entender de una manera más clara los límites y vulneraciones posibles en el ámbito jurídico, pero no debemos olvidar el ámbito social y sentimental en el que sin lugar a dudas la invasión de la intimidad representa un problema digno de una solución estatal.

Definición de Privacidad e Intimidad

El término privacidad se refiere al derecho de las personas a controlar su información personal y a decidir cómo, cuándo y a quién se comparte esa información. Es un concepto amplio que abarca tanto el ámbito físico como el digital. En el entorno físico, la privacidad implica el derecho a ser libre de intrusiones o vigilancia no deseada y en el ámbito digital, se relaciona con el control sobre los datos personales y la protección contra su recopilación y uso indebido. Por otro lado, **intimidad** es un término más estrecho que denota el espacio personal y emocional que una persona tiene el derecho a mantener incluyendo aspectos como la vida personal, las relaciones familiares y el derecho a ser

libre de interferencias no deseadas. Aunque privacidad e intimidad están estrechamente relacionados, la privacidad tiene un alcance más amplio, abarcando la protección de la información personal y la confidencialidad, mientras que la intimidad se enfoca más en el espacio personal y las relaciones cercanas¹.

El derecho a la intimidad en la doctrina española ha sido estudiado por numerosos autores, cada uno con su propia interpretación del concepto. Por ejemplo, Albadalejo (1990) describe el derecho a la intimidad como el poder otorgado a una persona para controlar y mantener en reserva las actividades de su esfera íntima, personal y familiar, permitiéndole excluir a terceros de este ámbito².

Otra definición nos la ofrece Iglesias Cubría (1990) lo define como aquello que está reservado y no puede ser invadido ni siquiera con conocimiento ajeno, destacando que la intimidad abarca todo aquello que uno puede mantener oculto al conocimiento de otros. Aunque no existe unanimidad en la definición de intimidad, la mayoría de la doctrina coincide en que esta implica un espacio privado donde el individuo tiene derecho a excluir a otros. En sus inicios, la doctrina tendió a enfatizar la dimensión negativa de la intimidad, centrándose en la posibilidad de mantener la vida privada fuera del alcance de otros. Sin embargo, hoy en día, también se reconoce el aspecto positivo, que implica el control y disposición de la propia información personal³.

En resumen, la visión del derecho a la intimidad ha evolucionado de una simple protección de la propiedad privada y la inviolabilidad del domicilio a un derecho fundamental que protege la privacidad y la dignidad de la persona.

¹ TOSCANO, M., "Sobre el concepto de privacidad: la relación entre privacidad e intimidad", Isegoría, (57), 2017, pp. 533–552.

² ALBADALEJO, M., *Definición de privacidad e intimidad*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1990, pp. 1-3.

³ IGLESIAS CUBRÍA, J., *Definición de privacidad e intimidad*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1990, pp. 1-3.

Esta protección abarca aspectos como el control de la información personal, el derecho al anonimato, y la exclusión de terceros de la esfera privada del individuo y aunque la doctrina ha prestado tradicionalmente más atención al derecho al honor, hoy en día la intimidad está adquiriendo mayor relevancia debido a las crecientes preocupaciones sobre privacidad y uso de datos en el mundo digital, así como las interferencias de los gobiernos en el control y rastreo de datos personales en aras de mantener la seguridad en un alto nivel.

La Constitución Española (CE) de 1978 representó un hito importante para el derecho a la intimidad en España, ya que por primera vez este derecho se incluyó en la Carta Magna⁴, ubicándolo entre los derechos fundamentales (Sección 1ª Capítulo II Título I). Esto significa que se garantizó su protección a través del ordenamiento jurídico español. Los autores y el legislador comprendieron la importancia de este derecho para salvaguardar la vida privada de los ciudadanos. En la Constitución Española, los derechos fundamentales abarcan desde el artículo 15 hasta el 29, y el artículo 30.2. Según Luis María Díez Picazo (1995), son *"aquellos derechos que se reconocen a todas las personas por el mero hecho de serlo, inherentes a la condición de persona o ciudadano, y que vinculan a todos los poderes públicos, incluido el legislador democrático"*⁵. Estos derechos tienen garantías específicas para su protección y procedimientos especiales para su restablecimiento en caso de vulneración, como su desarrollo por Ley Orgánica (artículo 81 CE), la protección judicial mediante procedimientos preferentes, y el recurso de amparo ante el Tribunal Constitucional. El derecho a la intimidad está expresamente recogido en el artículo 18.1 de la Constitución Española, que establece *"se garantiza el derecho al honor, a la intimidad personal y familiar, y a la propia imagen"*.

⁴ GOBIERNO DE ESPAÑA, *Constitución Española*, 1978.

⁵ DÍEZ PICAZO, L. M., *Los derechos fundamentales en la Constitución Española*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1995, pp. 45-50.

Sin embargo, como todos los derechos fundamentales, la intimidad tiene sus límites. Según palabras propias de Juan Manuel Goig Martínez (2000) *“hoy en día, tanto en la doctrina, como en la jurisprudencia constitucional se ha admitido que no existen derechos ilimitados, sino que todo derecho tiene sus límites (...). La doctrina ha defendido la existencia de límites internos de los derechos y libertades, entendiendo por tales aquellos que derivan del propio concepto del derecho y de las facultades que de él derivan, bien determinados legalmente o por la propia Constitución, y límites externos, derivados no del propio concepto del derecho o libertad, pero necesarios para proteger este propio concepto o bienes protegidos constitucionalmente”*⁶.

La doctrina española destaca que no existen derechos absolutos y que siempre hay que buscar un equilibrio cuando se produce un conflicto entre diferentes derechos fundamentales. Cuando hay un conflicto entre derechos, se aplica la técnica de ponderación para encontrar un punto de equilibrio sin caer en el subjetivismo y este proceso implica un análisis minucioso del caso concreto, determinando qué derecho es más digno de protección en la situación específica, y considerando la gravedad de la afectación y el rango normativo pero se debe tener en cuenta que no existe una respuesta absoluta, ya que cada situación requiere un análisis detallado para encontrar el equilibrio adecuado. El Tribunal Constitucional ha sostenido que el derecho a la intimidad, como cualquier otro derecho fundamental, no es absoluto y puede ceder ante intereses constitucionalmente relevantes, siempre que el recorte sea necesario, proporcionado y respete el contenido esencial del derecho⁷.

⁶ GOIG MARTÍNEZ, J. M., *Límites de los derechos fundamentales*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 2000, pp. 51-55.

⁷ ATIENZA, M., *Ponderación y sentido común jurídico*, Universidad de Alicante, 2014.

De esta manera, el derecho a la intimidad se define como un derecho subjetivo de defensa y un derecho positivo, de rango superior, por su importancia en la convivencia social. En nuestro país se ha llevado a cabo el desarrollo legislativo del Derecho a la Intimidad en la Ley Orgánica 1/1982⁸, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen (LO 1/1982), siendo la norma que desarrolla el derecho a la intimidad en el ordenamiento jurídico español. Esta ley establece el ámbito de protección de la intimidad, definiendo qué se considera una intromisión legítima o ilegítima y abordando el consentimiento del afectado dentro del ámbito del derecho civil. Las intromisiones ilegítimas se enumeran en el artículo 7.1 de la LO 1/1982, e incluyen acciones como el uso no autorizado de dispositivos de escucha o filmación para obtener información privada, la divulgación de información privada que afecte a la reputación o el buen nombre, y la revelación de datos privados obtenidos a través de actividades profesionales u oficiales determinando además que las acciones que constituyen vulneraciones del derecho a la intimidad requieren reparación. Por otro lado, para Moreno Boadilla (2016) la ley también describe las intromisiones legítimas, que son excepciones a las ilegítimas como las acciones autorizadas por ley o por una autoridad competente, o aquellas donde la información tiene un interés general. Sin embargo, el problema radica en definir qué constituye interés general, lo que a menudo implica un equilibrio entre el interés público y el derecho a la privacidad. Finalmente, cualquier intromisión que cuente con el consentimiento del titular del derecho afectado no se considera ilegítima. El artículo 2.2 de la LO 1/1982 establece que no habrá intromisión ilegítima si la acción está autorizada por ley o si el titular ha dado su consentimiento expreso. En conclusión, el derecho a la intimidad en España es un derecho fundamental con limitaciones y diseñado para proteger a las personas frente a injerencias no autorizadas en su vida privada, pero también debe equilibrarse con otros derechos fundamentales y con intereses públicos legítimos⁹.

⁸ LEY ORGÁNICA 1/1982, de 5 de mayo, de *Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen*, Boletín Oficial del Estado, 14 de mayo de 1982.

⁹ MORENO BOBADILLA, Á., "El derecho a la intimidad en España", *Ars Boni et Aequi*, 12(1), 2016, pp. 33-57.

Definición de Seguridad

La **seguridad** puede ser definida como el estado de estar libre de peligro o riesgo. En el contexto de este estudio, el término se refiere a las medidas y políticas destinadas a proteger a las personas y a la sociedad contra amenazas como el terrorismo, el crimen organizado, el cibercrimen y otros riesgos que puedan comprometer la estabilidad y el bienestar general¹⁰.

En España la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional¹¹ se desarrolla afirmando en su preámbulo *“La seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones. La legislación española así lo reconoce e interpreta, y contiene instrumentos normativos que, partiendo del marco diseñado por la Constitución, regulan los aspectos fundamentales que han venido permitiendo a los poderes públicos cumplir con sus obligaciones en esta materia. Así, las normas aplicables a los estados de alarma, excepción y sitio, a la Defensa Nacional, a las Fuerzas y Cuerpos de Seguridad, a la protección de la seguridad ciudadana, a la protección de infraestructuras críticas, a la protección civil, a la acción y el servicio exterior del Estado o a la seguridad privada, regulan, junto con la legislación penal y los tratados y compromisos internacionales en los que España es parte, distintos aspectos de la seguridad. Esta regulación se basa en la asignación de competencias a las distintas autoridades y Administraciones Públicas, y se articula en un modelo tradicional y homologable con los países de nuestro entorno, que se ha demostrado válido hasta ahora y que ha permitido hacer frente a las necesidades de seguridad de una sociedad abierta, libre y democrática como la española.”*

¹⁰ OBRADOR SERRA, F., *Análisis del concepto de seguridad*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1992, pp. 65-70.

¹¹ LEY 36/2015, de 28 de septiembre, de *Seguridad Nacional*, Boletín Oficial del Estado, 29 de septiembre de 2015.

Anterior a nuestra Ley de Seguridad Nacional existen otras como las que Francisco Obrador Serra (1992) reúne en su “*análisis del concepto de seguridad*”¹² relatando de forma histórica algunos de los hechos más significativos como el que ocurrió en agosto de 1941 en el que el presidente estadounidense Franklin D. Roosevelt y el primer ministro británico Winston Churchill se reunieron a bordo de un buque en el Atlántico para acordar un conjunto de principios y políticas que dieron lugar a la Carta del Atlántico. Esta carta, firmada el 1 de enero de 1942 por 26 países aliados en guerra contra el Eje (Alemania, Italia y Japón), sirvió de base para la creación de la Carta de las Naciones Unidas.

El punto 8 de la Carta del Atlántico establece que el mantenimiento de la paz en el futuro no será posible mientras las naciones continúen utilizando armamentos de tierra, mar o aire para amenazar o agredir a otras naciones. El documento propone el desarme de estas naciones y la creación de un sistema de seguridad general, amplio y permanente.

La Carta de las Naciones Unidas, que se firmó al término de la Conferencia de San Francisco en junio de 1945, menciona repetidamente la necesidad de paz y seguridad internacional. Este concepto es clave para el preámbulo de la carta, donde se expresa el compromiso de unir fuerzas para mantener la paz y la seguridad. También se menciona en diversos capítulos y artículos de la carta, más de una docena de veces.

El Consejo de Seguridad, uno de los órganos principales de la ONU, se encarga del mantenimiento de la paz y la seguridad internacional. Sus responsabilidades incluyen la resolución pacífica de disputas internacionales, la determinación de amenazas a la paz, y la implementación de medidas preventivas políticas, económicas o militares, cuando sea necesario, mediante acciones de algunos o todos los Estados miembros. Además, el Consejo de Seguridad tiene la responsabilidad de formular planes para la regulación de armamentos¹³.

¹² OBRADOR SERRA, F. *Análisis del..., Op. Cit. P.12.*

¹³ OMODEO, M. G., “*El Consejo de Seguridad de la ONU y la Seguridad Colectiva*”, *Ius Et Veritas*, 6(11), 1995, pp. 59-64.

La ONU define la seguridad como la condición en la que Estados e individuos están poco expuestos a ataques militares, problemas económicos, presiones políticas o injusticias sociales. La seguridad es, para un Estado-Nación, “*la estructura que evita su conquista material y protege su modo de vida*” (United Nations, n.d.)¹⁴. Otros tratados internacionales también abordan la seguridad y la defensa colectiva, como el Tratado de Bruselas de 1948 (que llevó a la creación de la Unión Europea Occidental), el Tratado del Atlántico Norte de 1949 (fundador de la OTAN), el Tratado del Sudeste Asiático de 1954 (SEATO), y el Pacto de Varsovia de 1955. Todos estos tratados se refieren a la paz y seguridad internacional y comparten una visión común, inspirada en la Carta de San Francisco (United Nations, 1945). Sin embargo, el concepto de seguridad en estos acuerdos suele aplicarse de manera más concreta al ámbito militar, centrándose en la defensa y la estrategia, aunque su alcance varíe respecto al campo internacional (Morgenthau, 2006).¹⁵

2. Marco Legal

El marco legal proporciona una base sólida para explorar cómo se define y regulan las limitaciones respecto a la privacidad e intimidad, y cómo esto se relaciona con las políticas de seguridad. A partir de dichas leyes se puede analizar el impacto de las leyes y políticas sobre la privacidad y el equilibrio entre seguridad e intimidad.

El derecho a la intimidad está reconocido en varias legislaciones y tratados internacionales para proteger a las personas de interferencias injustificadas en su vida privada y personal, entre las que se encuentran las siguientes:

- **Declaración Universal de los Derechos Humanos (DUDH):** El artículo 12 de la DUDH establece que nadie será objeto de injerencias arbitrarias en su vida privada, familia, hogar o correspondencia, y que todo el mundo tiene derecho a la protección de la ley contra tales injerencias.

¹⁴ UNITED NATIONS, *Charter of the United Nations*, San Francisco, 1945.

¹⁵ MORGENTHAU, H. J., *Politics among nations: The struggle for power and peace*, 7ª ed., McGraw-Hill Education, 2006.

- **Pacto Internacional de Derechos Civiles y Políticos (PIDCP):** Este pacto, que también menciona el derecho a la privacidad, obliga a los estados firmantes a proteger la intimidad de sus ciudadanos.
- **Convención Americana sobre Derechos Humanos (Pacto de San José 1969):** En su artículo 11 garantiza la protección contra injerencias arbitrarias en la vida privada de la ciudadanía y prohíbe los ataques al honor y a la reputación de las personas.
- **Constituciones Nacionales:** Muchas constituciones incluyen artículos que garantizan el derecho a la privacidad y a la intimidad. Por ejemplo, la Constitución Política de los Estados Unidos Mexicanos (1917) establece en su Artículo 16 la inviolabilidad del domicilio y en el Artículo 24 garantiza la libertad de creencias, que tiene relación con la privacidad y en Argentina la Constitución Nacional (1994) en su Artículo 19 establece el principio de privacidad de las acciones privadas.
- **En la Unión Europea, el Reglamento General de Protección de Datos (GDPR)** establece normas estrictas para la protección de datos personales y el consentimiento necesario para su recopilación y uso. En otros países, como Estados Unidos, las leyes de privacidad están más fragmentadas, pero existen regulaciones como la Ley de Protección de la Privacidad Electrónica (ECPA) y la Ley de Derechos de Privacidad de Educación Familiar (FERPA).
- **Leyes Relacionadas con la Seguridad Nacional:** Algunas leyes permiten la recopilación masiva de datos en nombre de la seguridad nacional. Ejemplos incluyen la Ley Patriota en Estados Unidos y el Reglamento de Investigaciones de Poderes en el Reino Unido. Estas leyes han sido criticadas por su impacto en la privacidad y la falta de transparencia.

En España, el derecho a la intimidad está recogido principalmente en la Constitución Española y en otras leyes específicas que se recogen a continuación:

- **Constitución Española (1978) artículo 18:** Este artículo establece varios aspectos relacionados con la privacidad e intimidad:
 - **Sección 1:** "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."

- **Sección 2:** "El domicilio es inviolable. Ninguna entrada o registro podrá hacerse sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito."
 - **Sección 3:** "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial."
 - **Sección 4:** "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."
- **Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen**
 - Esta ley desarrolla el artículo 18 de la Constitución y establece el marco legal para la protección civil del derecho al honor, la intimidad personal y familiar, y la propia imagen.
 - Define qué se considera intromisión ilegítima y establece las acciones y procedimientos para la protección de estos derechos.
 - **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (actualmente derogada y sustituida por el Reglamento General de Protección de Datos de la Unión Europea y la Ley Orgánica 3/2018)**
 - Aunque ya no está en vigor, es importante mencionar esta ley porque fue la legislación clave en España sobre protección de datos personales.
 - **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales**
 - Esta ley sustituye a la Ley Orgánica 15/1999 y adapta el Reglamento General de Protección de Datos de la Unión Europea (RGPD) al ordenamiento jurídico español.
 - Establece las bases para la protección de datos personales, que es una parte integral del derecho a la intimidad.

Aspectos Clave de la Ley Orgánica 3/2018

Como ya se ha mencionado anteriormente la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), fue creada para adaptar el Reglamento General de Protección de Datos de la Unión Europea (RGPD) al marco jurídico español. Esta ley es fundamental para la protección de la privacidad y los datos personales en España. Algunos de sus aspectos clave son:

- **Consentimiento para el tratamiento de datos:** La ley establece que el tratamiento de datos personales debe basarse en el consentimiento claro e inequívoco del titular de los datos. El consentimiento no puede ser asumido ni obtenido mediante coerción.
- **Derechos de las personas en relación con sus datos personales:** La LOPDGDD reconoce varios derechos para las personas cuyos datos se procesan, como el derecho de acceso, rectificación, cancelación, oposición, portabilidad de datos y derecho al olvido. Estos derechos permiten las personas controlar el uso y la difusión de sus datos personales.
- **Protección especial para datos sensibles:** La ley trata con especial cuidado los datos considerados sensibles, como aquellos relacionados con origen étnico, creencias religiosas, opiniones políticas, salud y orientación sexual. Su tratamiento está sujeto a estrictas restricciones.
- **Menores de edad:** La ley establece una edad mínima de 14 años para que un menor pueda consentir el tratamiento de sus datos sin el permiso de sus padres o tutores.
- **Delegado de Protección de Datos (DPO):** Algunas organizaciones están obligadas a nombrar a un DPO para garantizar el cumplimiento de la ley y servir de enlace entre la organización y la Agencia Española de Protección de Datos (AEPD).
- **Responsabilidad y sanciones:** La ley establece fuertes sanciones para las empresas y organizaciones que no cumplan con sus obligaciones respecto al tratamiento de datos personales, con multas significativas para los infractores.
- **Derecho a la Información:** La ley exige que cualquier entidad que recoja datos personales informe a las personas sobre el propósito de la recopilación, el uso que

se les dará, la duración de la retención de datos y con quiénes se compartirán esos datos.

- **Derecho a la Portabilidad de Datos:** Los individuos tienen el derecho de recibir sus datos personales en un formato estructurado y comúnmente utilizado, lo que les permite transferir sus datos de un controlador a otro.
- **Medidas de Seguridad:** Las organizaciones deben implementar medidas de seguridad técnicas y organizativas para proteger los datos personales de accesos no autorizados, pérdidas o filtraciones. Esto incluye la realización de evaluaciones de impacto cuando se procesan datos sensibles.
- **Violación de Datos Personales:** La ley obliga a las organizaciones a notificar a la Agencia Española de Protección de Datos (AEPD) y a los individuos afectados en caso de violación de datos personales que pueda comprometer sus derechos.

3. Equilibrio entre seguridad y privacidad

Tal y como se ha plasmado en la introducción el motivo principal de este trabajo es abordar un tema importantísimo en el mundo actual: la seguridad respecto a la privacidad de las personas. Es fundamental encontrar un equilibrio entre la seguridad y la privacidad ya que, por un lado, necesitamos medidas de seguridad efectivas para proteger a la sociedad de amenazas como el terrorismo o la delincuencia y, por otro lado, no podemos permitir que estas medidas invadan nuestra privacidad y socaven nuestras libertades individuales, pero a veces la seguridad debe primar sobre la privacidad. Si queremos vivir en una sociedad segura, es necesario que las autoridades puedan tomar medidas efectivas para prevenir y combatir el crimen, incluso si eso implica cierta intrusión en la privacidad de las personas. Sin embargo, no podemos ignorar los riesgos de abuso de poder y vigilancia excesiva por parte del Estado. Históricamente, hemos visto cómo regímenes autoritarios han utilizado la excusa de la seguridad para restringir las libertades individuales y perseguir a disidentes políticos por lo que debemos aprender de la historia y asegurarnos de que las medidas de seguridad respeten siempre los derechos humanos y las libertades fundamentales¹⁶.

¹⁶ MORENO BOBADILLA, Á. “El derecho a ... Op. Cit. P. 11.

Una parte importante de la inclinación de la balanza hacia un lado u otro es cómo se utilizan los datos personales en nombre de la seguridad. En la era digital, nuestras actividades en línea y fuera de línea generan una gran cantidad de datos que pueden ser utilizados para monitorear y controlar nuestras vidas y es fundamental que existan salvaguardas adecuadas para proteger nuestra privacidad en este contexto, la protección de datos y la privacidad en línea son cuestiones cada vez más relevantes por lo que se necesitan leyes y regulaciones sólidas que protejan nuestros datos personales y nos den control sobre cómo se utilizan siendo muy importante encontrar un equilibrio entre la seguridad y la privacidad, así como en la necesidad de proteger nuestros datos personales en la era digital.

4. Sentencias Judiciales relacionadas

En esta sección se incluirán algunas sentencias judiciales relevantes que ilustran los criterios empleados por los tribunales en casos de videovigilancia, intervención de comunicaciones y protección de la privacidad personal en relación con la seguridad pública ofreciendo un marco interpretativo sobre los límites legales de la seguridad y la privacidad, permitiendo observar la tendencia jurisprudencial en torno a esta relación seguridad-derecho a la intimidad.

4.1 Análisis de Sentencia Penal Nº 141/2020, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec 2749/2018 de 13 de mayo de 2020 El Derecho a la Intimidad y el uso de Dispositivos GPS en Vehículos.

A modo de introducción y para sumergirnos en este caso en concreto, de forma resumida podemos ver como el Tribunal Supremo, en su sentencia 141/2020 de 13 de mayo¹⁸, abordó la validez de la prueba obtenida mediante un dispositivo de seguimiento instalado en el vehículo de un sospechoso, lo que llevó al hallazgo de casi 100 gramos de cocaína. Esta prueba resultó de una investigación policial en la que se solicitó autorización judicial para usar un GPS en el vehículo del acusado. Tras localizar al sospechoso gracias a la baliza, la policía registró el vehículo y encontró la droga. El acusado fue condenado por un delito contra la salud pública por la Audiencia Provincial de León, sentencia que fue confirmada por el Tribunal Superior de Justicia de Castilla-León, si bien la defensa presentó un recurso de casación argumentando la vulneración del derecho a la intimidad,

al considerar que la autorización judicial para instalar el dispositivo no estaba suficientemente fundamentada, lo que invalidaría la prueba obtenida.

El Tribunal Supremo, al analizar el caso, consideró que la instalación de dispositivos de seguimiento afecta el derecho a la privacidad y requiere autorización judicial previa. Asimismo, señaló que la autorización judicial en este caso no cumplía los principios de proporcionalidad, necesidad y excepcionalidad, lo que hacía inválida la prueba. El Tribunal concluyó que los elementos presentados por la policía no eran suficientes para justificar la restricción de los derechos fundamentales del acusado, anulando así la sentencia y absolviendo al condenado.

Por otro lado, del análisis realizado por el Profesor de Derecho Procesal de la Universidad Pública de Navarra Manuel Richard González respecto a esta Sentencia absolutoria se puede interpretar que la instalación de dispositivos de seguimiento y localización (GPS) en vehículos dentro del marco de una investigación penal, como se regula en el artículo 588 quinquies b), genera una intervención en la privacidad que, aunque de menor intensidad que otros métodos investigativos, no deja de ser significativa. La privacidad, en tanto al derecho constitucional, presenta matices dependiendo del grado y tipo de intromisión que las herramientas tecnológicas permiten. Sin embargo, minimizar la intromisión gubernamental que implica el uso de un GPS podría llevar a trivializar una acción que afecta los derechos fundamentales de los ciudadanos.

En ciertos casos, conocer la ubicación exacta de una persona proporciona una ventaja estratégica a los investigadores sin implicaciones mayores; no obstante, pueden darse circunstancias en las que esta información permita revelar aspectos ideológicos o religiosos del investigado como la asistencia a actos políticos, la participación en ceremonias religiosas, la presencia en lugares de ocio que reflejen la orientación sexual, o la visita a centros médicos para tratamientos específicos son aspectos profundamente personales que podrían ser expuestos sin una protección adecuada contra el uso indebido de esta tecnología por parte del Estado.

¹⁷ RICHARD GONZÁLEZ, M., *Ilícitud de la prueba por falta de motivación del Auto de autorización judicial de un dispositivo de seguimiento GPS en el vehículo del sospechoso*, Diario La Ley, 9 de noviembre de 2020.

¹⁸ STS N° 141/2020, Sala de lo Penal, Sección 1, Rec 2749/2018 de 13 de mayo de 2020

Los fundamentos jurídicos que sustentan la sentencia respecto a la protección de la intimidad vienen reflejados en la jurisprudencia internacional y europea como la del Tribunal Europeo de Derechos Humanos, en la propia sentencia de absolución se referencian algunas resoluciones al respecto a continuación cito textualmente una amplia parte de la sentencia con el fin de entender los fundamentos en los que se basa dicha absolución: *“El legislador consideró necesario someter a autorización judicial la instalación de ese tipo de dispositivos, pese a que la jurisprudencia de esta Sala no caminaba de forma decidida en esa misma dirección. El debate acerca de la conveniencia de la habilitación judicial no era exclusivo de la dogmática ni de la jurisprudencia españolas. Puede ser suficiente en tal sentido la cita de la conocida sentencia del Tribunal Supremo americano de 23 de enero de 2012 -caso United States v. Antoine Jones, 565 US-. en la que, después de intensos debates que llevaron a lo que algún jurista ha llamado un esfuerzo argumental agónico, los Magistrados pudieron liberarse de la rígida singularidad del sistema constitucional americano que asocia la defensa de la privacidad a la del derecho de propiedad. Con una vocación eminentemente rupturista, el Tribunal Supremo americano consideró nula la prueba que había llevado a los agentes a la instalación de un GPS en el vehículo usado por el sospechoso declarando que esa diligencia de investigación menoscababa la privacidad del sospechoso y, por consiguiente, vulneraba la cuarta enmienda.*

La jurisprudencia del TEDH -sentencia 2 de septiembre de 2010, caso Uzun v. Alemania, incluyó en el contenido material del art. 8.1 del CEDH el derecho de todo ciudadano a mantener contacto con cualesquiera otras personas y a desarrollar relaciones personales sin ser sometido a innecesarias injerencias en su vida privada. Pese a ello, consideró que la legislación alemana, que no exige autorización judicial para la instalación de esos dispositivos, no vulneraba los principios del Convenio de Roma, siempre que se definan legalmente los presupuestos de limitación temporal y su adopción respete las exigencias del principio de proporcionalidad.

La Sala de lo Penal del Tribunal Supremo ha tenido ocasión de pronunciarse en varias ocasiones acerca de la legitimidad del empleo por los investigadores de este tipo de dispositivos. La ausencia de una cobertura normativa precisa y el uso ordinario en procedimientos penales para la investigación de delitos de especial gravedad ha venido condicionando la respuesta judicial al respecto.”

Si continuamos analizando las referencias jurídicas que alude el texto podemos observar las siguientes citadas también textualmente y en las que no solo permite la utilización de los medios de seguimiento, sino que no deja dudas de la legalidad de tales métodos al no vulnerar en estos casos el derecho a la intimidad:

“La STS 798/2013, 5 de noviembre, ante la alegada quiebra del derecho a la inviolabilidad de las comunicaciones por parte del recurrente -que invocaba en su favor la STEDH 2 de septiembre de 2010 (caso Uzun v. Alemania)-, descartó cualquier vulneración constitucional. Se trataba de la utilización de este tipo de instrumentos adoptada por iniciativa del Servicio de Vigilancia Aduanera para conocer la ubicación geográfica de un barco que portaba un importante cargamento de droga. La sentencia subraya la normalidad de la utilización de esas balizas y concluye: «...siendo así no se aprecia violación alguna del derecho a la intimidad. El uso de radiotransmisores (balizas de seguimiento GPS), para la localización de embarcaciones en alta mar por la policía no vulnera el derecho fundamental al secreto de las comunicaciones o supone una injerencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional. Para la Sala Segunda Tribunal Supremo la ausencia de relevancia constitucional se deriva de que se trata de 'diligencias de investigación legítimas desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiera en su derecho fundamental que requeriría la intervención judicial' (SSTs 22.6.2007 , 11.7.2008 , 19.12.2008), e incluso la sentencia TEDH citada en el recurso, caso Uzun c. Alemania de 2.9.2010, en un caso de intervención de una cabina telefónica habitualmente usada por un supuesto terrorista, si bien consideró que tal vigilancia a través del sistema GPS, y procesamiento de los datos obtenidos constituía una injerencia en la vida privada, art. 8 Convenio, también precisó que la vigilancia GPS, por su propia naturaleza debe distinguirse de otros métodos de seguimiento acústico o visual que, por regla general son más susceptibles de interferir en el derecho de la persona al respeto de su vida privada, porque revelan unas informaciones sobre la conducta de una persona, sus operaciones o sus sentimientos».

La STS 523/2008, 11 de julio, avaló la utilización de este tipo de dispositivos que, en el caso enjuiciado, habían sido adosados por agentes de policía a una embarcación. La equívoca invocación por la defensa del derecho a la inviolabilidad domiciliaria (art. 18.2 de la CE), facilitó el argumento mediante el que la Sala desestimó la alegada vulneración de derechos fundamentales: «...el submotivo 2 b) concierne a la vulneración del derecho a la 'intimidad de domicilio', reconocido en el art. 18.2 CE . Para lo que se aduce que en el puente del (buque) fue colocado por el SVA una baliza de seguimiento y localización. En primer lugar, no consta que para situar el artilugio fuera necesario entrar en algún recinto que constituyera un domicilio de los previstos en los arts. 554 o 561 LECrim . (...) Atendidos los documentos de los folios 3510 a 3515 y las declaraciones en el juicio oral de los funcionarios del SVA con números terminados en NUM001 y NUM002 respecto a la colocación exterior de la baliza en la magistral. Por otra parte, nada permite afirmar que la baliza fuera utilizada para clase alguna de injerencia en las conversaciones o mensajes de los investigados».

Similar desenfoque está en la base del discurso argumental mediante el que la defensa del recurrente intentó obtener la nulidad probatoria por la utilización de una baliza.

No han faltado precedentes que han desconectado el valor intrusivo de este tipo de dispositivos respecto del contenido material del derecho constitucional a la intimidad. Es el caso de la STS 562/2007, 22 de junio: «...en el segundo de los motivos de su oposición denuncian la vulneración de su derecho fundamental al proceso debido y a la intimidad que concretan en el hecho de haber colocado una baliza de seguimiento sin autorización judicial. La sentencia impugnada da respuesta a la pretensión deducida como motivo de casación con una argumentación que ha de ser reproducida para la desestimación del motivo. El artificio colocado permitió a los agentes de investigación el seguimiento por mar de la embarcación respecto a la que existían fundadas sospechas de su dedicación al tráfico de drogas. La colocación de esa baliza permitió realizar el seguimiento de la embarcación, ubicarla en alta mar y para su colocación, en los exteriores del barco, no se precisó ninguna injerencia en ámbitos de intimidad constitucionalmente protegidos. Se trata, en definitiva, de una diligencia de investigación, legítima desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiriera en un derecho fundamental que requeriría la intervención judicial».

La misma desconexión entre el uso de una baliza y el derecho a la intimidad, late en la argumentación de la STS 906/2008, 19 de diciembre. Esta resolución enfatiza el margen de error propio del sistema de localización a partir de los datos electrónicos asociados a una llamada telefónica. En su FJ 1º puede leerse lo siguiente: «...respecto de la utilización de herramientas electrónicas, sistema GPS, que pudieran producir injerencias, no autorizadas, en la intimidad del investigado, al permitir, entre otras utilidades, que fuera espacialmente ubicado, el propio Tribunal de instancia, con todo acierto, se encarga de replicar este extremo afirmando que, en efecto, podría asistirle la razón al recurrente si esa localización (SITEL o Sistema de Intervención Telefónica) permitiera conocer el lugar exacto en el que el comunicante se encontraba, pero que, cuando como en este caso, esa ubicación sólo puede concretarse con una aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal, en modo alguno puede considerarse afectado, al menos de forma relevante, el derecho a la intimidad del sometido a la práctica de la diligencia».”

4.2 Análisis de Sentencia Penal Nº 329/2016, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec 1789/2015 de 20 de abril de 2016 sobre el derecho a la inviolabilidad del domicilio (art. 18.2 ce). Observación por agentes de policía del interior de un domicilio mediante prismáticos.

Como introducción a la STS 329/2016 podemos observar como el Tribunal Supremo revocó la sentencia condenatoria de la Audiencia Provincial de Ourense, que había condenado a dos acusados tras la intervención de un alijo de drogas. La intervención se originó a partir de una vigilancia no autorizada del domicilio de uno de los acusados, realizada desde la vivienda de un agente de policía, utilizando prismáticos para observar el interior de la vivienda sin obstáculos, de modo que cuando los agentes presenciaron la entrega de una bolsa con drogas y, tras el posterior desplazamiento de uno de los acusados, procedieron a su detención.¹⁹

¹⁹ STS, Sala Segunda, de lo Penal, Sentencia 329/2016 de 20 de abril de 2016, Rec. 1789/2015 (LA LEY 32932/2016).

La Audiencia Provincial fundamentó su decisión en la ausencia de intromisión ilegítima en el ámbito de la intimidad, argumentando que la observación fue posible debido a que los moradores no establecieron obstáculos que impidieran la visión del interior del domicilio, considerando esto una autorización implícita para la observación si bien, el Tribunal Supremo anuló la prueba obtenida al entender que la intervención vulneró el derecho a la intimidad domiciliaria, establecido en el artículo 18.2 de la Constitución Española. El propio Tribunal destacó que el uso de medios técnicos, como prismáticos, para observar el interior del domicilio sin autorización judicial no puede ser justificado, incluso si los moradores no cierran las ventanas y además, subrayó que la utilización de estos instrumentos constituye una intromisión en el derecho fundamental a la inviolabilidad del domicilio, que no puede depender de la voluntad del morador de cerrar o no las ventanas. Asimismo, el Tribunal Supremo citó la Ley Orgánica 4/1997, que prohíbe el uso de videocámaras para grabar imágenes o sonidos en el interior de viviendas sin el consentimiento del titular o una autorización judicial, reafirmando la protección constitucional del derecho a la intimidad.

De forma resumida, de la misma STS actuando como ponente D. Manuel Marchena Gómez se desprende que el derecho a la inviolabilidad del domicilio, protegido por el artículo 18.2 de la Constitución Española no ha sido ampliamente abordado por la jurisprudencia en relación con el uso de prismáticos por parte de agentes de policía para observar el interior de una vivienda. Aunque existen algunos precedentes, estos se centran principalmente en la suficiencia de pruebas cuando, mediante prismáticos, se observa un delito cometido en lugares públicos a gran distancia.²⁰

El derecho a la inviolabilidad domiciliaria no se ve anulado por el hecho de que el propietario o usuario de la vivienda no haya tomado medidas para bloquear la visibilidad desde el exterior, como cerrar las cortinas. El hecho de que las cortinas o persianas no estén cerradas no debe interpretarse como una autorización tácita para que el interior sea observado, ya que este tipo de interpretación podría debilitar gravemente la protección constitucional del domicilio.

²⁰ MARCHENA GÓMEZ, M., "Nulidad de la prueba por la intromisión virtual en domicilio. Una breve reflexión sobre la observación policial ilícita de la intimidad personal y familiar", Diario La Ley, Nº 8788, 22 de junio de 2016.

En esta ocasión, conforme al análisis realizado por D. Manuel Richard González, éste define la intromisión virtual como aquella injerencia en el domicilio que se produce a distancia sin procederse a la entrada material en el mismo y que permite observar lo que allí acaece sin el consentimiento de sus titulares, pero igualmente invasiva en comparación con la intromisión física y al mismo tiempo imperceptible también lo que podría causar indefensión, a continuación cito textualmente en palabras de Don Manuel Richard González *“la intromisión virtual puede tener lugar mediante el simple uso de los sentidos y consistir en la mera observación a más o menos distancia de lo que sucede en el domicilio ajeno viendo y/u oyendo lo que allí acaece. La observación puede facilitarse por la ausencia de cortinas, ventanas, toldos, vallas o cualquier otra clase de elemento de los usuales que contribuyen a delimitar el espacio íntimo de protección en el que se desarrolla la vida personal y familiar. También cabe la posibilidad de que el observador emplee medios técnicos que permitan la observación e incluso la grabación a distancia de imagen y sonido provenientes del interior del domicilio protegido. Entre estos artefactos se hallan los teleobjetivos fotográficos, dispositivos direccionales de grabación de sonido, prismáticos o telescopios o también drones provistos de aparatos de captación de imágenes y sonido.”*²¹

En el análisis realizado por el Profesor D. Manuel Richard González está de acuerdo en que el Tribunal Supremo declarara ilícita la prueba obtenida por la policía mediante la observación con prismáticos del interior del domicilio de los acusados, sin consentimiento ni autorización judicial, si bien la sentencia protege el derecho a la intimidad en el ámbito domiciliario recogido en el artículo 18.2 de la Constitución Española y subraya que no se puede vulnerar este derecho utilizando medios técnicos para observar clandestinamente el interior de una vivienda.

²¹ RICHARD GONZÁLEZ, M., *"Nulidad de la prueba por la intromisión virtual en domicilio"*, Diario La Ley, Nº 8788, 22 de junio de 2016.

Sin embargo, la reflexión final sostiene que el Tribunal Supremo, al condicionar la ilicitud de la prueba al uso de medios técnicos como los prismáticos podría estar restringiendo innecesariamente la protección del derecho a la intimidad. El autor de la reflexión considera que la cuestión de la ilicitud no debería depender exclusivamente del uso de tecnología, sino del hecho mismo de la intromisión en el ámbito privado del domicilio, independientemente de si se utilizan o no dispositivos técnicos, en otras palabras, la observación sin consentimiento de una vivienda, aunque no se utilicen medios técnicos, debería considerarse igualmente una vulneración de la intimidad y por lo tanto la prueba obtenida debería ser declarada ilícita.

Para ilustrar este argumento, se presentan ejemplos prácticos que muestran cómo la simple intromisión en la vida privada, sin el cumplimiento de los requisitos del artículo 18.2 de la Constitución (flagrancia, consentimiento o autorización judicial), debe ser considerada ilícita. Por ejemplo, si un policía observa la comisión de un delito desde la vía pública sin la necesidad de hacer un esfuerzo adicional, la prueba obtenida es lícita, pero si el mismo policía se coloca en una posición de observación que invada la intimidad del domicilio sin cumplir los requisitos legales, la prueba debe ser considerada ilícita, aunque no se empleen dispositivos técnicos.

El autor concluye que el Tribunal Supremo debería adoptar una postura más amplia y garantizar la inviolabilidad del domicilio y la intimidad personal, independientemente de la utilización de tecnologías o de la existencia de obstáculos físicos evitando así que las autoridades obtengan pruebas de manera ilícita mediante la simple injerencia en la vida privada de los ciudadanos sin las debidas garantías legales.

5. Medidas de seguridad en la actualidad

Vigilancia masiva

Una de las definiciones que podemos encontrar sobre la vigilancia masiva la describe David Nel (2022) como *“el control indiscriminado de las comunicaciones por Internet y telefónicas de un gran número de personas sin que existan indicios suficientes de conducta delictiva”* diferenciándola además de la simple vigilancia *“Seguimiento de las comunicaciones o movimientos de un individuo u organización por parte de un gobierno, grupo o persona.”* Según comenta el autor la vigilancia puede ser legal o ilegal, mientras que la vigilancia masiva siempre se considera ilegal. Sin embargo, esto genera un debate sobre los límites legales y éticos de la vigilancia²². Según las leyes internacionales de derechos humanos, la vigilancia debe estar respaldada por una autorización judicial y estar dirigida a objetivos específicos, como en casos de amenaza terrorista o peligro para el orden público. Sin embargo, organizaciones como Amnistía Internacional argumentan que las amenazas no deberían ser una justificación suficiente para violar los derechos a la privacidad y la presunción de inocencia. Muchos en Occidente comparten esta visión, creyendo que los gobiernos deben equilibrar la seguridad con el respeto a los derechos individuales en un estado de derecho.

Una tendencia emergente en el campo de la vigilancia masiva es el creciente uso de tecnologías de inteligencia artificial (IA) y análisis de Big Data para mejorar la capacidad de recopilación y análisis de información. Estas tecnologías están revolucionando la forma en que los sistemas de vigilancia operan, permitiendo a los Gobiernos obtener y procesar grandes volúmenes de datos de manera más rápida, eficiente y precisa que nunca antes.

²² NEL, D., *La vigilancia masiva en el futuro*, David Nel, 15 de agosto de 2022.

Con la proliferación de datos digitales en todas las facetas de la vida moderna, desde las redes sociales hasta las transacciones financieras, los Gobiernos y las empresas están aprovechando estas tecnologías avanzadas para identificar patrones, tendencias y relaciones ocultas en conjuntos de datos masivos. Esto les permite detectar amenazas potenciales, prever comportamientos futuros y tomar decisiones basadas en datos de manera más informada. Además, la expansión de la vigilancia masiva se está acelerando con la proliferación de dispositivos de Internet de las cosas (IoT). Desde cámaras de seguridad y sensores hasta dispositivos inteligentes en hogares y ciudades, estos dispositivos recopilan constantemente datos sobre el comportamiento y las actividades de las personas. Esto amplía aún más el alcance de la vigilancia masiva en la vida cotidiana, generando enormes cantidades de datos que pueden ser utilizados para diversos fines como la toma de decisiones políticas y el control social.

El hecho de que se estén explorando nuevas formas de colaboración entre gobiernos y empresas privadas para compartir datos y mejorar la vigilancia plantea interrogantes sobre la privacidad y la protección de datos, así como sobre el equilibrio entre la seguridad y las libertades individuales en una sociedad cada vez más digitalizada y conectada.

Breve referencia a la Ley de Servicios Digitales

En el marco de la UE recientemente se ha elaborado la Ley de Servicios Digitales²³ que establece reglas para plataformas y mercados en línea, protegiendo los derechos de los usuarios y promoviendo un mercado único en la UE. Desde su entrada en vigor en noviembre de 2022, la Ley ha introducido una serie de obligaciones para los intermediarios, como combatir el contenido ilícito en línea y rastrear a los vendedores en los mercados en línea para prevenir estafas.

²³ PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA, *Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales (Ley de Servicios Digitales)*, Diario Oficial de la Unión Europea, L 277, 27 de octubre de 2022, pp. 1-102.

Además, se han implementado medidas para salvaguardar a los usuarios, incluido el derecho a impugnar decisiones de moderación de contenidos. La transparencia también es clave, con nuevas normas para las plataformas en línea sobre condiciones y algoritmos de recomendación de contenidos. Se han establecido protecciones adicionales para los menores y se prohíbe la publicidad personalizada basada en perfiles de niños. La Ley también aborda la manipulación de usuarios y garantiza el acceso de investigadores a datos clave. Los usuarios ahora tienen derechos ampliados, incluida la posibilidad de buscar acuerdos extrajudiciales y reclamar indemnizaciones por incumplimientos. La Comisión supervisa las plataformas más grandes, mientras que los Estados miembros supervisan otras.

Acceso gubernamental a datos personales

Recientemente la Organización para la Cooperación y Desarrollo Económico (OCDE) ha realizado la Declaración sobre el Acceso de los Gobiernos a los Datos Personales²⁴ estableciendo los Principios rectores del acceso de los gobiernos a los datos personales en poder de entidades del sector privado proponiendo que el acceso gubernamental a datos personales esté regulado por el marco legal de cada país, que debe ser vinculante para las autoridades gubernamentales. Establece además los propósitos, condiciones y límites del acceso, garantizando salvaguardias para proteger contra el uso indebido y el abuso. Siendo el objetivo legítimo del acceso gubernamental contribuir a objetivos específicos, como la seguridad nacional o el mantenimiento del orden público, y se debe llevar a cabo de manera proporcionada y conforme al Estado de derecho.

Se establecen también los requisitos de aprobación para garantizar que el acceso cumpla con las normas legales y se documenten las decisiones relacionadas con la aprobación. Además, se aplican medidas de tratamiento de datos para mantener la privacidad, seguridad y confidencialidad de la información.

²⁴ ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (OCDE), *Declaración sobre el Acceso de los Gobiernos a los Datos Personales en poder de las entidades del sector privado*, 2023.

Según estos Principios la transparencia es fundamental en el acceso gubernamental a los datos, con mecanismos para informar al público sobre las solicitudes de acceso y el cumplimiento de los requisitos legales. La supervisión efectiva garantiza que el acceso se realice de manera adecuada, y se proporcionan medios de reparación para las personas afectadas por infracciones del marco legal, por ejemplo, pueden incluir la supresión de datos, el restablecimiento de la integridad de la información y compensaciones por daños y perjuicios.

En resumen, parece que el acceso que los gobiernos tienen a datos personales está regulado o debe estar regulado por marcos legales que definen sus propósitos, condiciones y límites garantizando la protección de los derechos individuales frente a posibles abusos en el manejo de la información por parte de los Estados. Los objetivos legítimos de este acceso suelen estar vinculados con la seguridad nacional, el cumplimiento de la ley, la protección del orden público y la lucha contra el terrorismo.

La aprobación previa es un requisito común en estos marcos, asegurando que el acceso se realice de manera adecuada y proporcional requiriendo en algunos casos la autorización de autoridades judiciales o no judiciales imparciales, especialmente en situaciones que implican una mayor intrusión en la privacidad.

El tratamiento de los datos obtenidos debe realizarse de manera segura y legal, cumpliendo con las disposiciones establecidas y protegiendo la confidencialidad de la información. Se deben aplicar medidas técnicas, físicas y administrativas para garantizar la seguridad y la integridad de los datos.

La transparencia y la supervisión son aspectos clave en este proceso. Los marcos legales deben ser claros y accesibles para el público, y se deben establecer mecanismos efectivos para supervisar el cumplimiento de las regulaciones.

Por otro lado, como veremos a continuación, en relación a los Principios expuestos anteriormente existen varios tipos de programas especializados en recopilación masiva de datos y análisis utilizados por los Gobiernos para la administración de la seguridad, que generan algunas controversias en cuanto a la concordancia con esos principios de transparencia descritos anteriormente.

El **Sistema de Intercepción de Comunicaciones XKEYSCORE**²⁵ utilizado por la Agencia de Seguridad Nacional (NSA) de los Estados Unidos que permite la interceptación y monitoreo de comunicaciones electrónicas, como llamadas telefónicas, correos electrónicos, mensajes de texto y chats en línea, es un sistema de vigilancia masiva que permite a la NSA recopilar y analizar grandes cantidades de datos de comunicaciones electrónicas, incluidos correos electrónicos, chats en línea, historiales de navegación web y más, sin necesidad de una orden judicial específica.

Desde una perspectiva de privacidad y derechos de intimidad, plantea serias dudas sobre el mantenimiento del derecho a la intimidad de las personas, aunque por otro lado se puede argumentar que este tipo de vigilancia puede ser necesaria para la seguridad y la prevención del terrorismo.

Otro de los programas que podemos referenciar como una de las herramientas de vigilancia y recopilación de datos es el **Software de Monitoreo de Redes Sociales PRISM** que sirve para rastrear y monitorear la actividad en línea, incluido el tráfico web, la navegación y el uso de aplicaciones, para identificar amenazas cibernéticas y actividades sospechosas recopilando datos de servicios en línea como Google, Facebook y Microsoft entre otras, ha sido muy criticado por la opinión pública por carecer de las garantías para garantizar la privacidad de las personas, en el análisis que elaboró Elena Contreras Saura (2022) en la revista Sec2Crime²⁶ expone que las revelaciones sobre PRISM, conocido como "El caso Snowden"²⁷ continúan generando controversia en la actualidad. Fue un punto de inflexión que indignó a los ciudadanos estadounidenses al descubrir que una Agencia de Inteligencia recopilaba datos de sus propios ciudadanos, en violación de las leyes, argumentando la necesidad de sacrificar privacidad por seguridad, lo que cambió la percepción sobre la privacidad digital y la confianza en empresas de seguridad.

²⁵ GREENWALD, G., *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, 7 de junio de 2013.

²⁶ SAURA, E. C., *¿Qué es el programa PRISM y cómo se filtró?*, Sec2Crime, 29 de agosto de 2023.

²⁷ GREENWALD, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Metropolitan Books, 2014.

Reconocimiento biométrico

Resulta muy interesante conocer como los avances tecnológicos pueden llegar a individualizar de manera inequívoca a cada una de las personas que habitamos en este planeta con los sistemas de reconocimiento facial o incluso, como recientemente se ha comprobado, también con el reconocimiento del iris, estos sistemas utilizan algoritmos de reconocimiento para identificar y rastrear personas a través de imágenes y videos. Se trata de identificar de forma biométrica a las personas, aunque para esta identificación es necesario disponer de una imagen, vídeo o datos biométricos de forma previa, en cualquier caso, es una medida de seguridad muy eficiente en contra de la delincuencia o el terrorismo, pero al mismo tiempo ejerce un control sobre los movimientos de las personas que supera con creces el anonimato y la libertad de movimientos al que la sociedad en general está acostumbrada.

Como ya se ha mencionado anteriormente para la identificación individual a través de los datos biométricos se ha de disponer previamente de esa biometría de forma indubitada en las bases de datos utilizadas, recientemente empresas como OpenAI²⁸ han llevado a cabo campañas de recopilación de datos biométricos del iris poniendo en alerta a varios países entre los que se encuentra precisamente el nuestro, que ha llegado a prohibir tal práctica por temor a la mala praxis en la utilización de esos datos.

Por otro lado, la empresa norteamericana Clearview AI, proporciona un software de reconocimiento facial utilizado por algunos Gobiernos de varios países. En el Artículo de la revista La Voz de Galicia realizado por Carlos Manuel Sánchez expone que Clearview AI²⁹ mantiene una colosal base de datos que actualmente cuenta con 30.000 millones de imágenes y sigue expandiéndose. La empresa comenzó este proyecto en secreto en el año 2017 y desde entonces ha incrementado su base de datos con todas las imágenes que ha podido recolectar de Internet.

²⁸ PEIRANO, M., *Por qué Sam Altman quiere escanear dos mil millones de ojos*, El País, 22 de agosto de 2023.

²⁹ MANUEL SÁNCHEZ, C., *Clearview, la polémica app que nos controla*, La Voz de Galicia, XL Semanal, abril de 2024.

En esta plataforma, que opera sin restricciones ni supervisión, se encuentran los valiosos datos biométricos de los rostros de cientos de millones de personas en todo el mundo. Es posible que nuestro rostro también esté incluido. Incluso si se trata de una foto o video de nuestras redes sociales, aunque se encuentre borroso, en un ambiente oscuro o rodeado de otras personas, la inteligencia artificial (IA) habrá registrado nuestros rasgos y podrá identificarnos para compararnos con las imágenes captadas por cámaras de vigilancia en una gasolinera o un cajero automático durante una investigación.

Abordando el tema que motiva el presente estudio, la recopilación masiva de datos biométricos por parte de Clearview AI, sin el consentimiento ni supervisión adecuada, plantea una seria amenaza a la privacidad de los individuos. Al crear una base de datos gigantesca con imágenes de rostros obtenidas de internet, la empresa permite que millones de personas sean potencialmente identificadas y rastreadas sin su conocimiento ni aprobación.

Este enfoque erosiona significativamente el derecho a la intimidad, ya que convierte a cualquier persona en un posible objetivo de vigilancia. Al catalogar y almacenar estas imágenes, Clearview AI elimina el control de los individuos sobre su información personal y como ya se mencionó anteriormente incluso imágenes borrosas o capturadas en condiciones de poca luz pueden ser procesadas y utilizadas para identificaciones de todo tipo de personas, que pueden ser catalogadas como amenazas pero también como personas normales de una sociedad moderna en la que parece que hemos perdido una cierta capacidad de movimientos sin exponernos a un cierto control. La capacidad de mantener la privacidad de nuestros movimientos y acciones cotidianas se ve severamente comprometida y la invasión de la privacidad se hace presente en una era donde el derecho a la intimidad debería estar bien defendido.

La falta de transparencia y regulación en el uso de estos datos por parte de empresas como Clearview AI expone a los ciudadanos a un nivel de vigilancia sin precedentes, donde cada acción puede ser monitoreada y registrada sin su consentimiento, lo que podría estar erosionando así uno de los derechos humanos fundamentales como el derecho a la intimidad en aras de mantener un cierto nivel de seguridad.

Big Data: Recopilación masiva de datos, la inteligencia artificial y el análisis predictivo

Thomas Hobbes lo reflejó en su obra *Leviatán*³⁰ con la frase: "*Quien tiene la información tiene el poder*" pero en la reflexión que practica el Abogado Ricardo Martínez Barros pregunta ¿Quién controla realmente la información? ¿El poder?³¹ A menudo parece que "*quien tiene el poder tiene la información*". Los medios de comunicación, actuando como intermediarios, transmiten la información proporcionada por el Gobierno en sus diversas formas: política, económica y religiosa. En este sentido podemos reflexionar también sobre la vulneración de la intimidad que se puede perder en aras de mantener esa perseguida seguridad, en los últimos tiempos como en otras ocasiones el avance de la tecnología y la Inteligencia Artificial nos brinda también la posibilidad de analizar tal cantidad de datos tan abrumadora que cuesta entender la magnitud de la misma.

Como ya se ha mencionado anteriormente actualmente existen softwares de análisis de datos que se utilizan para analizar grandes volúmenes de datos y extraer información relevante para investigaciones de seguridad y aplicaciones de inteligencia, desempeñan un papel importantísimo en las estrategias de seguridad antiterrorista y de seguridad nacional al permitir a los Estados recopilar, analizar y actuar sobre grandes volúmenes de datos para prevenir y responder a todo tipo de amenazas pero al mismo tiempo también plantea importantes consideraciones éticas y de privacidad que deben considerarse para garantizar el equilibrio entre la seguridad y las libertades individuales³².

Una de las empresas pioneras en el análisis de macrodatos es "Palantir Technologies" es una empresa de tecnología estadounidense fundada en 2003 por Peter Thiel, Alex Karp, Joe Lonsdale, Stephen Cohen y Nathan Gettings.

³⁰ HOBBS, T., *Leviatán (Extractos)*, 1859.

³¹ MARTÍNEZ BARROS, R., "*¿Quién controla realmente la información?*", *Revista de Derecho y Tecnología*, 8(2), 2023, pp. 45-59.

³² SMITH, J., "*The Impact of Big Data on Privacy and Security*", *Journal of Data Protection*, 15(3), 2022, pp. 123-145.

La empresa se especializa en análisis de datos, minería de datos y análisis de Big Data para diversas aplicaciones, incluida la inteligencia artificial, la seguridad nacional, la ciberseguridad, la salud, las finanzas y otras áreas, su software “Palantir”, que lleva el mismo nombre que la empresa, se utiliza principalmente para integrar, visualizar y analizar grandes conjuntos de datos para ayudar a las organizaciones a tomar decisiones informadas. Entre los clientes de Palantir se encuentran los servicios de seguridad de algunos Gobiernos, instituciones financieras, empresas de atención médica y otras organizaciones en todo el mundo. Sin embargo, Palantir también ha sido objeto de controversia debido a sus contratos con agencias de inteligencia y aplicación de la ley, lo que ha planteado preocupaciones sobre la privacidad y el potencial uso indebido de los datos.

En la publicación de Europapress del pasado 16 de octubre 2023 se anuncia que el Ministerio de Defensa ha otorgado a la filial española de Palantir Technologies³³, conocida por sus vínculos con la CIA y el Pentágono, un contrato de 20 millones de euros para proporcionar una solución de fusión y análisis de inteligencia para el Sistema de Inteligencia de las Fuerzas Armadas (SIFAS). La empresa, fundada por el controvertido Peter Thiel, se encargará de esta tarea clave en el ámbito de la seguridad nacional. Según Europapress Palantir ha sido criticada por usar grandes cantidades de datos y en otras ocasiones ha sido acusada de que sus algoritmos poseían prejuicios raciales.

La metodología empleada para la recopilación y análisis de datos se puede simplificar en:

- Detección de patrones: Identificación de patrones y comportamientos anómalos que podrían indicar actividades delictivas o terroristas. Esto incluye la vigilancia de comunicaciones electrónicas, movimientos financieros sospechosos y actividades en redes sociales.
- Análisis de redes: Permite analizar las conexiones entre individuos y organizaciones del crimen organizado para identificar líderes, células terroristas y nexos financieros. Esto ayuda a dismantelar redes terroristas y prevenir ataques.

³³ EUROPAPRESS, *El Ministerio de Defensa adjudica un contrato a Palantir para el Sistema de Inteligencia de las Fuerzas Armadas*, Europapress, 16 de octubre de 2023.

Identificación de amenazas emergentes: Mediante el análisis de datos en tiempo real de fuentes como redes sociales, foros en línea y medios de comunicación, los Gobiernos pueden identificar rápidamente amenazas emergentes y potenciales.

- Vigilancia fronteriza: El análisis de big data se utiliza en la vigilancia fronteriza para identificar posibles ataques y otros individuos peligrosos que intentan ingresar al país. Esto incluye el análisis de datos de pasaportes, visas y listas de vigilancia.
- Respuesta a emergencias: Durante crisis de seguridad el análisis de macrodatos facilita la coordinación y la respuesta rápida de las agencias de seguridad y los equipos de respuesta de emergencia. Esto incluye el análisis de datos de ubicación en tiempo real para dirigir los esfuerzos de rescate y la evaluación de la situación.

En definitiva, la inteligencia artificial (IA) ha transformado significativamente el ámbito de la seguridad, proporcionando herramientas avanzadas para prevenir y responder a amenazas. Sin embargo, su implementación puede plantear serias preocupaciones respecto a la privacidad y el derecho a la intimidad.

En situaciones de emergencia, la IA puede procesar datos rápidamente para ofrecer información crítica a las fuerzas de seguridad, lo que permite tener una respuesta más eficaz y coordinada, reduciendo el tiempo de reacción y potencialmente salvando vidas, de hecho, los Gobiernos de todo el mundo están adoptando tecnologías de IA para proteger infraestructuras críticas y monitorear actividades sospechosas a nivel nacional e internacional, la IA ayuda a analizar datos de inteligencia para detectar amenazas potenciales y planificar estrategias de defensa. Al mismo tiempo la Inteligencia Artificial potencia las capacidades de los Gobiernos para la vigilancia masiva, permitiendo la monitorización constante de individuos y poblaciones enteras. Por otro lado, requieren el acceso a grandes cantidades de datos personales e información como la obtenida de redes sociales, comunicaciones digitales, y registros financieros, lo que plantea riesgos en el uso indebido de estos datos.

Como uno de los factores negativos que podemos encontrar en la utilización de la Inteligencia Artificial por parte de los Gobiernos podría ser la posible discriminación a ciertos grupos demográficos ya que en caso de utilizar bases de datos existentes erróneas los algoritmos pueden perpetuar sesgos existentes en los datos y llevar a cabo prácticas

de vigilancia de forma injusta y también, dada la complejidad de la Inteligencia Artificial y su opacidad pueden dificultar la rendición de cuentas y la supervisión. Los ciudadanos a menudo no tienen control sobre cómo se recopilan, almacenan y utilizan sus datos, lo que erosiona el derecho a la intimidad.

En el ámbito de la Inteligencia Artificial podemos destacar a **Dataminr** como una empresa de tecnología que utiliza inteligencia artificial (IA) para analizar grandes volúmenes de datos en tiempo real, proporcionando alertas e información relevante para diversos sectores, incluyendo la seguridad, la gestión de emergencias, y las noticias. Fundada en 2009, Dataminr ha desarrollado una plataforma que se especializa en detectar eventos significativos y tendencias emergentes a partir de múltiples fuentes de datos, tales como redes sociales, blogs, sitios de noticias, y otros canales públicos. La plataforma recopila y analiza una gran cantidad de información pública, lo que puede incluir datos personales compartidos en redes sociales y otras plataformas. Si bien Dataminr se enfoca en datos accesibles públicamente, la magnitud y el alcance de su análisis pueden suscitar inquietudes sobre la privacidad y la protección de la información personal.

En resumen, el Big Data es una herramienta poderosa en la protección de la seguridad nacional al proporcionar a los Gobiernos la capacidad de recopilar, analizar y actuar sobre grandes volúmenes de datos para prevenir amenazas, proteger infraestructuras críticas y responder eficazmente a emergencias y crisis de seguridad. Sin embargo, su uso plantea importantes consideraciones éticas y de privacidad que deben ser estudiadas para garantizar un equilibrio adecuado entre la seguridad y el derecho a la intimidad.

6. Impacto social, psicológico y medidas de protección

Impacto social

El uso de la inteligencia artificial (IA) para fines de seguridad, es sin duda una medida muy positiva para proteger a la sociedad y a los Estados de posibles ataques terroristas, crimen organizado o crisis de seguridad de todo tipo, no solo en el contexto bélico o delincriminal, también en una posible crisis sanitaria o social, pero también tiene un profundo impacto social y psicológico en los individuos y en la sociedad en general debido a la pérdida de intimidad que puede suponer la implantación institucional de este tipo de tecnologías y puede generar diversas consecuencias.

Por un lado es evidente que en el ámbito de la Seguridad Pública la IA ha mejorado la eficiencia de las fuerzas de seguridad mediante el análisis de grandes volúmenes de datos en tiempo real, permitiendo la detección temprana de actividades sospechosas y la prevención de delitos, herramientas como el reconocimiento facial, la vigilancia predictiva y el análisis de redes sociales han potenciado la capacidad de las autoridades para responder rápidamente a amenazas y esto ha llevado a una mayor sensación de seguridad entre los ciudadanos, quienes pueden beneficiarse de un aumento en su seguridad o una reducción en la tasa de criminalidad y una respuesta más eficaz ante emergencias pero la pérdida de privacidad que genera el uso intensivo de tecnologías de vigilancia basadas en IA ha suscitado desconfianza entre la ciudadanía, estos sistemas de reconocimiento facial, cámaras de vigilancia inteligentes y análisis de datos personales pueden recolectar información detallada sobre las actividades diarias de las personas sin su consentimiento explícito y esta intrusión en la vida privada puede llevar a un sentimiento de constante vigilancia y a reducir la libertad de las personas para moverse y expresarse sin temor a ser observadas o registradas³⁴.

Por otro lado, como ya se ha dicho anteriormente las tecnologías de IA no están exentas de sesgos inherentes, los cuales pueden derivar en prácticas discriminatorias y que pueden discriminar a individuos o grupos específicos, basándose en datos y algoritmos que reflejan prejuicios existentes e incluso puede dar como resultado una vigilancia desproporcionada de ciertas comunidades favoreciendo la injusticia y la desigualdad³⁵.

El uso por parte del Gobierno de tecnologías de vigilancia sin suficiente transparencia o supervisión puede erosionar la confianza pública en el Gobierno y las Instituciones haciendo que los ciudadanos se puedan sentir recelosos de su propia intimidad si perciben que sus datos personales se utilizan de manera inapropiada o sin las debidas garantías de privacidad y la falta de confianza puede llevar a una disminución en la cooperación con las autoridades y una mayor “resistencia” a las políticas de seguridad.

³⁴ CRAWFORD, K., *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021.

³⁵ EUBANKS, V., *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, 2018.

Impacto psicológico

El contante cambio al que la sociedad está expuesta puede tener consecuencias psicológicas que van más allá del estrés y la ansiedad, si a esto le sumamos las características inherentes de la utilización de este tipo de tecnologías tan avanzadas pueden acrecentar algunos factores psicológicos negativos como la sensación de vigilancia constante, que viene influenciada por el conocimiento de que la Inteligencia Artificial puede monitorear y analizar prácticamente todos los aspectos de la vida cotidiana de la ciudadanía provocando esta sensación de vigilancia constante y que puede llevar a una disminución del sentimiento de privacidad afectando a la comodidad y libertad con la que las personas realizan sus actividades diarias. Concretamente en el aspecto psicológico la constante vigilancia y la falta de privacidad pueden aumentar los niveles de estrés y ansiedad provocando además que las personas puedan sentirse incómodas y preocupadas por la posibilidad de que sus datos personales sean mal utilizados o caigan en manos equivocadas. La incertidumbre sobre cómo se utilizan sus datos y quién tiene acceso a ellos puede ser una fuente constante de preocupación favoreciendo que las personas puedan volverse más reservadas y eviten expresarse libremente o provocar que modifiquen sus hábitos para evitar ser monitorizadas y este cambio de comportamiento puede afectar negativamente las relaciones interpersonales y la creatividad³⁶.

En resumen, la utilización de la inteligencia artificial para la seguridad puede traer consigo una serie de efectos psicológicos adversos debido a la pérdida de intimidad. Desde la sensación de vigilancia constante hasta la desconfianza en las instituciones, estos impactos pueden afectar profundamente el bienestar emocional y psicológico de las personas, alterando la forma en que se comportan, interactúan y se perciben a sí mismas.

³⁶ SOLOVE, D. J., *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, 2004.

Medidas de protección

Encontrar un equilibrio entre la mejora o el mantenimiento de la seguridad utilizando la tecnología moderna, la inteligencia artificial (IA) u otros sistemas de vigilancia masiva sin menoscabar el derecho a la intimidad de las personas es un desafío actual en esta sociedad moderna que ve como a medida que las tecnologías avanzan, la capacidad de los Gobiernos para analizar y utilizar datos personales se ha incrementado exponencialmente. Esta situación plantea serias preocupaciones sobre cómo garantizar que el uso de IA no comprometa los derechos fundamentales de las personas a la privacidad y la intimidad por lo que se deben implantar estrategias y medidas para proteger a los ciudadanos de unas injerencias inadecuadas, pero al mismo tiempo no podemos perder de vista la protección y seguridad de la ciudadanía que es tan importante como lo anterior. En relación a ello se proponen algunas medidas que podrían servir para este fin de mantener una seguridad adecuada por encima de todo, pero sin perder la identidad de un país democrático y de derecho como el nuestro:

En primer lugar, podemos distinguir uno de los puntos más importantes tratándose de una correcta regulación de las normas y una legislación adecuada. Establecer unos marcos legales claros que regulen el uso de los datos que se utilizan para proteger debidamente a la sociedad en el ámbito de la seguridad y que al mismo tiempo protejan los derechos de privacidad definiendo los límites en la recopilación de datos.

Otro de los puntos importantes que podemos implementar de forma correcta en el mantenimiento de la seguridad es la transparencia en cómo el Estado utiliza los datos, informar a la ciudadanía sobre cómo funcionan los sistemas de recopilación y tratamiento de esos datos, tal vez no de forma explícita y concreta pero sí de forma genérica los ciudadanos tienen derecho a conocer que tipos de sistemas poseen y tratan los datos personales y de qué forma están utilizando los mismos. Esto es esencial para fomentar la confianza de la sociedad y facilitar a los usuarios el poder para tomar decisiones sobre el uso de sus datos³⁷.

³⁷ ZUBOFF, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019.

Para ser verdaderamente transparentes, los Gobiernos deben proporcionar políticas de privacidad claras y accesibles, evitar el lenguaje técnico o legal complejo, ofrecer explicaciones sobre el funcionamiento de los algoritmos y mantener a los usuarios informados sobre cualquier cambio en el uso de sus datos. Además de la transparencia, es importante el hecho de que la utilización de esos datos en aras de la seguridad debe estar acompañado de una responsabilidad por parte del personal a cargo de la administración de esos datos, implicando que las Instituciones deban rendir cuentas en caso de una vulneración excesiva en la privacidad y el derecho a la intimidad de las personas. Para ello se deben realizar evaluaciones de impacto en la privacidad antes de implementar sistemas de IA, establecer mecanismos de supervisión y auditoría, tener planes claros para responder a violaciones de datos y recoger y considerar el feedback de los usuarios.³⁸

Por otro lado, se deben desarrollar y adoptar tecnologías que incorporen principios de privacidad desde el diseño, como la utilización de datos anónimos de forma general salvo amenaza real o el uso de sistemas de almacenamiento y uso de datos que minimicen la recopilación de información personal o Sistemas de Identificación Descentralizada que Implementen sistemas de identidad digital descentralizada que permitan a los usuarios tener control sobre sus datos personales. En definitiva, podemos ayudarnos de la tecnología para utilizar precisamente esa tecnología de forma adecuada y mantener la seguridad óptima con un adecuado mantenimiento de los derechos en general.

Por último y no menos importante no podemos despreocuparnos y dejar en manos ajenas aspectos tan importantes como la seguridad o los derechos de los ciudadanos sin un mínimo de participación y por eso la Participación Ciudadana en ámbitos tan importantes como estos podrían ayudar a mantener los límites en ambos sentidos. El hecho de que la sociedad se involucre en el debate sobre el uso de datos personales respecto al incremento o mantenimiento de la seguridad o incluso de la propia seguridad asegurando que las políticas reflejen un consenso social y respeten los derechos fundamentales es algo verdaderamente importante para cumplir con los objetivos descritos³⁹.

³⁸ ANGWIN, J., *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, Times Books, 2014.

³⁹ SCHNEIER, B., *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, 2015.

9. Conclusiones

PRIMERA. - En una sociedad moderna, democrática, con acceso a tecnologías que hasta hace relativamente poco eran imposibles de imaginar, aludiendo a las amenazas de que nuestro derecho a la vida o a la integridad física pueda ser aniquilado por ataques terroristas o delincuenciales, guerras, o enfermedades pandémicas, **es legítimo el uso por parte del Estado de las herramientas necesarias para mantener la seguridad adecuada.** Según el artículo 1º de la Ley Orgánica 2/86 de 13 de marzo de Fuerzas y Cuerpos de Seguridad expone “*La Seguridad Pública es competencia exclusiva del Estado. Su mantenimiento corresponde al Gobierno de la Nación.*” Seguridad pública que ofrece beneficios claros en términos de eficiencia y prevención del delito y aunque también plantea serios riesgos para el derecho a la intimidad, **se debe encontrar un equilibrio que permita aprovechar las ventajas de las nuevas tecnologías sin sobrepasar los límites** de los derechos fundamentales de las personas y esto requiere un marco legal robusto, transparencia en el uso de tecnologías de vigilancia y una supervisión adecuada para prevenir abusos y garantizar que los beneficios de la seguridad no influyan negativamente en la libertad de las personas o en los derechos fundamentales.

SEGUNDA. – Como fiel defensor del progreso aplaudo la implementación de la inteligencia artificial (IA) y tecnologías de vigilancia en aras de la seguridad ya que, aunque plantea importantes desafíos principalmente respecto al derecho a la intimidad, la **balanza entre mejorar la seguridad y proteger la privacidad debe inclinarse en mantener una seguridad óptima para poder disfrutar del resto de Derechos Fundamentales.** Como ya hemos visto, programas como PRISM y otras herramientas utilizadas para la seguridad como las de reconocimiento facial, son muy efectivos para la seguridad y no generan injerencias significativas en la privacidad de la población, aunque la transparencia y la responsabilidad del Gobierno o de las organizaciones que utilizan estas tecnologías deben ser claras sobre cómo se recopilan, utilizan y almacenan los datos, y rendir cuentas por las injerencias indebidas en la privacidad de las personas. Como ejemplo, el caso de Clearview AI, con su vasta base de datos de imágenes faciales, escenificando la necesidad de una regulación estricta y una vigilancia constante para evitar abusos y la recopilación masiva de datos biométricos que sin el consentimiento adecuado puede llevar a una erosión significativa de la intimidad de la sociedad.

El acceso por parte de los Gobiernos a datos personales, la utilización de Inteligencia Artificial, Softwares de identificación, injerencias en las comunicaciones, programas de seguimiento de Redes o cualquier otro que se utilice en aras del mantenimiento o mejora de **la seguridad debe estar por encima del derecho a la intimidad** pero también tiene que estar estrictamente **regulado por un marco legal que garantice la protección de los derechos** humanos, confeccionándose leyes que especifiquen claramente los fines, condiciones y limitaciones de dicho acceso, asegurando que se realice de manera proporcional y justificada.

TERCERA. - Los medios técnicos actuales, como cámaras de videovigilancia, fotográficas y reconocimiento biométrico han demostrado ser muy efectivos para las Fuerzas y Cuerpos de Seguridad (FFCCS), pues ayudan a identificar a los infractores y determinar su modus operandi. La grabación de imágenes de forma legal puede esclarecer hechos delictivos, lo que resalta la importancia de instalar cámaras en lugares específicos cumpliendo con la ley de videovigilancia. Actualmente, algunas instalaciones críticas están obligadas a tener cámaras de video-vigilancia, pero esa obligación debería ampliarse a otros lugares y a algunas vías públicas que también deberían contar con cámaras debido a la alta concentración de personas y delitos, ya que la grabación de infracciones es útil como prueba y puede ser verificada por peritos para garantizar su autenticidad, además de la gran labor de prevención de la seguridad que se hace efectiva tan solo con la mera presencia de estas cámaras de vigilancia o cualquier otro método de identificación, facial o biométrica. Los avances tecnológicos también permiten la creación de informes periciales a partir de grabaciones, lo que podría sustituir el reconocimiento fotográfico tradicional y hacer más preciso el proceso de identificación.

Después de haber analizado y reflexionado sobre el tema, considero que **la vulneración de la intimidad en aras de mantener una seguridad optima no siempre debería requerir un mandamiento judicial**. Cuando la ley establece de manera clara la obligación de ceder datos para la prevención de delitos o la represión de infracciones, este proceso debería ser más ágil. La legislación vigente, como el Reglamento General de Protección de Datos de la Unión Europea y la Ley Orgánica 3/2018, permite que los responsables de ficheros cedan datos a la Policía Judicial, siempre que se cumplan los requisitos establecidos para que la investigación sea efectiva lo que favorece la eficiencia en la resolución de los casos por lo que considero que **la intervención judicial solo**

debería ser necesaria en situaciones excepcionales, como en el caso de la intervención de las comunicaciones o la entrada y registro en domicilios. Fuera de esos casos específicos, el hecho de comprobar los movimientos que realiza por ejemplo un posible terrorista o delincuente no debería requerir autorización judicial adicional, podría poner varios ejemplos como ese mismo terrorista que visita una fábrica de explosivos o incluso a través de Internet la búsqueda de procesos para fabricar bombas, o un delincuente sexual que pasa horas observando a niños en un colegio etc.

CUARTA. - Este trabajo me ha permitido comprender más a fondo las normativas que regulan el derecho a la intimidad, la obtención de datos personales y su uso para mantener una seguridad adecuada. He podido formular opiniones basadas en la legislación vigente, y creo que **es necesario mejorar la claridad y agilidad de los procesos judiciales para que la seguridad sea más efectiva y eficiente**. La utilización de las nuevas tecnologías, Big Data, obtención de datos personales, el uso de imágenes y biometrías, inteligencia artificial y análisis predictivos deben ser reguladas de manera que respeten los derechos fundamentales, pero también tienen que facilitar el mantenimiento o restablecimiento, en su caso de la seguridad y para ellos **debemos despojar al proceso de dilaciones indebidas y burocracias que dificultan el mantenimiento de la seguridad**. Sin duda, aún queda mucho por legislar y clarificar en este ámbito ya que nos encontramos en el principio de un nuevo mundo que está en constante evolución.

Bibliografía

ANGWIN, J. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, Times Books, 2014.

ALBADALEJO, M. *Definición de privacidad e intimidad*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1990, pp. 1-3.

ATIENZA, M. *Ponderación y sentido común jurídico*, Universidad de Alicante, 2014.

CRAWFORD, K. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021.

DÍEZ PICAZO, L. M. *Los derechos fundamentales en la Constitución Española*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1995, pp. 45-50.

EUROPAPRESS. *El Ministerio de Defensa adjudica un contrato a Palantir para el Sistema de Inteligencia de las Fuerzas Armadas*, Europapress, 16 de octubre de 2023.

EUBANKS, V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, 2018.

GOIG MARTÍNEZ, J. M. *Límites de los derechos fundamentales*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 2000, pp. 51-55.

GREENWALD, G. *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, 7 de junio de 2013.

GREENWALD, G. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Metropolitan Books, 2014.

HOBBS, T. *Leviatán (Extractos)*, 1859.

IGLESIAS CUBRÍA, J. *Definición de privacidad e intimidad*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1990, pp. 1-3.

MARCHENA GÓMEZ, M. *Nulidad de la prueba por la intromisión virtual en domicilio. Una breve reflexión sobre la observación policial ilícita de la intimidad personal y familiar*, *Diario La Ley*, Nº 8788, 22 de junio de 2016.

MANUEL SÁNCHEZ, C. *Clearview, la polémica app que nos controla*, *La Voz de Galicia*, XL Semanal, abril de 2024.

MARTÍNEZ BARROS, R. *¿Quién controla realmente la información?*, *Revista de Derecho y Tecnología*, 8(2), 2023, pp. 45-59.

MORGENTHAU, H. J. *Politics among nations: The struggle for power and peace*, 7ª ed., McGraw-Hill Education, 2006.

MORENO BOBADILLA, Á. *El derecho a la intimidad en España*, *Ars Boni et Aequi*, 12(1), 2016, pp. 33-57.

NEL, D. *La vigilancia masiva en el futuro*, David Nel, 15 de agosto de 2022.

OBRADOR SERRA, F. *Análisis del concepto de seguridad*, en M. Albadalejo, J. Iglesias Cubría, L. M. Díez Picazo, J. M. Goig Martínez y F. Obrador Serra, *Estudios sobre la privacidad y la seguridad en España*, Editorial Jurídica Española, 1992, pp. 65-70.

OMODEO, M. G. *El Consejo de Seguridad de la ONU y la Seguridad Colectiva*, *Ius Et Veritas*, 6(11), 1995, pp. 59-64.

PEIRANO, M. *Por qué Sam Altman quiere escanear dos mil millones de ojos*, *El País*, 22 de agosto de 2023.

RICHARD GONZÁLEZ, M. *Ilícitud de la prueba por falta de motivación del Auto de autorización judicial de un dispositivo de seguimiento GPS en el vehículo del sospechoso*, *Diario La Ley*, 9 de noviembre de 2020.

RICHARD GONZÁLEZ, M. *Nulidad de la prueba por la intromisión virtual en domicilio*, *Diario La Ley*, Nº 8788, 22 de junio de 2016.

SAURA, E. C. *¿Qué es el programa PRISM y cómo se filtró?*, *Sec2Crime*, 29 de agosto de 2023.

SCHNEIER, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, 2015.

SMITH, J. *The Impact of Big Data on Privacy and Security*, *Journal of Data Protection*, 15(3), 2022, pp. 123-145.

SOLOVE, D. J. *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, 2004.

TOSCANO, M. *Sobre el concepto de privacidad: la relación entre privacidad e intimidad*, *Isegoría*, (57), 2017, pp. 533–552.

ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019.

Otras fuentes

GOBIERNO DE ESPAÑA. *Constitución Española*, 1978.

LEY 36/2015, de 28 de septiembre, de Seguridad Nacional, *Boletín Oficial del Estado*, 29 de septiembre de 2015.

LEY ORGÁNICA 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, *Boletín Oficial del Estado*, 14 de mayo de 1982.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (OCDE). *Declaración sobre el Acceso de los Gobiernos a los Datos Personales en poder de las entidades del sector privado*, 2023.

PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. *Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo*

a un mercado único de servicios digitales (Ley de Servicios Digitales), Diario Oficial de la Unión Europea, L 277, 27 de octubre de 2022, pp. 1-102.

STS N° 141/2020, Sala de lo Penal, Sección 1, Rec 2749/2018 de 13 de mayo de 2020.

STS, Sala Segunda, de lo Penal, Sentencia 329/2016 de 20 de abril de 2016, Rec. 1789/2015 (*LA LEY 32932/2016*).

UNITED NATIONS. *Charter of the United Nations*, San Francisco, 1945.

