UNIVERSIDAD MIGUEL HERNÁNDEZ

FACULTAD DE CIENCIAS SOCIALES Y HUMANAS

TRABAJO FIN DE GRADO EN SEGURIDAD PÚBLICA Y PRIVADA

Ciber-tecnologías de la vigilancia:

Un estudio comparativo a escala nacional sobre la aplicación de las nuevas técnicas de control en la seguridad pública y privada.

Cyber-surveillance technologies:

A nationwide comparative study on the application of new monitoring techniques in public and private security.

Curso académico 2021 - 2022

AUTOR: Victor Savall Ibiza

TUTOR: Rafael Cuesta Ávila

RESUMEN

El presente TFG tiene por objetivo principal estudiar la aplicación de las nuevas ciber-tecnologías de la vigilancia empleadas en la seguridad pública y privada en España a través de la descripción de las nuevas tendencias de ciber-tecnologías utilizadas en seguridad, la identificación de sus aplicaciones en la seguridad pública y privada; así como también, la explicación de las cuestiones éticas en su uso en cuanto a la privacidad y la libertad de las personas, para posteriormente analizar la eficacia de la aplicación de las ciber-tecnologías en la mejora de la seguridad pública y privada en España. La metodología de investigación a implementar en este TFG será de tipo documental o revisión bibliográfica, con un enfoque cualitativo y carácter multimetódico comprendiendo la aplicación de las ciber-tecnologías en la seguridad, tanto pública y privada, y haciendo énfasis en el contexto español. Además, a través de un análisis reflexivo sobre el uso de las ciber-tecnologías en la vigilancia de seguridad se comprenderá las cuestiones éticas en su uso para lograr alcanzar un equilibrio entre la seguridad y la libertad de las personas, a partir de la información obtenida de artículos científicas publicados en revistas científicas e información obtenida de organismos oficiales.

ÍNDICE

1. INTRODUCCION

En la actualidad el uso de las tecnologías de información y comunicación están siendo cada vez más utilizadas en la prevención de delitos, permitiendo establecer controles de seguridad ciudadana, tanto privado como público. En este sentido, estas ciber-tecnologías, han propiciado políticas de gobernanza a través de la cooperación constructivista entre las autoridades públicas y privadas a fin aumentar la seguridad y mejorar los controles de prevención de delitos. Por lo tanto, el control de la seguridad a través de la aplicación de ciber-tecnologías ha favorecido el control de la delincuencia; así como la gestión de los riesgos, permitiendo así disminuir los índices delictivos.

La seguridad ciudadana es una necesidad social, que busca establecer garantías de protección frente a la delincuencia, el riesgo para las personas y bienes; así como situaciones de vulnerabilidad, por lo que el uso de ciber-tecnología busca resolver o minimizar el impacto de las amenzas a la seguridad, estableciendo mecanismos de vigilancia, seguridad y control contra el crimen.

En este orden de ideas, la aplicación y expansión apresurada del uso de las tecnologías de vigilancia por motivos de seguridad ha sido considerada como un sistema que pueda vulnerar la intimidad y los derechos de libertad de las personas, pues a través de ellos todo individuo puede ser considerado como un potencial sospechoso. En consecuencia, el uso de la ciber-tecnologías disminuye la libertad y puede cercenar la intimidad; por lo que esta situación ha traído consigo reflexiones importantes desde el punto de vista ético, las garantías de los derechos y libertades fundamentales de las personas, justificado en la violencia legítima del Estado y su lucha contra el crimen.

Vale destacar que el uso de las ciber-tecnologías traspasa su uso en los espacios públicos, porque la necesidad legal de su uso argumenta que los individuos deben estar dispuestos a sacrificar su libertad y privacidad a cambio de a seguridad; por lo que se plantean dilemas éticos y legales en cuanto al alcance de su uso hasta el punto de ser consideradas como una amenaza por su uso indiscriminado y por los propios riegos que conlleva el uso de estas tecnologías.

Este Trabajo de Fin de Grado busca abordar de manera científica las controversias en el uso de las ciber-tecnologías usadas en la prevención, control y lucha contra el crimen estudiando las limitaciones de su uso e impacto en las garantías de libertad y privacidad de los ciudadanos, tomando como caso de estudio España. En este sentido, el objetivo general de la investigación es estudiar la aplicación de las nuevas ciber-tecnologías de la vigilancia empleadas en la seguridad pública y privada en España a través de la descripción de las nuevas tendencias de ciber-tecnologías utilizadas en seguridad pública y privada, la identificación de las aplicaciones de las ciber-tecnologías en la seguridad pública y privada y las explicaciones de las cuestiones éticas en el uso de las ciber-tecnologías en la seguridad pública y privada en cuanto a la privacidad y libertad. Además, se implementó una metodología de tipo revisión bibliográfica o documental de carácter descriptivo, mediante la obtención de información sobre ciber-tecnologías a través de artículo, ensayo y trabajo académicos publicados en revistas científicas de alto impacto, en buscadores como Google Scholar, Scielo, entre otros.

Vale destacar que esta investigación se justifica porque presente una temática de estudio novedosa, pues siempre la seguridad ha sido estudiada desde el punto de vista de los controles para combatir el crimen organizado y los grupos terroristas; siendo el uso de las ciber-tecnologías un control de apoyo para la seguridad. No obstante, son escasos los estudios realizados para comprender el impacto del uso de las ciber-tecnologías en la libertad y privacidad de las personas, planteados desde la perspectiva del dilema petico, por lo que poco se ha dicho sobre el papel desempeñado de estas nuevas tecnología de seguridad que se han desarrollado y desplegado de manera masiva tanto a nivel público, como privado. Finalmente, el investigador se presenta las siguientes interrogantes para este Trabajo de Fin de Grado.

¿Cuáles son las nuevas tendencias de ciber-tecnologías utilizadas en seguridad pública y privada?.

¿Cómo se aplican las ciber-tecnologías en la seguridad pública y privada?

¿Cuáles son las cuestiones éticas en el uso de las ciber-tecnologías en la seguridad pública y privada en cuanto a la privacidad y libertad?.

2. MARCO TEÓRICO

2.1. La seguridad pública

2.1.1. Definición

De acuerdo a Bosch *et al*. (2004) y Ramos (2005) se define la seguridad pública como la paz que puede tener una sociedad o comunidad debido a los componentes penales y los que se encargan de prevenir los delitos o faltas graves a otros individuos, estas personas que cometen estos delitos penetran las zonas más vulnerables. También, en el ámbito institucional, esta se define como la función que cumple un estado de resguardar y proteger los derechos que tienen las personas, preservando la paz y el orden de la comunidad. Es importante señalar, que el programa nacional de prevención y readaptación social es el encargado de prevenir y preservar la libertad pública, el mismo programa indica que estas funciones de la seguridad pública son constituidas por aquellos programas o actividades enfocadas para la prevención y minimización de delitos, de acuerdo a este programa las actividades son coordinadas por el ministerio público y otros organismos gubernamentales, difundiendo la justicia en cada comunidad, para obtener una mejor situación pública.

Por otra parte, Briceño (2009) la seguridad pública también conocida como la seguridad ciudadana, es conocida como todos aquellos organismos que promueven la seguridad y los derechos de cada persona y resguardan su integridad física para la mejora de las personas y el bienestar de cada cuidad, así mismo se puede entender a la seguridad como el conjunto de políticas que trabajan conjuntamente para el resguardo de las personas y la prolongación de la paz, por medio de la prevención y minimización de los delitos.

También, Escobar (2021) expresa que es comprendida como una cualidad publica que se aplica en el ámbito privado, es caracterizada por la eliminación de

situaciones que desmejoren la seguridad ciudadana o terminen el bienestar de los derechos de cada persona.

En la seguridad ciudadana existen políticas que resguarden la seguridad de la ciudadanía expresando aspectos en el ámbito externo, pero estos aspectos no son tan importantes debido a que se han centrado únicamente en prepararse para proteger y resguardar la nación del ataque de aquellos grupos armados los cuales son ilegales y se ha dejado un poco de lado el asunto sobre seguridad interna, equivalente, a seguridad ciudadana, lo que con el paso de los años ha ido mutando de la seguridad pública a la seguridad privada. El ideal de la seguridad es mantener en perfecto orden y libre de cualquier riesgo tanto las personas como sus bienes, para ello han de generarse todo tipo de políticas y procedimientos que permitan a todos los ciudadanos tener un ambiente sano, libre de peligro tal como lo manifiesta El diccionario Webster's New Collegiate en el cual se define la seguridad como la cualidad o estado de estar seguro o libertad del peligro. Lo seguro, libertad de, o libre de temor o ansiedad “protección” medidas tomadas para proteger en contra del espionaje, el sabotaje, el crimen, el ataque, el escape. una organización o departamento cuya labor es la seguridad (Rojas, 2011). A continuación, en la siguiente imagen se muestran los entes que componen la seguridad pública.

Figura 1: Entes de la seguridad pública. **Fuente:** Ramírez (2016)

2.1.2. Objetivos

La seguridad pública es aquella que se emplea en una comunidad la cual se encarga solo de vigilar la seguridad y los derechos de las personas, esta seguridad cuenta con objetivos los cuales se centran en el bienestar de las personas; llevando a cabo la concientización con el objetivo de minimizar o acabar con la amenaza de los deberes y derechos ciudadanos, vale destacar, que el más importante objetivo de la seguridad pública es mejorar la calidad de vida de las personas que conviven en la sociedad, estos se alcanza con un gobierno que sea más cercano a la ciudadanía y a las necesidades que estas tengan, con capacidad de respuesta inmediata, que siente las bases de un verdadero desarrollo político, económico, social, deportivo y cultural, garantizando las oportunidades de la comunidad. (Izquierdo, 2009)

De acuerdo a Vásquez (2008) los objetivos de la seguridad pública son los encargados de llevar a la misma para el mejoramiento de cada comunidad es por ello que otro de estos objetivos es establecer estrategias que ayuden a organizar la

ciudadanía, con la finalidad de obtener o promover una mejor trasparencia, la responsabilidad y la eficacia en la gestión local; luchando contra la corrección y los criminales inyectados en cada gobierno. A continuación, en la siguiente figura se presentan los objetivos de proporcionar soluciones en materia de seguridad pública.

Figura 2: Objetivos de proporcionar soluciones en materia de seguridad pública. **Fuente:** Palacio (2016).

La seguridad pública o seguridad ciudadana se encarga de proteger y fortalecer el orden civil en una comunidad, eliminando las amenazas que arremeten contra la integridad de las personas y permite mantener la existencia de la paz en la sociedad. La seguridad publica también se considera como la que salvaguarda la eficacia de los derechos humanos, la integridad personal, la inviolabilidad del domicilio y la libertad de movimiento. (Ramírez, 2020)

2.1.3. Elementos

Los elementos que conforman la seguridad pública se basan en el derecho de la población para transitar pacífica y libremente por las vías y espacios públicos sin tener que enfrentar ningún tipo de amenaza que coloque en riesgo la moralidad y lealtad psicológica y física como una consecuencia de la agresión a terceros. Es importante señalar, que por lo general el sistema de seguridad pública comprende tanto a los miembros de recursos humanos, como a cada uno de los entes administrativos de la

comunidad en relación a las funciones policiales y de auxilio a la población, que de una manera u otra son organizadas a fin de promover la prevención de delitos, las sanciones de infracciones, la protección de la paz y la tranquilidad pública del territorio y localidades municipales. (Castro, 2013; Fuentes *et al*., 2017)

Los elementos que componen la organización de la seguridad pública de acuerdo a Gudiño (2007); Peñaloza (2019); Martínez (2019) son:

- **Dirección de Seguridad Pública:** Este organismo se encargar de conducir las políticas coordinando los programas en materia de seguridad pública, las acciones que van a efectuar los policías para prevenir y sanción de faltas administrativas, la estancia de infractores y protección civil.

- **Policía Municipal:** Estos cuerpos de policiales son órganos o entes de seguridad ciudadana encargados de ejercer el servicio de policía en su espacio territorial y ámbito de competencia con la finalidad de mejorar la calidad de vida de las personas que habitan una comunidad, primordialmente estos cuerpos son orientados hacia actividades preventivas y control del delito.

- **Policía nacional:** La policía nacional se denomina como una institución armado de naturaleza civil, dependiente del Ministerio del Interior, principal responsable de la vigilancia policial de todas las capitales de provincia y núcleos urbanos que el Gobierno determine.

- **Policía aduanera:** La Policía Aduanera presta un servicio público para garantizar la seguridad fiscal y la protección del orden económico del país, mediante el apoyo y soporte operacional a la Dirección de Impuestos y Aduanas Nacionales, contrarrestando los delitos del orden económico a través de su investigación

- **Juzgados Calificadores:** Los juzgados calificadores son los encargados de sancionar las infracciones cometidas al reglamento de policía y buen gobierno.

- **Guardia civil:** Es un cuerpo de seguridad pública de naturaleza militar y ámbito nacional que forma parte de las Fuerzas y Cuerpos de Seguridad del Estado.

- **Centros de Detención (Cárceles):** Son una rama del complejo industrial carcelario que a su vez es parte del sistema de encarcelamiento masivo.

- **Órganos de Participación Ciudadana en Materia de Seguridad Pública:** son los encargados de dar la seguridad y la tranquilidad a una comunidad llevando a cabo patrullajes o monitoriamente de la misma para dar una mejora a dicha comunidad

Los avances de la seguridad pública son expuestos a través de la verificación del incremento de valores, equipo y elementos destinados a la seguridad pública, la evaluación positiva se realiza por el mecanismo de incremento. (Gudiño, 2007)

2.2. La seguridad privada

2.2.1. Definición

La seguridad privada de acuerdo a Pérez (2018) expone que al hablar de seguridad privada primero se tiene que exponer qué es seguridad. La misma es definida como cualquier elemento o cosa que no dañe a nadie. El término seguridad es derivado del latín *securitas.* En otro orden de ideas, la palabra privado en latín es *privatus* la cual se define como algo meramente cubierto o de un propietario.

Por otra parte, también se define la seguridad privada como las empresas que proveen servicios para mantener bienes e instalaciones de una institución protegidos para eliminar el riesgo de robo o intrusión. También, la seguridad privada se define como la que se encarga de proteger a una persona en específico, una empresa o eventos, la palabra privado es lo contrario de pública, es decir, no es el estado quien brinda ese servicio, sino que para obtenerlo se debe pagar por él. (Significados, 2022)

Se entiende a la seguridad privada como un sistema conformado por individuos cuyas funciones se establecen por medio de jerarquías, también la seguridad privada

está conformada por recursos lógicos y tecnológicos los cuales se encargan de minimizar o eliminar los riesgos de daños que una persona o empresa pueda estar expuesta. La seguridad privada tiene los recursos que les permiten afrontar todos los peligros que les rodean. (Valcarce, 2013)

Figura 3: Seguridad privada. **Fuente:** Segurilatam (2020)

Por otra parte, De las Fuentes (2015) define a la seguridad privada como a cada una de los servicios o actividades los cuales están conformados por una disposición jurídica vigente, los cuales son ejecutadas para terceras personas, ya sean los autorizados, los prestadores, y las instituciones oficiales debidamente registrados por la dependencia administrativa competente, las cuales tienen como objetivo general proteger o salvaguardar la integridad física de personas especificas cubriendo en cada momento a la misma para prevenir el daño de la misma. Estas organizaciones, las cuales otorgan seguridad privada, se encargan de auxiliar a las personas en caso de desastres, y colaborar en la aportación de datos o elementos para la investigación y persecución de delitos, en forma auxiliar y complementaria a la seguridad pública y previa autorización, licencia, permiso o aviso de registro expedido por las autoridades competentes.

La seguridad privada se puede definir, como el conjunto de servicios por entes u organizaciones meramente privadas, ayudando a resguardar a sus clientes de algún daño o delito. Un concepto más claro para la seguridad privada, la cual se podría definir como el conjunto de individuos los cuales se encargan de proteger a las personas u

organizaciones, los cuales le piden sus servicios efectuando pagos por el mismo. Muchas personas creen que están más resguardadas si contratan un servicio de seguridad privada, estas personas o clientes pueden ser personas como empresarios, empresas, centros comerciales etc. (Pérez, 2018; Rojas, 2011).

Vale destacar, que la seguridad privada, sirve para guiar a una institución a funcionar de una manera correcta, llevando a cabo funcionamiento en las organizaciones las cuales solicitan el servicio. Las personas muchas veces no saben la diferencia de seguridad pública o privada ya que la seguridad pública es la que se encarga de brindar la mejora para todos los ciudadanos, en cambio para que la seguridad privada otorgué su servicio, se debe contratar. En ese sentido, seguridad y ciudadanía van de la mano, ya que el nivel de seguridad de las naciones denota progreso y libertad. Esta es una cuestión evolutiva y relativa porque está en constante transformación. Con el tiempo, cambian los riesgos y también su percepción, tolerancia, implicaciones, y las respuestas sociales hacia ellos. (Torrez, 2018)

2.2.2. Objetivos

La seguridad privada es el conjunto de elementos los cuales son encargados de brindar la protección de una persona u empresa. La misma tiene como objetivo principal minimizar o acabar con las amenazas que puedan afectar las partes que reciben su protección, sin alterar o perturbar las condiciones para el ejercicio de los derechos y libertades públicas de la ciudadanía y sin invadir la órbita de competencia reservada a las autoridades. (Carrión *et al*., 2016)

La seguridad privada es la que prestan las empresas de servicios de seguridad con objeto de proteger el conjunto de bienes e inmuebles y derechos para los que han sido contratadas. Estos intereses protegidos suelen ser de naturaleza privada o de particulares: edificios, almacenes, hogares, terrenos, gasolineras, cotos privados, terrenos privados, vehículos privados, vienes o residenciales etc. Debido a su importancia, la seguridad privada de una empresa debe funcionar las 24 horas del día. (González, 2021)

Para que las empresas de seguridad privada puedan dar estos servicios, los entes públicos o autoridades del ese estado debe otorgarle una licencia. También cabe la posibilidad de que el estado pague por los servicios de estas empresas como complemento a las actividades que realizan los organismos y funcionarios públicos para salvaguardar la seguridad ciudadana. (González, 2021)

La seguridad privada ocupa un rol fundamental en la sociedad actual ya que para que las empresas, hogares o personas puedan sentirse protegidas requieren de la contratación de Seguridad Privada. Hoy en día existen distintas áreas dentro de este servicio, y cada una se enfoca en objetivos diferentes. (Oiron, 2021)

En la actualidad, la Seguridad Privada cumple un papel irreemplazable la misma, brinda garantías y tranquilidad a quienes adquieren el servicio, son importantes para las Fuerzas y Cuerpos de Seguridad del Estado. La seguridad constituye el cimiento sobre la cual la sociedad puede desarrollarse y garantizar la prosperidad de sus ciudadanos. (García, 2019)

2.2.3. Tipos

De acuerdo a Betancourt (2007) la seguridad privada se encarga de proteger a quienes compran sus servicios y está compuesto por diversos tipos de servicios tales como: la vigilancia, la seguridad, la protección e investigaciones, los cuales se les ofrece a empresa, ciudadanos individuales, entidades gubernamentales e instituciones, etc.

En este sentido el sector de la seguridad privada comprende una serie de productos y servicios brindados por personas individuales y empresas, destinados a satisfacer los requerimientos de particulares, instituciones, industrias, entidades gubernamentales y todo aquel interesado. (Carrasco *et al*., 2009)

La seguridad privada comprende muchos aspectos y facilidades para cada persona; por ejemplo, un guardia de seguridad puede asumir una variedad de roles. Esto no puede cambiar la forma en que ejerce cada trabajo ya que cada sitio de trabajo es diferente pero el objetivo es el mismo el cual es resguardar a las personas o

empresas las cuales se esté protegiendo. Los guardias de seguridad siempre deben estar listos para hacer lo que sea necesario para la seguridad de las personas y la propiedad. (Dimark, 2021)

El personal de seguridad privada, que cumplen la denominada seguridad física, muchas veces realizan tareas más allá de la prevención del delito. Desde la revisión de que la mercadería llegue en condiciones hasta la revisión del correcto orden de materiales o la carga de extintores manuales, los límites de la seguridad privada exceden la prevención del delito permitiendo proteger a los beneficiarios del servicio de distintos riesgos. (Dimark, 2021)

Hay distintos tipos de Seguridad privada, cada uno tiene diferentes actividades y cumple determinadas funciones. Para poder interiorizarte y evaluar los tipos de roles que la seguridad privada tiene son los siguientes según Oiron (2021):

- **Servicio de vigilancia fija:** Este tipo de seguridad privada consiste en que cada guardia de seguridad debe estar posicionado en una sola posición, el mismo puede realizar recorridos breves para no alejarse mucho de la posición en la que pertenece, los entes u organizaciones que contratan más este tipo de seguridad privada son los edificios, apartamentos y centro comerciales.

- **Servicio de vigilancia móvil:** Este tipo de seguridad privada consiste en que cada guardia de seguridad debe patrullar en grandes escalas para supervisar lugares amplios, deben tener algún tipo de transporte para trasladarse desde su lugar de guardia hasta donde ellos tienen que vigilar.

- **Servicio de escolta o servicio de guarda espalda:** Este tipo de seguridad privada es de los servicios más completos ya que por ser el más completa combina los 2 anteriores, este guardia de seguridad privada es el encargado de proteger una persona o carga mientras la misma se traslada de un lugar a otro. Este servicio se distingue por el uso de armas de fuego pesadas, pero también se usan armas no letales, las personas que son este tipo de guardias deben de estar

capacitadas para usar y portar armas de fuego, los cuales deben tener sus permisos para portar las mismas

- **Servicio de transporte de valores:** Este tipo de seguridad privada se encarga de proteger un artículo o varios los cuales son de muy alto valor valiosos. La seguridad del transporte privado se encarga de trasladar y proteger determinadas mercancías de un lugar a otro. Este servicio de seguridad privada es muy popular en el sector bancario, al igual que la entrega de efectivo. Haciendo las entregas mucho más eficientes ya que el personal que realiza el servicio de transporte de valores debe estar sumamente catalogado y entrenado para cumplir su rol completamente.

- **Seguridad de eventos:** Este tipo de seguridad privada se encarga de resguardar y proteger a las personas en aquellos eventos en las que se encuentran multitudes de personas, los cuales pueden ser desde partidos de fútbol hasta conciertos de músicas, estas personas que ejercen este tipo de seguridad se encargan también que las personas circulen con tranquilidad y garantizar la protección de las instalaciones y de quienes están dentro de ellas.

- **Protección Ejecutiva:** Este tipo de seguridad privada se encarga de cuidar a personalidades que a menudo necesitan protección tales como cantantes, actores gente muy adinerada, etc. Estos profesionales de la seguridad privada deben proteger correctamente a sus clientes ya que las personas que están cuidando son muy importantes.

- **Servicios de patrulla:** Este tipo de seguridad privada consiste en que cada profesional patrulle constantemente por los negocios, las casas o edificios privados en horarios determinados. Con una persona custodiando las instalaciones es poco probable que alguien entre a robar o dañe la propiedad privada.

- **Seguridad del lobby:** Este tipo de seguridad privada se encarga de cuidar el vestíbulo de una empresa. Es por eso que el guardia de seguridad debe ser muy

visible, este guardia debe estar capacitado para responder rápidamente a las violaciones y controlar quién entra y sale del edificio.

- **Sistema CCTV**: Este tipo de seguridad privada se encarga de proteger un circuito cerrado de televisión o como comúnmente se la llama CCTV. es una instalación de equipo tecnológicos conectados, las personas que se encargan de vigilar esta área deben adaptarse a las necesidades de cada cliente.

Figura 4: Agentes de seguridad pública. **Fuente:** Hernández (2019)

2.2.4. Fuerzas de seguridad

De acuerdo a Rubert (2013) las fuerzas de seguridad son las encargadas de brindar la paz en una sociedad o país, estas fuerzas cumplen distintos roles dentro de cada estado ya que son varias las organizaciones encargadas de darle al estado seguridad, estos órganos de seguridad comúnmente conocidas como organismos de seguridad del estado, fuerzas del orden, agencias del orden público, fuerzas y cuerpos de seguridad, agencias de aplicación de la ley y agencias de policía; las cuales cumplen un muy importante rol dentro de un país ya que las mismas ponen en orden a la sociedad.

En la actualidad en muchas partes del mundo las debilidades de los gobiernos han llevado a los conflictos civiles a los países ya que no saben cómo administrar los

organismos de seguridad del estado, muchos estudios arrojan que la principal problemática de la seguridad lo forma el fenómeno de la criminalidad, cuyas delincuencias que bajo a cualquiera de sus tipologías, por medio de manifestaciones o potencial lesivo de gran magnitud y por la extrema nocividad de sus actividades, la promoción de alto perfil de la delincuencia organizada transnacional, elevándola al nivel de problema de máxima seguridad. Así adquiere, por consiguiente, en mayor o menor medida, un espacio propio en las agendas de actuación de las Fuerzas de seguridad.

Estas fuerzas de seguridad por lo general minimizan la criminalidad otorgando una paz a sus ciudadanos, los cuales son el conjunto de organizaciones encargadas de la seguridad de carácter profesional y permanente, que la Ley Orgánica 2/1986 pone al servicio de las Administraciones Públicas para el mantenimiento de la seguridad ciudadana. España cuenta con cuerpos de seguridad muy bien entrenados las cuales son divididos en 3 niveles los cuales son el local, nacional y autonómico. Cada Administración territorial puede tener un Cuerpo de Seguridad inserto en su organización (Marín, 2009). Los 3 niveles que son regulados por la ley en España son:

- Las Fuerzas y Cuerpos de Seguridad del Estado, dependientes del Estado.
- Los Cuerpos de Policía dependientes de las Comunidades Autónomas.
- Los Cuerpos de Policía dependientes de las Corporaciones Locales.

2.3. Ciber-tecnologías de la vigilancia empleadas en la seguridad

2.3.1. Definición de ciber-tecnologías

De acuerdo a Hernández (2018) las ciber-tecnologías también conocida como la ciberseguridad es conocida como la habilidad de defensa de los servidores, las computadoras, los dispositivos móviles, los ataquen cibernéticos y las redes. Vale destacar, que esta tecnología también se conoce como seguridad de la información electrónica o seguridad de tecnología de la información, estos términos son aplicados en diversos contextos muy amplios los cuales se derivan desde informática hasta los

negocios más pequeños, los cuales se pueden dividir en diversas categorías conformadas por los argumentos de seguridad.

Bermejo *et al*. (2018) define a la ciber-tecnologías como el conjunto de herramientas y procedimientos que se realiza para proteger o mantener en constante seguridad la información que se genera y procesa a través de servidores, computadoras, redes, dispositivos móviles y sistemas electrónicos; es decir, una capa de protección para los archivos de información.

Por otra parte, la ciber-tecnologías pueden definirse como el grupo constante de acciones e implementaciones consignadas para proteger dispositivos informáticos ante ataques del contexto informático o posibles intentos de robar la información. El significado de esta palabra es considerado por la combinación de ciber que se entiende como todo dispositivo o aspecto vinculado de informática, y la palabra tecnologías se entiende como todas aquellas innovaciones que hoy en día socavan al mundo de cosas nuevas. Estas ciber-tecnologías son propuestas con la finalidad de implementar tecnologías o herramientas hardware y software que ejecutan barreras para evitar el acceso desconocido la información y de protegernos y expulsar al enemigo en caso de vulneración (Avansis, 2021). Cabe destacar, que estas ciber-tecnologías pueden tener un impacto significativo en el futuro. Históricamente las tecnologías han sido usadas para satisfacer necesidades esenciales para obtener placeres corporales y estéticos y como medios para satisfacer deseos. (Morales, 2011)

2.3.2. Tipos de ciber-tecnologías

Las ciber- tecnologías son todas aquellas tecnologías implementadas para la seguridad de servidores, computadoras y redes informativas con el fin de proteger información importante de dispositivos informáticos. Los tipos de ciber-tecnologías son los siguientes.

2.3.1. Cámaras

De acuerdo a Von Hirsch (2007); Ferrer (2020) uno de los tipos de ciber-tecnologías son las cámaras de seguridad las cuales están constituidas por sistemas

tecnológicos avanzados que consiste en vigilar un área a través de cámaras de videos situadas en distintos lugares. Estos sistemas de cámaras de seguridad se conocen como circuito cerrado de televisión o CCTV que en su traducción en inglés es closed circuit televisión. Esta tecnología de cámaras de seguridad es muy útil para identificar una persona no deseada en un lugar en específico o cualquier persona que realice alguna actividad indebida que ponga en riesgo la integridad de un lugar o individuo.

Las cámaras de seguridad son específicamente utilizadas para monitorear materiales, áreas o personas desde una sala central de control, desde la misma se puede configurar la dirección de las cámaras de seguridad, el enfoque y la vista panorámica, actualmente estos sistemas de video vigilancia tienen incluida muchos beneficios para la óptima visualización desde la cabina de control ya sea en locales, empresas o comercios.

Figura 5: Cámaras de vigilancia. **Fuente:** Mota (2015)

2.3.2. Drones

De acuerdo a Ríos (2021); Carrillo (2018) otro de los tipos de ciber-tecnologías son los drones los cuales son llamados los vehículos no tripulados este vehículo es capaz de mantener un nivel de vuelo muy controlado y continuo, estos vehículos fueron originados a principios del siglo XX, aunque solo en unos pocos años atrás fue que se hizo popular. Esta popularidad de los drones se manifestó de manera masiva y el precio de los mismos subió de manera exagerada tanto así que en la actualidad uno de estos

vehículos no tripulados tiene un costo de 22.000 millones de euros, y para el año 2026 puede llegar a costar unos 35.000 millones de euros. (Burrueco, 2021; Zapata *et al*., 2021)

Actualmente existen diversas aeronaves no tripuladas los cuales se manejan a control remoto, estos drones los adquieren tanto los ciudadanos como las empresas para fines lúdicos o profesionales, estos drones tienen diversos tamaños y modelos los cuales cuentan con muchos avances tecnológicos. Algunos cuentan con GPS, cámaras de grabación digital y comunicación a través de redes WI-FI. (Martínez *et al*., 2015; Burrueco, 2021)

Estos vehículos no tripulados se pueden utilizar para desplazarse tanto en zonas no pobladas como actividades comerciales y de investigación, así como también, en zonas pobladas como playas, parques, ciudades o fiestas etc. (Ríos, 2021; Martínez *et al*., 2015)

Figura 6: Drones. **Fuente:** Rodríguez (2016)

2.3.3. Reconocimiento facial

De acuerdo a Domingo (2021) el reconocimiento facial es un tipo de ciber-tecnologías el cual es compuesto por un sistema de identificación biométrica y es desarrollado para identificar o verificar a una persona comparando y analizando patrones basados en los registros almacenados de los contornos faciales de la persona en tiempo real. Estos sistemas biométricos toman patrones y puntos de las características más prominentes de la cara de un individuo. Si una persona que no está

registrada en el sistema, intenta burlar el sistema, el mismo lo rechaza ya que para para proceder, el sistema tiene que tener guardados los patrones de cada persona autorizada. (Paredes, 2021)

Estas tecnologías son cada vez más innovadoras ya que cada vez se están actualizando de igual manera las mismas son utilizadas para el acceso a aplicaciones o servicios online; autenticación de doble factor, acceso a edificios/oficinas, métodos de pago en tiendas física y en aplicaciones mobile, verificación de identidad en hoteles o aeropuertos. (Paredes, 2021)

Figura 7: Reconocimiento facial. **Fuente:** Excle (2021)

2.3.4. Weareables

La palabra Weareables proviene de la palabra en ingles wearable computing que en español significa computación usable, esta son computadoras o aparatos electrónicos los cuales comúnmente se utilizan como atuendos, estos atuendos son de uso común bien sea gafas las cuales tienen por nombre Google Glass los cuales sirven como un dispositivo de visualización de información, también otros atuendos son los

zapatos deportivos que tienen un chip que almacena información sobre la posición y rendimiento, y por último los dispositivos computarizado de ante brazo tales como los relojes inteligentes las cuales son pequeños computadores que se usan en la muñeca como un reloj (Ávila, 2017)..

Los dispositivos Weareables son el resultado de la evolución de los avances tecnológicos alcanzada con la miniaturización de los componentes electrónicos, el desarrollo de los protocolos de comunicación, la geolocalización y el software de gestión de datos. En definitiva, la tecnología wearable representa una nueva etapa en la evolución de la industria de los dispositivos móviles. (Iberdrola, 2022; Martínez *et al*., 2020)

Figura 8: Weareables. **Fuente:** Iberdrola (2022)

2.3.5. Sistema biométrico

De acuerdo a Incibe (2017) la biometría es un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento. Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.

En la actualidad, la tecnología ha permitido automatizar y perfeccionar estos procesos de reconocimiento biométrico, de forma que tienen multitud de aplicaciones y finalidades especialmente aquellas relacionadas con la seguridad. Como los identificadores biométricos son exclusivos de los individuos, se consideran más confiables para verificar la identidad de uno que los sistemas de identificación basados en tokens tradicionales, como un pasaporte, así como los sistemas de identificación basados en el conocimiento, como una contraseña. (Incibe, 2017). Todos estos sistemas de identificación basados en reconocimiento de voz, huellas dactilares, iris o análisis facial tienen algo en común que ofrecen mayor seguridad al usuario y facilitan el acceso sus dispositivos, evitando errores o pérdidas de contraseña. (Juanes, 2017)

Figura 9: Sistema biométrico. **Fuente:** Juanes (2017)

2.3.6. Otras tecnologías

De acuerdo a Lechner (2016) estas tecnologías están cada vez más avanzadas y están alcanzando un óptimo redimiendo en la seguridad ciudadana las cuales están conformados por 3 sistemas los cuales son los más fundamentales para el cuidado de

los ciudadanos estos 3 sistemas son: los sistemas de geolocalización, los sistemas de video-vigilancia públicos y privados y por último los sistemas biométricos y de controles accesos públicos.

- **Sistemas de Geolocalización**

El sistema de geolocalización se basa en el sistema conocido mundialmente como GPS (Global Positioning System) o Sistema de Posicionamiento Global. Está compuesto por una red de 24 satélites denominada NAYSTAR, situados en una órbita a unos 20.200 kilómetros de la Tierra. (Lechner, 2016)

La expansión del GPS está particularmente ligada a los nuevos sistemas operativos como Android que va desde el uso del celular para la localización punto a punto, hasta las principales aplicaciones Web como Twitter, Google+ y Facebook, las cuales publican la ubicación del dispositivo automáticamente. (Lechner, 2016)

Figura 10: Sistemas de Geolocalización. **Fuente:** Guerrero (2017)

- **Sistemas de videovigilancia públicos y privados**

Los sistemas de videovigilancia se puede decir que se utilizan para la monitoriza ción de un área definida y se constituyen en una forma de vigilancia sobre la totalidad de sus ciudadanos y sus instituciones alcanzándose así, niveles de control social nunca

antes observadas. Si bien los sistemas de videovigilancia son utilizados dentro de las políticas de prevención, con el fin de tener un objetivo disuasorio, en general pasan a ser un elemento represivo, debido a que resguardan la información por un tiempo determinado; para luego, ante la ocurrencia de un hecho delictivo o su sospecha, procede a buscar en los registros de imágenes para individualizar a los sospechosos del resto de la sociedad. (Capistrán, 2003)

Los sistemas de videovigilancia se fueron innovando a sí mismos y pasaron a modificar sus estructuras como sus prestaciones, de a poco se fueron instalando en diferentes dispositivos móviles, entre ellos los drones y patrulleros tecnológicos de las distintas fuerzas de seguridad, y junto a software diseñados especialmente para las fuerzas que poseen múltiples aplicaciones llevando a mantener una comunidad mucho más segura que antes. (Lechner, 2016)

Figura 11: Sistemas de videovigilancia. **Fuente:** Securactiva (s.f.)

- **el sistema pegasus:** Este programa se conoce como (spyware) el cual es un software de espionaje que sirve para iOS y Android. Este programa informático no necesita que ningún usuario lo comande, ya sea abrir un archivo adjunto, para poder acceder a los teléfono móvil u ordenador. Además, es capaz de entrar en los

teléfonos inteligentes de forma totalmente invisible para el usuario. Una vez que este software es instalado a cualquier dispositivo es capaz de acceder a todos sus datos, además de activar la cámara o el micrófono, la geolocalización y leer el contenido de sus mensajes, aunque estén encriptados como Telegram o WhatsApp. (Garcia, 2021)

- **Seguridad informática:** se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros. Este tipo de ciberseguridad se refiere a todas aquellas actividades destinadas a la protección y privacidad de los datos que transitan por una red informática y por los dispositivos conectados a ella. (Pérez *et al*., 2021)

- **Seguridad operativa:** Este tipo de ciberseguridad involucra todas aquellas prácticas, procesos y decisiones destinadas al manejo adecuado de los recursos y datos informáticos. También, incluye las estrategias y políticas que se ejecutarán ante cualquier incidente o manejo inadecuado de los protocolos de seguridad. La idea es abordar el factor más impredecible de la ciberseguridad, que es el personal. (Sierra, 2021)

- **Apps de seguridad:** El uso de aplicaciones o Apps para teléfonos inteligentes es una de las maneras más fáciles de aprovechar la tecnología para evaluar, monitorizar y mejorar la seguridad. (González, 2022)

- **Sistemas de identificación virtual:** Este sistema de seguridad se basa en el uso de tarjetas virtuales para temas de identificación de personas y control de acceso. Es una tecnología muy innovadora pues reemplaza las tarjetas de acceso físicas que se perdían todo el tiempo o dejaban de funcionar. (Herrera, 2021)

2.3.3. Cuestiones éticas en el uso de la ciber-tecnologías de la vigilancia empleada en la seguridad

De acuerdo a Rodríguez (2014) las nuevas tecnologías que han surgido son de suma importancia para la vigilancia de la sociedad, la cual impacta a las nuevas tecnologías de información y comunicación en la conducta de los seres humanos, en las sociedades y en las organizaciones los problemas y dilemas éticos que se producen en medio de la utilización de estas tecnologías. Si bien, la ética es una rama de la filosofía, relacionada con la moral, que ha sido estudiada durante miles de años, por lo que no cabría encontrar respuestas y soluciones sencillas. (Rodríguez, 2014)

Estas tecnologías proponen definitivamente nuevos estilos de vida y formas de pensar; plantean nuevos paradigmas de relaciones entre los individuos, de allí el surgimiento de los problemas éticos en el uso de éstas y la necesidad de realizar estudios que proporcionen soluciones para lograr el bienestar social y la preservación de una cultura informática en las organizaciones. Los cambios en los aspectos sociales, culturales, políticos y económicos de la sociedad actual generados por los nuevos paradigmas y el avance vertiginoso han producido modificaciones en las características morales y éticas en el uso de las computadoras, programas, información y otros aspectos de índole tecnológico, los cuales a su vez han creado dilemas éticos para los usuarios, los profesionales informáticos y la cultura informática en las organizaciones. (Silva *et al.,* 2006)

Los problemas éticos han sido estudiados durante muchos años, se han realizado conferencias en el ámbito internacional en los problemas éticos de tecnología de información. La ética de la información está basada en la fundación filosófica de ética informática, esta ética informática es calificada como una disciplina filosófica, comparte con otras disciplinas filosóficas la tradición analítica, tres rasgos importantes la caracterizan: es lógicamente argumentativa, se conecta con tierra empíricamente y por último endosa un problema que resuelve el acercamiento. Por lo tanto, es evidente que cualquier organización debe asumir el reto de pasar a la sociedad de la información y del conocimiento, no es nada fácil. La incorporación del uso de las ciber-tecnologías en los procesos organizacionales trae consigo fuertes amenazas. (Pérez, 2003)

En general, todo el mundo considera que las tecnologías de apoyo y de ayuda a la dependencia son una oportunidad para conseguir la autonomía personal, y en ese

caso se considera ética su aplicación, pero también se ven riesgos si no se incluyen suficientes elementos de control, como por ejemplo el uso de códigos éticos. (Rodríguez, 2014)

Estos problemas implican mucho más que un análisis profundo de la ética informática y de la implantación de los códigos de ética en el uso de las ciber-tecnologías. Las organizaciones actuales discuten sobre la posibilidad de formular proyecto de vida organizacional, fortaleciendo sus principios éticos, promulgando y estimulando el pensamiento moral y ético, todo esto con el único fin de constituirse en una organización vital donde lo más importante es la vida. La ética de la lógica de la vida les permitirá prepararse para enfrentar los retos de la guerra de la información en la era actual de la post-información. Es importante destacar, que la cultura informática en sí, no es el tema central de este artículo, sin embargo, guarda cierta relación con las implicaciones éticas que se evidencian en la utilización de las TIC en las organizaciones. (Silva *et al.,* 2006)

Figura 12: Ética y TIC. **Fuente:** Rodríguez *et al*. (2014).

Estos problemas éticos están en cada una de los aspectos de la vida de los seres humanos, de la sociedad y de las organizaciones esto deriva a que ocurran violaciones como es el llamado “spamming” la cual se comprende como el uso inadecuado de la red para hacer publicidad no solicitada, las cuales son las llamadas cartas cadena, que pueden incluso hacerle perder su acceso a Internet, el «flameo» que no es otra cosa que responder agresivamente los ataques violentos de un remitente, la seguridad, la piratería de la computadora, la copia ilegal de software, la libertad de palabra, las discriminaciones intelectuales y sociales, el vandalismo los crackers, los hackers, los virus, la desinformación, el anonimato, la propiedad intelectual y derechos de propiedad. (Silva *et al.,* 2006)

En este mismo orden de ideas, los problemas en los sitios de trabajo informatizados, las aplicaciones de las leyes en el ciberespacio, la ética de la computadora profesional y la metodología de códigos profesionales son temas para el estudio de la ética. Surgen entonces problemas en los ambientes de trabajo, códigos de ética profesionales para los consumidores y profesionales de la informática, la ética de la inteligencia artificial y la vida artificial, los problemas éticos de la sociedad de la información son transformados profundamente por la tecnología de la información. (Silva *et al.,* 2006)

Figura 13 Nuevas Tecnologías de Información y Comunicación. **Fuente:** Avilés (2015).

2.4. La ciber-tecnologías en la seguridad pública y privada en España

En España los conflictos y cada uno de los criterios de ponderación judiciales y legislativos que se analizaran se refieren básicamente al interés por preservar la seguridad pública y el derecho a la privacidad. El modelo de la seguridad ciudadana en un contexto europeo y americano tiene varias décadas. Por otra parte, la seguridad privada también protege el contexto en que una persona puede comportarse como si estuviese en privado, más allá de si lo está o no. Lo importante es que la seguridad privada posibilita ejercer la libertad de hacer aquello que sólo se haría en privado. (Ramírez, 2016)

La innovación tecnológica ha logrado transformar la forma en que se comportan y se relacionan las personas, ya que con tan solo un click, se puede interactuar con personas que están en el otro lado del mundo; desde el celular se puede conocer con precisión la cantidad de tiempo que durará el recorrido hasta un lugar de destino, se pueden saber con exactitud las condiciones climáticas durante la semana y hasta realizar transacciones bancarias desde la comodidad del hogar, entre otras muchas tareas cotidianas. Situaciones que en el pasado eran impensables o que simplemente no era posible predecirlas, pues se tomaba mucho tiempo haciéndolo. (Villalobos, 2020)

A nivel de seguridad, la innovación tecnológica se ha evidenciado principalmente en el campo de la seguridad informática, donde la telemática y la informática han coincidido para crear una serie de avances para la protección de todo activo o bien de la información. Sin embargo, a nivel de la seguridad pública, el avance tecnológico no se ha desarrollado con la misma rapidez o, al menos, con el mismo impacto, pues aún se observa que muchos cuerpos policiales, en algunos países, siguen utilizando los mismos medios e instrumentos convencionales para prevenir el delito y combatir el crimen (Villalobos, 2020). Los cuerpos policiales se enfrentan a nuevas modalidades de crimen que hace menos de un lustro no existían. Su principal reto es el cómo utilizar la tecnología como su principal aliado para prevenir y combatir el delito en su territorio y dar una respuesta rápida y efectiva a los problemas de la criminalidad, demanda que se hace cada vez más frecuente por parte de las personas habitantes de estas regiones (Aguirre, 2016).

A pesar de que los ciudadanos consideran que la seguridad efectiva es una prioridad alta, y los países están dispuestos a invertir fuertemente para satisfacer esta demanda, se producen contradicciones entre los requisitos legislativos, por un lado, y los aspectos prácticos de la seguridad, por el otro, apareciendo consecuencias no deseadas. (Rodríguez *et al*., 2019)

El desarrollo tecnológico de los últimos años es particularmente relevante para el desarrollo de sistemas de seguridad efectivos, pero las discusiones sobre las amenazas e inseguridades hacen hincapié en la necesidad de más investigación en este campo. El afianzamiento de alianzas entre los sectores público y privado en el campo de la policía y la seguridad, es esencial, sin embargo, la experiencia muestra que el logro de estos objetivos no es sencillo. (Rodríguez *et al*., 2019)

La relación entre las compañías de seguridad privada y los cuerpos policiales presenta problemas de competencia y conflictos agravados cuando, como ocurre en España, es la propia policía la institución de supervisión que otorga las autorizaciones a las empresas del sector de seguridad privada y vigila el cumplimiento de la ley por parte de las mismas. Si además los políticos están involucrados en estos temas, situación que también se produce en España, aprobando Leyes y redactando Reglamentos, el tema es aún más complejo. (Rodríguez *et al*., 2019)

La Seguridad Privada desde sus comienzos, después de ser derogada la Ley de Seguridad Privada en España, en el año 1992, no ha parado su crecimiento debido al desarrollo económico del país. En un principio, el mayor objetivo de los guardias de seguridad era la prevención del robo, con el paso del tiempo y por las necesidades del país, sus funciones se ampliaron a otros objetivos. (Gómez, 2012)

En cuanto a innovación tecnológica, la seguridad corporativa en España debería ser predictiva y preventiva, para permitir predecir riesgos y eventos de seguridad, y ofrecer soluciones integrales que ya están en el mercado. Los expertos del sector sostienen que estas innovaciones no se están implementando por falta de inversión, de regulación normativa y de formación de los equipos de personas y tecnologías en este importante ámbito de la seguridad de las empresas. (Álvarez, 2022)

2.4.1. Marco legal de la seguridad

El internet y la aparición de nuevas tecnologías ha originado la aparición de nuevas modalidades de delitos e infracciones a las normas que ni siquiera estaban previstas. Por tanto, es necesario que las diferentes leyes existentes se adapten para regular y proteger a ciudadanos y empresas de todos estos ataques cibernéticos en la medida de lo posible. Y que se establezcan nuevas normativas que regulan las situaciones nuevas, no previstas hasta ahora en el mundo físico. (Cabrera *et al*., 2005)

Normativa de ciberseguridad en Europa

Durante las últimas décadas, los servicios electrónicos, las nuevas tecnologías, los sistemas de información y las redes se han incorporado a nuestra vida cotidiana. Es de conocimiento común que los incidentes deliberados que causan la interrupción de los servicios y las infraestructuras críticas constituyen una grave amenaza para su funcionamiento y, en consecuencia, para el funcionamiento del mercado interior y la Unión Europea. (García, 2018)

Este riesgo, combinado con el hecho de que las contramedidas existentes en términos de herramientas y procedimientos de seguridad no están suficientemente desarrolladas en la UE, y ciertamente no son comunes en todos los Estados miembros, hizo necesario un enfoque integral a nivel de la Unión, con respecto a la seguridad de redes y sistemas de información. (Consejo europeo, 2022)

Asegurar la red y los sistemas de información en la Unión Europea es esencial para mantener en funcionamiento la economía en línea y garantizar la prosperidad. La Unión Europea trabaja en varios frentes para promover la resiliencia cibernética. Por lo tanto, se ha creado en Europol un Centro Europeo de Ciberdelincuencia para ayudar a los países de la Unión a investigar los delitos en línea y desmantelar las redes delictivas. Asimismo, la UE está tomando medidas para hacer frente a los desafíos en materia de ciberseguridad (Consejo europeo, 2022).

Es importante señalar, que la normativa europea de ciberseguridad se rige por las siguientes leyes:

- Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información de la Unión.

- Reglamento Europeo de Protección de Datos 2016/679 (RGPD). Establece la implantación de nuevas medidas de seguridad para las empresas europeas, los autónomos y la Administración pública. (Consejo europeo, 2022)

- Ley de Seguridad Cibernética (Cybersecurity Act), aprobada el 27 de junio de 2019 por la UE. Esta ley moderniza y refuerza la Agencia de la UE para la ciberseguridad (ENISA) y establece un marco de certificación de la ciberseguridad en toda la UE para productos, servicios y procesos digitales. (García, 2018)

Normativa de ciberseguridad en España

De acuerdo a Giménez (2014) en nuestro país existe un Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio. Este código hace referencia a las siguientes leyes sobre ciberseguridad. No obstante, la ley de seguridad informática en España establece los siguientes mecanismos para mejorar en materia de ciberseguridad:

- Prevención: adoptar las medidas necesarias para prevenir ataques informáticos.

- Detección: si se produce una intrusión, debes detectar el momento en el que se produce y tomar las medidas necesarias para minimizar los daños.

- Restauración: debes restaurar el sistema dañado con las copias de seguridad realizadas anteriormente.

- Análisis forense: con él puedes ver las acciones que el atacante ha realizado en tu sistema.

Ley sobre la seguridad de las redes y sistemas de información

Lo objeto del presente Real Decreto-ley es regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes. (BOE, 2018)

El Real Decreto se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad. Adicionalmente, en el caso de las actividades de explotación de las redes y de prestación de servicios de comunicaciones electrónicas y los recursos asociados, así como de los servicios electrónicos de confianza, expresamente excluidos de dicha Directiva, el Real Decreto se aplicará únicamente en lo que respecta a los operadores críticos. El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información tiene por objeto:

- Regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y
- Establecer un sistema de notificación de incidentes.

Para ello, la nueva normativa sobre ciberseguridad en España se adapta al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo conocida como Directiva europea sobre ciberseguridad. Esta Ley de seguridad de la información identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan dichos servicios. (BOE, 2018)

Normativas de seguridad nacional

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que regula los principios y organismos clave, así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional. (BOE, 2015)

- Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

Normativas de seguridad

- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. (BOE, 2015)

- Ley 5/2014, de 4 de abril, de Seguridad Privada.

Referidas a las telecomunicaciones

Las telecomunicaciones han experimentado en la década analizada cambios notables hacia una situación de mercado y competencia. Las reestructuraciones de la industria y de los agentes básicos no siempre han sido fáciles. (Gaitán, 2018)

- Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.

- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.

- Ley 50/2003, de 19 de diciembre, de firma electrónica.

- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Todas esas leyes relacionadas con la seguridad de la información están diseñadas con el objetivo de ofrecer un marco normativo que permita garantizar la seguridad de la información digital y establecer una legislación común a nivel europeo.

Sobre la ciberdelincuencia

- Código Penal,
- Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores;
- Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal.

Normativa de protección de datos

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.
- Reglamento, aprobado por el Real Decreto 1720/2007, de 21 de diciembre. Esto mientras no se apruebe la nueva Ley de Protección de Datos.

2.4.2. Uso de las ciber-tecnologías en la seguridad pública y privada

El uso de tecnología se ha convertido en una herramienta potencial para la seguridad ciudadana. A lo largo del tiempo existen investigaciones que evidencian la numerosa cantidad de programas y acciones que demandan distintas innovaciones tecnológicas para su implementación. Se advierte que este uso, particularmente por parte de los gobiernos, ha sido recurrente, y es previsible que en los próximos años continúe en aumento, de manera tal que coincido en que estamos inmersos en un proceso de tecnificación del Estado dentro del campo de la seguridad ciudadana. (Jasso, 2021)

Es importante señalar, que en la seguridad ciudadana y la tecnología hay tensiones. Por una parte, la seguridad ciudadana se dirige hacia el fortalecimiento de la ciudadanía en el sentido de potenciar los derechos individuales y colectivos; se trata de una propuesta orientada más hacia la ciudadanía que a la seguridad, mientras que la mayor parte de la tecnología apunta hacia el aumento de evidencia de la seguridad. El proceso de tecnificación muestra una tendencia creciente, y se ha especializado con el

tiempo: cada vez se recurre a mayor diversidad de tecnología, y hay desarrollos e innovaciones enfocadas en atender problemas o situaciones específicas. (Jasso, 2021)

Por ejemplo, el uso de sistemas de información geográfica para el análisis de la incidencia delictiva y la generación de inteligencia, los desarrollos para la atención de emergencias, la geolocalización para atender incidentes y delitos en tiempo real, el control automatizado de acceso a áreas estratégicas, la revisión de vehículos y personas mediante escáneres, la gestión de alarmas instaladas en comunidades y vía pública, así como el uso de apps para atender problemas como el acoso callejero, entre otras tantas variedades que se encuentran disponibles en el mercado y que son adquiridas y apropiadas por los gobiernos y la ciudadanía. En gran medida, desde la óptica gubernamental, se asume que la inversión en tecnología es una medida prioritaria para la seguridad ciudadana. (Jasso, 2021)

Estas tecnologías también tienen su lado negativo ya el mal uso de las mismas puede traer una serie de riesgos los cuales afectan a las personas, el mal uso de estas tecnologías puede dar lugar a una serie de consecuencias negativas las cuales afectan la salud física y mental de las personas, estos efectos negativos pueden ser desde obesidad hasta enfermedades crónicas como el cáncer y la diabetes. También, estos individuos pueden llegar al aislamiento perdiendo así el contacto con el exterior, ya sea con la realidad familiar y social (Cuervo *et al*., 2018). El uso incorrecto de estos servicios tecnológicos puede generar múltiples riesgos los cuales son mejor conocerlos antes para prevenirlos (Castillo, 2020). Algunos de ellos son:

- Ciberadicción.
- Grooming.
- Suplantación de la identidad.
- Sexting

Por un lado, el uso inadecuado o el uso excesivo de las ciber- tecnologías puede llegar a tener consecuencias familiares ya que al no dedicarle tiempo a la familia se crea un ocio, perjudicando su salud y su seguridad. También, este crea cierta carga de estrés como consecuencia de que debe estar actualizándose continuamente en sus

habilidades y conocimientos tecnológicos para llevar a cabo su trabajo correcto, lo que implica una mayor presión por producir. (Cuervo *et al*., 2018)

3. OBJETIVOS E HIPÓTESIS

3.3. Objetivos

3.3.1. Objetivo general

Estudiar la aplicación de las nuevas ciber-tecnologías de la vigilancia empleadas en la seguridad pública y privada en España.

3.3.2. Objetivos específicos

Describir las nuevas tendencias de ciber-tecnologías utilizadas en seguridad pública y privada.

Identificar las aplicaciones de las ciber-tecnologías en la seguridad pública y privada.

Explicar las cuestiones éticas en el uso de las ciber-tecnologías en la seguridad pública y privada en cuanto a la privacidad y libertad.

3.4. Hipótesis

Existe un equilibrio entre la seguridad y la libertad de las personas en la aplicación de las nuevas ciber-tecnologías de la vigilancia empleadas en la seguridad pública y privada en España.

4. METODOLOGÍA

El presente Trabajo de Fin de Grado estuvo fundamentado la aplicación de las nuevas ciber-tecnologías de la vigilancia empleadas en la seguridad pública y privada en España. En este orden de ideas, la investigación se enmarcó en un estudio de tipo descriptivo, por lo que se caracterizó las nuevas tendencias en ciber-tecnologías, sus características principales y su uso en la seguridad tanto privada, como pública. La metodología del TFG permitió obtener la información necesaria para analizar y

comprender como las ciber-tecnologías han promovido la seguridad ciudadana, pero a su vez han creado conflictos éticos en cuanto a la libertad y privacidad de las personas. El investigador se enfocó en comprender de manera cualitativa las ciber-tecnologías en el campo de seguridad, permitiendo así, la descripción de los acontecimientos analizados. (Mejía, 2020).

También la metodología de la investigación se apoyó en la recopilación de información sobre fuentes de carácter primario en relación a la ciber-tecnologías en la seguridad ciudadana, mediante consultas a fuentes académicas y científicas en la materia, por lo que el Trabajo de Fin de grado tiene carácter de revisión documental, o también denominada revisión bibliográfica (González, 2020). Además, este TFG implementó una metodología con enfoque cualitativo, para comprender las nuevas tendencias ciber-tecnología y sus impactos en la seguridad privada y pública en España; realizando un análisis crítico, reflexivo y con profundidad la influencias de estas tecnologías en el equilibrio entre la seguridad, la privación y libertad. (Mata, 2019)

El enfoque cualitativo implementado en este Trabajo de Fin de Grado tiene carácter multimetódico, interpretando de forman natural el objeto investigado, es por ello, que el investigador con enfoque cualitativo y reflexivo se orienta a observar los acontecimientos en su ambiente natural, interpretando los hechos, acontecimiento o fenómenos en base a los significados ya establecidos por otras personas, a través de los artículos científicos consultados (Álvarez *et al.*, s.f.); permitiendo mediante un enfoque reflexivo comprender como las ciber-tecnologías han generado cambios en la sociedad.

El diseño de investigación es no experimental. Martínez (2013) define el diseño de esta investigación como aquella donde las variables de estudio no son manipuladas, por lo que la información es obtenida tal cual como ocurren los acontecimiento estudiados por otros investigadores. Además, considerando que el estudio posee una metodología bibliográfica, se utilizaron las técnicas de análisis, comparación y reflexión a través de comentario críticos en función a la información obtenida de las fuentes documentales consultadas. Vale destacar que no se desarrolló un instrumento de investigación específico debido al carácter bibliográfico del TFG.

La confiabilidad de una investigación científica de acuerdo a Cortés (1997) se refiere a la capacidad que posee la investigación para permitir encontrar resultados similares, con lo que el estudio se puede replicar cuando se requiera; brindando confianza de que los hallazgos son reales. La información académica referenciada en este Trabajo de Fin de Grado comprensión artículos, ensayos, publicaciones en revistas científicas de alto impacto y universidades reconocidas, y bibliotecas o buscadores académicos, como Google Scholar y Scielo. Todos los artículos científicos considerados en este TFG han sido revisados rigurosamente por las revistas científicas para su aceptación.

Por su parte la validez del estudio, de acuerdo a Cortés (1997) se refiere a la capacidad de la investigación para explicar el fenómeno estudiado con profundidad científica mediante la crítica que realizar la investigación a los acontecimientos encontrados producto de la revisión bibliográfica obtenida de las fuentes de información, presentando de manera adecuada la información construida por el investigador. Por lo tanto, se establecieron los siguientes criterios de inclusión y exclusión:

Criterios de inclusión: artículos en español, tiempo de publicación: últimos 20 años, artículos científicos, ensayos académicos, revisiones bibliográficas que traten de las ciber-tecnologías, cuestiones éticas entre la seguridad, privacidad y libertad, artículo en españa.

Criterios de exclusión: artículos que incluya otro tipo tecnologías, artículo en otro idiomas al español, artículo que no sean españoles, otro tipo de seguridad que no se ciudadana.

La recolección de datos según Hernández *et al.* (2020) es el método, recurso o medio a través del cual se obtiene la información para el estudio científico. Mediante la recolección de datos se inspeccionan y examina la información útil para alcanzar los objetivos; apoyando las conclusiones y la toma de decisiones a través del análisis. La información académica utilizada en este estudio se obtuvo de artículos, ensayos, publicaciones en revistas científicas de alto impacto y universidades reconocidas, y bibliotecas o buscadores académicos, como Google Scholar y Scielo, entre otros.

Finalmente, el análisis de los datos, de acuerdo a Urbano (2016) es un proceso reflexivo donde el investigador sintetiza la información de manera clara y precisa para dar respuesta a los objetivos establecidos en la investigación; por lo tanto el autor descifra, comprender, relaciona e interpreta la información para extraer su significado y llegar a conclusiones; por lo cual Torres et al. (s.f.) expresa que a través del análisis de datos se responde a los que se pretende demostrar con los objetivos planteados

5. RESULTADOS

Bosch *et al.* (2004) desarrolló su estudio científico sobre el Estado, mercado y seguridad ciudadana: análisis de la articulación entre la seguridad pública y privada en España. El investigador establece que el tema de la seguridad ciudadana se ha convertido en un tema prioritario para las democracias occidentales, por lo que la seguridad debe ser una responsabilidad compartida del Estado con los entes privados, incluyendo a la sociedad civil, por lo que estas partes interesadas deben articular acciones y un sistema de seguridad eficaz. En este sentido, el investigador analiza la aplicación en la seguridad privada y pública en España, obtenido como resultado que tanto la Unión Europea, como España han desarrollado legislaciones en esta materia para ayudar a la articulación de controles para cooperar y mejorar los sistemas externos e internos de seguridad español a través del uso de ciber-tecnologías .

Aguirre (2016) realizó su investigación sobre las tecnologías de información y comunicación en prevención del delito. El objetivo principal del estudio fue mostrar los beneficios del uso de las tecnologías basadas en el internet como estrategias de prevención de delitos. En consecuencia, el autor señala que la prevención de los delitos se debe originar de las proyecciones estadísticas, de los modelos de prevención y la gobernanza entre los organismos públicos y los ciudadanos; así como también, se refuerza la importancia del uso de las redes cibernéticas la prevención del delito y de las plataformas tecnológicas electrónicas. Finalmente, Aguirre concluye que se debe ampliar el margen de acción de los controles de seguridad a través de las ciber-tecnologías integradas a las gobernanza.

Gómez (2020) realizó su estudio científico sobre la intimidad y tecnología biométrica aplicada a la seguridad ciudadana en Colombia: nuevos desafíos. En ensayo científico tuvo como objetivo principal identificar los desafíos que plantea el uso de la ciber-tecnología, específicamente el uso de tecnología biométrica en la intimidad y seguridad ciudadana en Colombia. El investigador obtiene como resultado a través de una encuesta de percepción que las personas consideran que este tipo de medidas puede vulnerar la información privada y su intimidad, por lo cual se deben desarrollar proyectos tecnológicos de seguridad ciudadana que ayuden a informar sobre el papel de estos sistemas electrónicos de seguridad por biometría con el propósito de que la sociedad pueda conocer sus beneficios y su alcance y comprendan su valor desde el punto de vista de su seguridad y no como una herramienta de seguimiento, rastreo por parte del gobierno.

Giménez (2014) realizó sus estudios sobre la madurez del sector de seguridad privada en España: Análisis de su evolución legislativa. Este artículo científico tuvo como objetivo principal realiza una revisión de la legislación en materia de seguridad privada en España en los últimos 20 años. Los resultados obtenidos muestran que las legislaciones en materia de seguridad han sufrido cambios debido al contexto social y la evolución del sector seguridad y tecnológico en los últimos años. El autor considera que tanto la Ley de seguridad Privada del años 1992 y la promulgada en 2014, representan filosofías inspiradoras para la seguridad privada en España y lo momento claves para la seguridad del país. El investigador concluye que la legislación en seguridad privada por parte de Estado Español está centrada en el control, profesionalización y sanción delas conductas delictivas hacia la seguridad, observando que la seguridad privada debe ser un complemento de la seguridad pública. No obstante, el investigador concluye que la última Ley de seguridad privada de 2014 se estable una mayor amplitud en os controles utilizados para la seguridad privada, permitiendo el uso de tecnología avanzadas para aumentar el espacio de actuación.

Espinola *et al.* (2012) desarrolló su estudio sobre la video vigilancia y el discurso de la seguridad. El investigador expresa que el uso de la video vigilancia, sus procesos e implicaciones tiene implicaciones importantes sobre el contexto donde su utilización

es fundamental para la seguridad. En consecuencia, Espinola *et al.* señala que el uso de estas tecnologías ha convergido en problemas por uso de las tecnologías de comunicación e información en seguridad, conocidas como ciber-tecnologías, sobretodo en su política de uso. También, el investigador obtiene como resultados que el uso de la ciber-tecnologías para el tratamiento de la información sobre la inseguridad, las tecnologías de registro y la reproducción de imágenes pueden representar instrumentos de poder, orden social, la eficacia de las políticas de gobierno, incluyendo el uso del espacio público. Finalmente, se concluye que el uso de tecnologías y dispositivos digitales para la seguridad expone problemáticas como el incremento de empresas privadas a disponibilidad del sector público y privado; así como la sobrevaloración del uso de los recursos tecnologías implementados en la seguridad; además de que la percepción ciudadana sobre el uso de la video vigilancia no será un factor de importancia para mejorar las condiciones de seguridad.

Gómez *et al.* (2018) realizó su investigación sobre las tecnologías de la vigilancia: una mirada hacia la violencia legítima del Estado en cuestiones de seguridad y control. El investigador señala que luego de los actos terroristas del 11-S se ha desplegado el uso de diversas tecnologías de vigilancia en un contexto social caracterizado por el miedo y la incertidumbre antes amenzas a la seguridad mundial. Por lo tanto, las tecnologías de vigilancia ayudan a fortalecer los sistemas de seguridad ayudando a la protección, prevención y lucha contra el crimen. Asimismo, el autor obtiene como resultado de su investigación que la justificación del uso de la ciber-tecnologías en seguridad está argumentada en que los ciudadanos están dispuesto a sacrificar su libertad y privacidad personal con tal de recibir mayor garantía de seguridad, por lo cual esta forma de implementar las tecnologías plantea dilemas en cuanto a su utilidad y riesgos de uso. El investigador concluye que existen diferencias encontradas en cuanto a la implementación de ciber-tecnología en argumentos de aceptación o rechazo.

6. DISCUSIONES

Las nuevas tendencias de ciber-tecnologías utilizadas en seguridad pública y privada.

Los cambios en el contexto de la seguridad público y privada y los avances en los desarrollos tecnológicos han llevado consigo el uso de ciber-tecnologías para aumentar la capacidad de control y prevención de hechos delictivos. En este sentido, de acuerdo a la revisión bibliográfica realizada el uso de estas nuevas tecnologías cada vez es más implementada en los sistemas de seguridad del Estado y de las instituciones privadas para aumentar la confianza y la garantía de protección y vigilancia.

Bosch *et al.* (2004), Espinola *et al.* (2012) y Gómez (2020) expresa que cada vez el uso de estas tecnologías se vuelve una dependencia en el sistema de seguridad, tales como sistemas de identificación biométrico, cámaras de video vigilancia con tecnología de información, Weareables, sistemas de reconocimiento facial, escáner, geolocalización, entre otros, están siendo utilizadas para aumentar la capacidad de detección, control y prevención de delitos. En este sentido, Jasso (2021) señala las aplicaciones y desarrollo de tecnologías en seguridad son muy variadas y dependen de la funcionalidad y aplicación en la que se pretende utilizar. Por lo tanto, en el mercado es posible encontrar una variedad importante de ciber-tecnologías que se pueden utilizar en los sistemas de seguridad ciudadana. Por ejemplo.

El Estado español de acuerdo a las investigaciones realizadas ha asumido que la inversión tecnológica en sistemas de seguridad es una medida prioritaria como parte de su agenda de políticas de Estado de acuerdo a Gómez *et al.* (2018). Además, Giménez (2014) expresa que para España es fundamental el uso de la ciber-tecnología después de los acontecimientos ocurridos el 11-S y las situaciones de actos terroristas ocurridos en territorio español después de este acontecimiento terrorista, por lo que el uso de estas nuevas tendencias tecnológicas en sistemas de seguridad y vigilancia se ha convertido en una necesidad del contexto social producto del miedo y amenzas de grupos terroristas y el crimen organizado. En ese orden de ideas, la inversión en

herramientas de ciberseguridad se concibe como una necesidad imperante para aumentar la seguridad ciudadana y que los sistemas ya establecidos puedan aumentar su eficacia y capacidad de detección, control y prevención. (Gómez, 2020).

Es importante destacar que de acuerdo a Giménez (2014) y Aguirre (2016) señalan que las ciber-tecnologías utilizadas en los sistemas de seguridad so considerando por muchos como sistemas discriminatorios sobre el comportamiento de los individuos, debido a propician situaciones que disminuyen las garantías y derechos de la libertad privacidad de las personas, inclusive algunos las consideran intrusivas, violencia así su derecho a la intimidad. Consideran este contexto, las investigaciones en el campo de las ciencias sociales buscan evaluar la conceptualización de la seguridad, con el contexto social y jurídico que busquen apoyar la implementación de las ciber-tecnologías en los sistemas de vigilancias, pero sin vulnerar o poner en riesgos los derechos humanos.

Las aplicaciones de las ciber-tecnologías en la seguridad pública y privada.

Es importante considerar que las ciber-tecnologías están siendo cada vez más utilizadas en diversos campos de la seguridad ciudadana, tanto público, como privado. En función a los artículos de investigación científicas consultados hay una clara tendencia a que estas tecnologías sean implementadas en diversas actividades de la sociedad y en diversos niveles, siendo algunos más y otros menos invasivo a la intimidad de las personas. Principalmente, de acuerdo a lo señala por Gómez (2020) las tendencias de ciber-tecnología buscan la recopilación de datos para realizar una trazabilidad de la información en anonimato para asegurar la privacidad de las personas. Asimismo, el uso de las nuevas tendencias tecnológicas es de importancia en la retroalimentación de los resultados en cuanto a la eficacia de los sistemas de seguridad, sobre todo aquellos donde son usado como herramientas de recopilación de datos en operativos secretos de seguridad contra la criminalidad.

En este sentido, el desarrollo de la ciber-tecnologías no solo incluye equipos tecnológicos, sino también sistemas de seguridad a través de software analíticos. Es importante señala que en España, el uso de ciber-tecnologías tiene una gran variedad

de implicaciones jurídicas, Ley sobre la seguridad de las redes y sistemas de información, las diversas normas en materia de seguridad nacional, incluyendo las leyes de seguridad privada y pública; otras normativas jurídicas referidas a las telecomunicaciones, la ciberdelincuencia y la protección de datos. Por lo tanto, toda esta red jurídica que regula el uso y el propósito de ciber-tecnología tiene como finalidad proteger a los ciudadanos y hacer un uso adecuado de las aplicaciones tecnológicas en los sistemas de seguridad ciudadano, tanto público, como privado.

Vale destacar, que actualmente Jasso (2021) señala el uso de sistemas informáticos para la incidencia delictiva, el desarrollo de atención emergencias, los equipos de geolocalización o Weareables para comprender los incidentes y delitos en tiempo real y áreas estratégicas, tales como revisión de los vehículos, personas; también las nuevas tecnologías en escáner; así como también, el uso de sistemas de alarmas inteligentes en las vías públicas, comercios y comunidades. Asimismo, el uso de tecnologías apps, entre otros.

Las cuestiones éticas en el uso de las ciber-tecnologías en la seguridad pública y privada en cuanto a la privacidad y libertad.

El uso de las ciber-tecnología ha atraído consigo dilemas y problemas éticas asociadas al alcance de uso y la utilizada de los datos personales de las personas; por que ha se ha abierto debates para analizar el equilibrio que debe tener el uso de estas nuevas tecnologías sin vulnerar los derechos fundamentales de libertad, dignidad e intimidad de las personas. De acuerdo a estos hechos y los debates suscitados en cuanto a las garantías a la privacidad y la libertad se ha entablado un sistema jurídico bastante robusto en España para asegurar de que estas tecnologías sean usadas apropiadamente para el fin que fueron concebidas. En este sentido, García (2018) señala que el objetivo de legislar en materia de ciberseguridad tiene como objetivo asegurar que el intercambio de información y la cooperación en los sistemas de seguridad sea eficaces para garantizar la seguridad ciudadana pero a su vez ayudan a garantizar los principios de libertad y privacidad de las personas

La Unión Europea y España han trabajado para desarrollar legislaciones que regulen el crecimiento del mercado de estas ciber-tecnologías, así como uso, la protección de los datos y de derechos de las personas a fin de genera confianza en las población. En consecuencia, se han desarrollado instrumentos jurídicos, como el Reglamento General de Protección de Datos (RGPD) en el año 2018, de aplicación obligatoria a todas las empresas fabricantes de ciber-tecnologías con la finalidad de asegurar la protección de los datos e información de los ciudadanos y proteger su privacidad desde el diseño y por defectos de estas ciber-tecnologías, por lo cual estas nuevas tecnologías debe pasar por un proceso de certificación. En este sentido, Espinola *et al.* (2012) señala que la incorporación de los sistemas de información a los dispositivos tecnológicos de be asegurarse la objetividad e el uso de la información de los usuarios, incluyendo el registro, la organización y sistematización de las gran cantidad de información manejada.

Es importante que los sistemas de seguridad y la implementación de las ciber-tecnología puedan desplegarse garantizando los derechos de libertad, privacidad e intimidad de las personas, cuestiones éticas muy importantes en el uso de estas tecnologías y el mantenimiento de los derechos fundamentales de las personas; por lo tanto el registro, la vigilancia y el control de seguridad como una medida social debe ser implementada cuidadosa y éticamente. En este orden de ideas, el uso de la información se vuelve un elemento sumamente peligro por lo que es importante el registro, almacenamiento y construcción de datos que contiene información privilegiada pueda ser jurídicamente controlado.

Debido a estas cuestiones éticas en cuanto al manejo de la información, las garantías de la libertad y la privacidad el España ha justificado la intervención jurídica de las seguridad privada con la finalidad de regular el ejercicio de poder sobre estos sistemas donde se implementar ciber-tecnología y así garantizar los derechos de las personas, ofreciendo garantías y confianza a la población de que no se será vulnerada por el uso de la información utilizada para controlar y prevenir actos delictivos o terroristas; por lo que Bosch *et al.* (2004) expresa la importancia de que los sistemas de

ciber-tecnologías para seguridad sean adecuado en su aplicabilidad como en sus riesgos hacia los derechos fundamentales de las personas.

También, es importante señalar que debido a la preocupación con respecto a las cuestiones éticas en uso de ciber-tecnologías para los sistemas de seguridad y los avances apresurados del sector las leyes y los instrumentos jurídicos han crecido para regular la seguridad informática, tal como el caso de España según lo señalado por Giménez (2014). No obstante, a pesar de las controversias éticas sobre el uso de estas nuevas tendencias tecnológicas la sociedad reconoce la importancia de su uso, por lo que solo queda regularlas a través de las normativas legales; por lo cual es importante que el diseño de un ciber-tecnologías se pueden considerar las implicaciones éticas, sociales y políticas asociadas a la introducción de estas nuevas tecnologías.

7. CONCLUSIONES

Los nuevos retos en la solución de los problemas de seguridad requieren nuevas formas de organización social, política y jurídica; así como la cooperación de todas las partes interesadas en la sociedad. En este sentido, el uso de la ciber-tecnología ha demostrado su eficacia y mejora en los sistemas de control, mitigación y prevención de actos delictivos y terroristas de acuerdo a la revisión documental desarrollada en este TFG. Las ciber-tecnología ha aumentado la capacidad de respuesta del Estado para generar confianza de seguridad en la ciudadanía, tanto a nivel público, como privado.

La seguridad pública y privada en España presenta una gran y variada legislación en materia de seguridad y ciberseguridad con la finalidad de aumentar la eficacia de los sistemas de seguridad pero a la vez proteger la libertad, privacidad e intimidad de las personas en el uso de la información. Por lo tanto, es evidente que el uso de las ciber-tecnologías ha traído dilemas éticos, sobre todo con lo relacionado a la protección y el uso de la información de las personas y el menoscabo de los derechos de libertad, privacidad e intimidad de los ciudadanos. No obstante, de acuerdo a la revisión bibliográfica realizada este riesgo en España es muy bajo debido a la estructura jurídica establecidas, muy robusta por cierto, que permite disminuir las probabilidades de uso de información inadecuada para valorar los derechos de libertad

y privacidad de las personas; ya que los instrumentos jurídicos no solamente esta orientados al control y uso de la información, sino también a garantizar que el diseño de estos dispositivos de ciber-tecnologías desde el diseño considerar el respeto y las garantías hacia la libertad e intimidad de las personas.

El análisis en este TFG permitió llegar a la conclusión de que el la seguridad es un área muy compleja que involucra aspecto como la calidad, la sostenibilidad, la ética y los derechos de las personas; por lo que las legislaciones ayudan a establecer una relación armoniosa entre todos estos aspectos a fin de que el uso de las ciber-tecnología alcance un equilibrio entre la seguridad y la libertad de las personas. Finalmente, el modelo jurídico español sobre seguridad y uso de ciber-tecnologías representa un sistema de regulación importante en sector público y privado ayudando a transferir confianza a la ciudadanía sobre los sistemas de seguridad implementada en el país.

8. REFERENCIAS BIBLIOGRÁFICAS

Aguirre, J. (2016). La tecnología de información y comunicación en prevención del delito. *Revista Latinoamericana de Estudios de Seguridad,* 18, 90-103. https://www.redalyc.org/journal/5526/552656690008/html/

Álvarez, J.; López, S.; Maldonado, G.; Trejo, C.; Olguín, A. & Pérez, M. (s.f.). *La Investigación Cualitativa.* Consultado el 18 de mayo de 2022. https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n3/e2.html

Álvarez, M. (2022). La seguridad corporativa en España necesita digitalizarse para no quedarse atrás. https://cso.computerworld.es/tendencias/la-seguridad-corporativa-en-espana-necesita-digitalizarse-para-no-quedarse-atras

Avansis. (2021). Qué es ciberseguridad. Definición, tipos y objetivos de la seguridad informática. https://www.avansis.es/ciberseguridad/que-es-ciberseguridad/

Ávila, J. (2017). *Wearables*. https://www.hola.com/tags/wearables/#:~:text=Los%20'wearables'%20son%20esos%20dispositivos,otra%20variable%20que%20podamos%20imaginar.

Avilés, O. (2015). Conflicto de valores. https://prezi.com/-pupbqrkr1jy/conflicto-de-valores/

Bermejo, F. & Martínez, G. (2018). Ciberseguridad, Ciberespacio y Ciberdelincuencia. https://udimundus.udima.es/handle/20.500.12226/84

Betancourt, A. (2007). La seguridad privada en América Latina: un mercado en crecimiento. *Ciudad Segura*, 19. https://repositorio.flacsoandes.edu.ec/bitstream/10469/2717/1/BFLACSO-CS19-03-Betancourt.pdf

Bosch, J. L., Farrás, J., Martín, M., Sabaté, J., & Torrente, D. (2004). Estado, mercado y seguridad ciudadana. Ánalisis de la articulación entre la seguridad pública y privada eb España. *Revista Internacional De Sociología*, *62*(39), 107–137. https://doi.org/10.3989/ris.2004.i39.251

Briceño, Y. (2009). Seguridad ciudadana, desempeño policial y la calidad de vida en las políticas sociales. *Revista de Economía y Ciencias Sociales, 15*(1), 37-47. http://ve.scielo.org/pdf/rvecs/v15n1/art03.pdf

Burrueco, A. (2021). Drones: la amenaza para la ciberseguridad que llega desde el aire. https://cybersecuritynews.es/drones-la-amenaza-para-la-ciberseguridad-que-llega-desde-el-aire/

Cabrera, P.; Martín, J.; Fernández, Y.; Fernández, S.; Vieytes, A.; Fernández, E.; Ruiz, L. & Malgesini, G. (2005). Nuevas Tecnologías y exclusión social Un estudio sobre las posibilidades de las TIC en la lucha por la inclusión social en España. https://www.ohchr.org/sites/default/files/Documents/Issues/CulturalRights/ConsultationEnjoyBenefits/UNESCONUEVAS_TECNOLOGIASyExclusionsocial.pdf

Capistrán, J. (2003). Videovigilancia en la Sociedad Panóptica Contemporánea. *Razón y palabra*, 31. https://dialnet.unirioja.es/servlet/articulo?codigo=307546

Carrasco, M. & Bustos, G. (2009). Diagnóstico de la seguridad privada en Argentina. Instituto latinoamericano de seguridad y democracia. https://ilsed.org/wp-content/uploads/2009/10/ILSED-Informe-Seguridad-Privada-2009-1.pdf

Carrillo, G. (2018). Sobrevolando la seguridad ciudadana con la nueva tecnología Dron en Bogotá. Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/handle/10654/20397

Carrión, F. & Dammert, M. (2016). *Economía Política de la Seguridad Ciudadana*. Editorial; FLACSO, Ecuador. https://biblio.flacsoandes.edu.ec/libros/digital/55131.pdf#page=258

Castro, M. (2013). Seguridad pública. https://es.slideshare.net/mariaelenacastroirene1/seguridad-publica-29231677

Castillo, M. (2020). *Estudio sobre el uso y el abuso de la tecnología en adolescentes*. [tesis doctoral, Universidad de córdoba]. https://helvia.uco.es/bitstream/handle/10396/20875/2020000002157.pdf?sequence=1&isAllowed=y

Consejo europeo. (2022). Ciberseguridad: cómo combate la UE las amenazas cibernéticas. https://www.consilium.europa.eu/es/policies/cybersecurity/

Cortés, G. (1997). Confiabilidad y validez en estudios cualitativos. *Nueva época, 1*(15), 72-82. https://d1wqtxts1xzle7.cloudfront.net/58962722/confiavilidad_y_validez_de_instrumentos_cualitativos20190419-121511-1yvjxtr-with-cover-page-v2.pdf?Expires=1651299537&Signature=ENqGtNyAxwkNTx-DUGI-KTixFTDuz~esJ6FiUCXixOXWGkmnudidPqZevBAc6tJNjJDqB0-VZRsdiXYRm-54clSAk0fI~T8r9wJHySoSRlNn6H0k7lwQY2xJKRBjjHQpt5CahcCiwykPjomFcl3IisvVVs01yJdxUfAQQI99AXI8SstvWKf4aaDjj2P6XlT0q5yKma9INXe~atqVPfN7RrJ3QAUd4jva1c4lXI0X97XHmzeSuTWrsPUJsDOfL0ZFvaR-J~62bUigCNIraFfGdAts4dQLVO4BDvmLgXM2szJm0CB6EMjPeQ3UTAICs5gfg2Ys72iaokFPynOixVLtQg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Cuervo, T.; Orviz, N.: Arce, S. & Fernández, I. (2018). Tecnoestrés en la Sociedad de la Tecnología y la Comunicación: Revisión Bibliográfica a partir de la Web of Science. *Arch Prev Riesgos Laborales, 21* (1), 268-275. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1578-25492018000100018

De las Fuentes, G. & Berumen, M. (2015). Las empresas de seguridad privada y su regulación en Baja California RICSH. *Revista Iberoamericana de las Ciencias Sociales y Humanísticas, 4*(7). https://www.redalyc.org/pdf/5039/503950655004.pdf

Dimark, O. (2021). Cuáles son los diferentes tipos de seguridad privada. https://serviboyltda.com/cuales-son-los-diferentes-tipos-de-seguridad-privada/

Domingo, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. *El Criminalista Digital. Papeles de criminología II Época, 9*, 20-37. https://revistaseug.ugr.es/index.php/cridi/article/view/20899

Duarte, O. (2021). Tecnología para la efectividad de la vigilancia marítima del siglo XXI. *Revista De La Escuela Superior De Guerra Naval*, *18*(2), 30-45. https://revista.esup.edu.pe/RESUP/article/view/125

Escobar, G. (2021). Que es la seguridad pública. https://www.seguridadenamerica.com.mx/noticias/articulos/27461/quE-es-la-seguridad-pUblica

Espinoza, D. & Esquivel, E. (2012). La video vigilancia y el discurso de la seguridad. *Políticas de inclusión digital y experiencias de apropiación de las TIC, 27,* 1-15. https://versionojs.xoc.uam.mx/index.php/version/article/view/453/451

Excle. (2021). Reconocimiento facial: características de una de las tecnologías más populares. https://ex-cle.com/reconocimiento-facial-caracteristicas-de-una-de-las-tecnologias-mas-populares/

Ferrer, V. (2020). Cámaras de seguridad y vigilancia. https://vicentferrer.com/camaras-seguridad-vigilancia/

Fuentes, S. & Sánchez, O. (2017). La distribución espacial del robo a transeúntes y el contexto socioeconómico en tres delegaciones de la Ciudad de México. Elementos para una política de seguridad pública. *Revista Gestión y política pública, 26*(2), 417-451. http://www.scielo.org.mx/scielo.php?pid=S1405-10792017000200417&script=sci_arttext

Gaitán, R. (2018). El sector de las telecomunicaciones. https://telos.fundaciontelefonica.com/archivo/numero041/el-sector-de-las-telecomunicaciones/

García, I. (2019). Importancia del profesional en seguridad privada: su rol en la prevención de delitos. https://www.iniseg.es/blog/seguridad/importancia-del-profesional-en-seguridad-privada-su-rol-en-la-prevencion-de-delitos/

García, P. (2018). Estándares europeos en ciberseguridad. *Revista de normativa española UNE*. https://revista.une.org/3/estandares-europeos-en-ciberseguridad.html

Garcia, G. (2021). Qué es Pegasus. https://www.revistaneo.com/articles/2021/07/19/que-es-pegasus

Giménez, F. (2014). La madurez del sector de seguridad privada en España: Análisis de su evolución legislativa. *Revista Policía y Seguridad Pública, 4(1)*, 53–77. https://doi.org/10.5377/rpsp.v4i1.1555

Gómez, E. & Rodríguez, C. (2018). Tecnologías de la vigilancia: una mirada hacia la violencia legítima del Estado en cuestiones de seguridad y control. *Encrucijadas. Revista Crítica de Ciencias Sociales, 16*, 1-18. https://dialnet.unirioja.es/descarga/articulo/6754569.pdf

Gómez, J. (2020). Intimidad y tecnología biométrica aplicada a la seguridad ciudadana en Colombia: nuevos desafíos. Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/handle/10654/37191

Gómez, J. (2012). Estudio s e g u r i d a d p r i v a d a e n e s p a ñ a estado de la cuestión. https://www.fundacionesys.com/sites/default/files/estudios_archivo/Estudio%20Seguridad%20Privada%20ESYS.pdf

González, G. (2020). *Investigación documental: características, estructura, etapas, tipos, ejemplos*. Lifeder. https://www.lifeder.com /investigacion-documental/

González, J. (2022). 4 tecnologías para mejorar la seguridad en los espacios de trabajo. https://www.chubb.com/co-es/pymes/articulos/4-tecnologias-para-mejorar-la-seguridad-en-los-espacios-de-trabajo.html

González, J. (2021). ¿Cómo organizar una empresa? 7 consejos para lograrlo. https://sendadelexito.com/como-organizar-una-empresa-7-onsejos-para-lograrlo/

Gracia, D. (2001). La deliberación moral: el método de la ética clínica. *Medicina Clínica,* 117(01), 18-23. https://derechoamorir.org/wp-content/uploads/2018/10/2011-deliberacion-moral-etica-clinica.pdf

Gudiño, J. (2007). De seguridad pública a seguridad ciudadana. https://archivo.estepais.com/inicio/historicos/127/7_Ensayo3_De%20seguridad_Gudino_127.pdf

Guerrero, M. (2017). Gana importancia los sistemas de geolocalización en los envíos de paquetes. *noticiaslogisticaytransporte*. https://noticiaslogisticaytransporte.com/nuevas-tendencias/27/10/2017/gana-importancia-los-sistemas-de-geolocalizacion-en-los-envios-de-paquetes/109834.html

Hernández, C. (2018). Control a las exportaciones de cibertecnologías: Un análisis del Arreglo de Wassenaar y sus implicancias para la ciberseguridad. Revista chilena de derecho y tecnología, 7(1), 61-78. https://www.scielo.cl/pdf/rchdt/v7n1/0719-2584-rchdt-7-01-00061.pdf

Hernández, E. (2019). Servicio de Agentes de Seguridad. https://directoriodeseguridad.com/como-contratar-seguridad-privada-guatemala/

Hernández, S. & Duana, D. (2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico De Las Ciencias Económico Administrativas Del ICEA*, *9*(17), 51-53. https://repository.uaeh.edu.mx/revistas/index.php/icea/article/view/6019/7678

Herrera, A. (2021). 4 Nuevas tecnologías de seguridad de Siete24 para el 2021. https://blog.siete24.com/4-nuevas-tecnologias-de-seguridad-de-siete24-para-el-2021

Iberdrola. (2022). La tecnología 'wearable', mucho más que un complemento. https://www.iberdrola.com/innovacion/tecnologia-wearable

Incibe. (2017). Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Izquierdo, M. (2009). Seguridad pública – seguridad privada ¿dilema o concurrencia? "Aspectos del dilema seguridad pública - seguridad privada: reparto de funciones". Colección Estudios de Seguridad, 27-38.

https://helvia.uco.es/bitstream/handle/10396/11527/SPublica-SPrivada-.pdf?sequence=1&isAllowed=y

Jasso, L. (2020). Seguridad ciudadana y tecnología. Uso, planeación y regulación de la videovigilancia en américa latina. *Revista de Investigación en Derecho, Criminología y Consultoría Jurídica, 27*, 5-27. https://dialnet.unirioja.es/descarga/articulo/8133549.pdf

Jasso, L. (2021). Seguridad ciudadana y tecnología: uso, planeación y regulación de la videovigilancia en Latinoamérica. *Revista de Investigación en Derecho, Criminología y Consultoría Jurídica*, 27. http://portal.amelica.org/ameli/journal/48/481820001/481820001.pdf

Jasso, L. (2021). Tecnologías de vigilancia en las empresas mexicanas para protegerse de la inseguridad. *Hipertextos*, *8*(14), 91-110. https://doi.org/10.24215/23143924e021

Juanes, G. (2017). Autenticación biométrica, el futuro de la seguridad digital. https://cuadernosdeseguridad.com/2017/12/biometria-el-futuro-de-la-seguridad-digital/

Lechner, M. (2016). Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social. Repositorio Institucional Digital de Acceso Abierto de la Universidad Nacional de Quilmes, 1(1). https://ridaa.unq.edu.ar/handle/20.500.11807/264

Lechner, M. (2016). Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social. *Divulgatio, 1*(1). Disponible en RIDAA-UNQ Repositorio Institucional Digital de Acceso Abierto de la Universidad Nacional de Quilmes. https://ridaa.unq.edu.ar/bitstream/handle/20.500.11807/264/D1_A6_lechner_2016.pdf?sequence=1&isAllowed=y#:~:text=Para%20ello%2C%20las%20tecnolog%C3%ADas%20aplicadas,y%20de%20controles%20accesos%20p%C3%BAblicos.

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. *Boletín Oficial del Estado*, de 29 de septiembre de 2015. https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10389

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. Boletín Oficial del Estado, de 31 de marzo de 2015. https://boe.es/buscar/pdf/2015/BOE-A-2015-3442-consolidado.pdf

López, J. & Montes, A. (2020). Empleo de tecnología en los puestos de vigilancia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. Escuela Militar de Chorrillos. http://repositorio.escuelamilitar.edu.pe/handle/EMCH/466

Martínez, C. & Peláez, J. (2021). Principales retos de ciberseguridad en Drones (Parte I). https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-drones

Martínez, M. (2013). Diferencia entre diseños experimentales y no experimentales. *Prezi*. https://prezi.com/khtcmrcc9y4i/diferencia-entre-disenos-experimentales-y-no-experimentales/#:~:text=el%20dise%C3%B1o%20experimental%20implica%20mantener,se%20pueden%20manipular%20las%20variables.

Martínez, R.; Palma, A. & Velásquez, A. (2020). Revolución tecnológica e inclusión social. ISSN: 1680-8983. https://repositorio.cepal.org/bitstream/handle/11362/45901/1/S2000401_es.pdf

Martínez, J. (2019). Libro blanco de la prevención y seguridad de y seguridad local valenciana. Valencia: IVASPE. https://dialnet.unirioja.es/descarga/libro/739767.pdf

Marín, C. (2009). Legislación sobre fuerzas y cuerpos de seguridad Estatal, autonómica y local. Madrid. España: Editorial Tecnos. https://www.marcialpons.es/libros/legislacion-sobre-fuerzas-y-cuerpos-de-seguridad/9788430948529/

Mata, L. (2019). *El enfoque cualitativo de investigación.* Investigalia. https://investigaliacr.com/investigacion/el-enfoque-cualitativo-de-investigacion/

Mejía, T. (2020). *Investigación descriptiva: características, técnicas, ejemplos*. Lifeder. https://www.lifeder.com/investigacion-descriptiva/

Miranda, M. (2020). Impacto de la aplicación de nuevas tecnologías en la Vigilancia y Seguridad Privada en la ciudad de Cartagena. Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/handle/10654/36574

Morales, C. (2011). Cibertecnologia. http://moralescarlos678.blogspot.com/2011/02/cibertecnologia.html

Mota, J. (2015). 10 consejos de expertos en seguridad y autodefensa. https://borrova.blogspot.com/2015/03/tipos-de-camaras-de-seguridad-y.html

Oiron. (2021). Cuáles son los tipos de Seguridad Privada. https://ideasseguridadprivada.com/cuales-son-los-tipos-de-seguridad-privada/

Oiron. (2021). Por qué es importante la Seguridad Privada. https://ideasseguridadprivada.com/por-que-es-importante-la-seguridad-privada/#:~:text=En%20la%20actualidad%2C%20la%20Seguridad,darle%20seguridad%20a%20los%20ciudadanos.

Ojeda, L. (2020). Vigilancia tecnológica versus derecho a la privacidad-intimidad: El caso de la pandemia. *Textos Y Contextos*, *1*(21), 123–134. https://doi.org/10.29166/tyc.v1i21.2513

Pacheco, P. (2006). Régimen jurídico de la seguridad privada en España. Reposito de la Universidad de Málaga. https://riuma.uma.es/xmlui/handle/10630/4723

Palacio, E. (2016). Foro por la Seguridad con Bases Firmes. http://pansonora.org.mx/propuestas-para-mejorar-la-seguridad-ciudadana/

Palmer, D. & Warren, I. (2012). Tecnologías de vigilancia y controles territoriales: Gobernanza y el pulso de la privacidad. Revista de Asociación de Técnicos de la Informática, 217, 15-20. https://www.researchgate.net/profile/Ian-Warren-3/publication/236623477_Tecnologia_de_vigilancia_y_controles_territoriales_Gobernanza_y_el_pulso_de_la_privacidad/links/5791156908ae108aa040219d/Tecnologia-de-vigilancia-y-controles-territoriales-Gobernanza-y-el-pulso-de-la-privacidad.pdf

Palop, F. & Vicente, J. (1999). Vigilancia tecnológica e inteligencia competitiva. Su potencial para la empresa española. https://www.eenbasque.net/guia_transferencia_resultados/files/COTEC%20-%20Vigilancia%20Tecnologica%20e%20Inteligencia%20Competitiva%20-%20su%20potencial%20para%20la%20empresa%20espanola.pdf

Paredes, J. (2021). El reconocimiento facial en los sistemas de video vigilancia del ECU 911 para mejorar la seguridad ciudadana en Babahoyo. Examen Complexivo-Ingeniería Sistemas, 415. http://dspace.utb.edu.ec/handle/49000/10519

Pérez, C. (2018). El sector de seguridad y vigilancia privada: evolución reciente y principales retos laborales, regulatorios y de supervisión. Bogotá: Fedesarrollo, *Cuadernos de Fedesarrollo. 65,* 154. https://repository.fedesarrollo.org.co/handle/11445/3689

Pérez, J. & Merino, M. (2021). Definición de seguridad informática. https://definicion.de/seguridad-informatica/

Pérez, L. (2003). Nuevas tecnologías de la información: problemas éticos fundamentales. *Revista ACIMED, 11*(3). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000300006

Peñaloza, P. (2019). La seguridad publica más allá de policías y ladrones. México, https://archivos.juridicas.unam.mx/www/bjv/libros/1/419/19.pdf

Ramírez, H. (2020). La seguridad ciudadana y sus elementos de protección. http://www.respuestaperiodistica.com/por-su-seguridad/la-seguridad-ciudadana-y-sus-elementos-de-proteccion/

Ramírez, R. (2016). Seguridad pública en el contexto de la seguridad nacional, ¿seguridad interior sinónimo de seguridad pública?. https://sites.google.com/site/cursorafar/la-seguridad-nacional-en-la-perspectiva-amplia-del-desarrollo-como-estado/home

Ramírez, T. (2016). Nuevas tecnologías al servicio de la seguridad pública y su impacto en la privacidad: criterios de ponderación. *Revista chilena de derecho y tecnología,* *5*(1), 57-86. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842016000100002

Ramos, M. (2005). Seguridad ciudadana y la seguridad nacional en México: hacia un marco conceptual. *Revista Mexicana de Ciencias Políticas y Sociales, 47*(194), 33- 52. https://www.redalyc.org/pdf/421/42119403.pdf

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. *Boletín Oficial del Estado, 8* de septiembre de 2018. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257

Ríos, R. (2021). Uso de los Drones o Vehículos Aéreos no Tripulados en la Agricultura de Precisión. *Revista Ingeniería Agrícola, 11*(4). https://www.redalyc.org/journal/5862/586268743010/html/

Rodríguez, C. & Gil, S. (2014). Ética y TIC. http://www.ceapat.es/interpresent3/groups/imserso/documents/binario/eticaytic.pdf

Rodríguez, J. & Caballero, J. (2019). La seguridad privada en España y la prevención del delito. *Revista de Criminología, Seguridad Privada y Criminalística, 7*(8), 86-93. https://dialnet.unirioja.es/descarga/articulo/7046414.pdf

Rodríguez, K. (2016). Tipos de drones. https://sites.google.com/site/fgtce04integridadpersonal10/home/los-drones/tipos-de-drones

Rojas, N. (2011). Apoyo de la seguridad privada a la seguridad pública. Administración de la Seguridad, 576. https://repository.unimilitar.edu.co/handle/10654/3454

Rubert, D. (2013). La seguridad ciudadana y las Fuerzas Armadas: ¿despropósito o último recurso frente a la delincuencia organizada?. Revista Criminalidad, 55(2), 119-133. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082013000200007

Securactiva. (s.f.). Videovigilancia y nuevas tecnologías. https://securactiva.com/category/videovigilancia/

Segurilatam. (2020). El Congreso Nacional de Seguridad abordará la transformación de la seguridad privada colombiana. https://www.segurilatam.com/actualidad/el-congreso-nacional-de-seguridad-abordara-la-transformacion-de-la-seguridad-privada-colombiana_20200922.html

Sierra, J. (2021). Ciberseguridad: qué es y para qué sirve, ventajas y desventajas. https://blog.lemontech.com/ciberseguridad-que-es/

Silva, N. & Espina, J. (2006). Ética Informática en la Sociedad de la Información. *Revista Venezolana de Gerencia,* 11(36). http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S131599842006000400004

Torres, P & Salazar, F. (s.f.). *Métodos de recolección de datos para una investigación*. Facultad de Ingeniería - Universidad Rafael Landívar. Boletín electrónico N° 03, 1-21. http://fgsalazar.net/LANDIVAR/ING-PRIMERO/boletin03/URL_03_BAS01.pdf

Torrez, D. (2018). Marco conceptual y normativo. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/77565/2/Seguridad%20privada_M%C3%B3dulo%201_Marco%20conceptual%20y%20normativo.pdf

Urbano, P. (2016). Análisis de datos cualitativos. *Fedumar Pedagogía Y Educación*, *3*(1), 113-126. http://editorial.umariana.edu.co/revistas/index.php/fedumar/article/view/1122

Valcarce, F. (2013). Estado, policías y criminalidad: seguridad pública y seguridad privada en la Argentina actual. *Revista Postdata,18*(1), 11-49. http://www.scielo.org.ar/pdf/postdata/v18n1/v18n1a01.pdf

Vásquez, H. (2008). Seguridad ciudadana, depende de la política municipal de familia. https://apps.contraloria.gob.pe/transferenciagestion/material/Modulo_I/Seguridad%20Ciudadana.doc#:~:text=El%20objetivo%20principal%20de%20la,situaci%C3%B3n%20de%20paz%20del%20vecindario.

Villalobos, H. (2020). El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito. *Revista de Relaciones Internacionales, Estrategia y Seguridad,* 4. https://revistas.unimilitar.edu.co/index.php/ries/article/view/4243/4261

Villalobos, H. (2020). El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 15*(1), 79–97. http://www.scielo.org.co/pdf/ries/v15n1/1909-3063-ries-15-01-79.pdf

Von Hirsch, A. (2007). Cuestiones éticas en torno a la vigilancia en espacios públicos mediante cámaras de televisión. *Revista para el análisis del derecho*, 4, 1-24. https://www.raco.cat/index.php/InDret/article/download/78454/102442

Zapata, G. & García, R. (2021). CyberDrone: una plataforma de ciberseguridad para detección de ataques a drones. *Revista de Ingenieria y Desarrollo, 39*(1), 45- 65. http://www.scielo.org.co/pdf/inde/v39n1/2145-9371-inde-39-01-44.pdf