UNIVERSITAS
Miguel Hernández

FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS
CAMPUS ELCHE

Grado en Seguridad Pública y Privada

TRABAJO FINAL DE GRADO
Curso 2021-22

USOS Y ABUSOS DE LA CIBERSEGURIDAD EN CONTEXTOS AUTOCRÁTICOS Y DEMOCRÁTICOS. PARALELISMOS Y DISCREPANCIAS ENTRE LA REPÚBLICA POPULAR CHINA Y LA SOCIEDAD ESPAÑOLA.

Tutor: Rafael Cuesta Ávila
GRADO EN SEGURIDAD PÚBLICA Y PRIVADA.

Alumno:David Leonés Dengra
GRADO EN SEGURIDAD PÚBLICA Y PRIVADA.

USOS Y ABUSOS DE LA CIBERSEGURIDAD EN CONTEXTOS AUTOCRÁTICOS Y DEMOCRÁTICOS. PARALELISMOS Y DISCREPANCIAS ENTRE LA REPÚBLICA POPULAR CHINA Y LA SOCIEDAD ESPAÑOLA.

Según diversos estudios de organizaciones de defensa de los derechos humanos, como Amnistía Internacional, se calcula que en los últimos años cerca de un millón de uigures y otras minorías musulmanas han sido internados en campos de reeducación en la región de Xinjiang. Los expertos consideran que es una de las persecuciones por razones étnicas y religiosas más importantes desde la Segunda Guerra Mundial, aunque las cifras son difíciles de contrastar a causa del firme control informativo del gobierno chino y la dificultad para poder hablar directamente con las personas afectadas. En Xinjiang, la población está controlada por una extensa red de vigilancia con cámaras de vídeo, aplicaciones móviles de descarga obligatoria y códigos QR, así como la presencia permanente de militares y policías en las calles. ¿Qué sabemos realmente sobre lo que está pasando en la región de Xinjiang? Después de un año de pandemia en que las tecnologías digitales se han vuelto todavía más presentes en nuestra vida cotidiana, ¿qué nos dice la experiencia de los uigures sobre el papel de la tecnología en el control social del futuro? *(fuente centre de cultura contemporánea de Barcelona 31/05/2021 https://www.cccb.org/es/actividades/ficha/el-ojo-omnipresente-vigilancia-digital-en-xinjiang/235973)*

"Xinjiang es el primer gran modelo en la era de la vigilancia digital masiva. Nunca se ha visto nada igual". El profesor Darren Byler, que lleva más de una década investigando el trato de China a la minoría uigur, en Xinjiang, afirma, que los móviles y el reconocimiento facial, se han convertido en herramientas de espionaje total. Como ejemplo, explica que Vera Zhou, una ciudadana de Xinjiang, cruzaba la calle a mediados de 2019 en Kuitun, una pequeña ciudad en la región de Xinjiang al noroeste de China, cuando sintió unos toques en el hombro. Era un policía. Al llega al cuartelillo vio su cara entre la muchedumbre en alta definición rodeada por un rectángulo amarillo. En el resto de las cámaras todos los rostros eran verdes. Zhou había salido del área que tenía permitida como exinterna de un campo de reeducación. Un sistema de reconocimiento facial la había detectado entre miles de rostros.

(Fuente Diario el País 05/05/2022 https://elpais.com/tecnologia/2022-05-05/xinjiang-es-el-primer-gran-modelo-en-la-era-de-la-vigilancia-digital-masiva-nunca-se-ha-visto-nada-igual.html)

Este primer caso, hace referencia a la tecno-vigilancia sobre la minoría separatista ugiers, en el contexto autocrático chino.

Pegasus, el programa espía más potente del mundo, se ha colado en silencio en los terminales de decenas de políticos y activistas en España (en algunos casos, cuando estaban en el extranjero). A unos los sorprendió después de la sentencia

del *procés* en octubre de 2019 y de la ola de disturbios que se desató en Cataluña tras esa condena del Tribunal Supremo a los nueve arquitectos del desafío independentista. Otros recibieron su visita en los prolegómenos de las negociaciones para formar Gobierno. E incluso entró en los despachos de La Moncloa, en plena crisis migratoria con Marruecos en 2020. La lista de víctimas conocidas se limitaba, hasta el lunes, a personas vinculadas al movimiento independentista. Pero ese día, el Gobierno reveló que el móvil del presidente, Pedro Sánchez, y el de su ministra de Defensa, Margarita Robles, también fueron monitorizados en 2021. Este es el relato, aún lleno de incógnitas, del rosario de ataques (tentativas de asalto) e infiltraciones (*hackeos*) de un virus que, según su vendedor, la firma israelí NSO Group, solo pueden adquirir organismos gubernamentales como policías, ejércitos y servicios de inteligencia para prevenir el crimen organizado y el terrorismo.

El independentismo lanzó el 18 de abril una gran campaña de denuncia contra los seguimientos, que, desde el minuto uno, atribuyó al CNI. La prueba que esgrimían era un informe realizado por Citizen Lab, un grupo ligado a la Universidad de Toronto (Canadá) y especializado en ciberseguridad. En él figuraban los nombres de 63 políticos, abogados y activistas independentistas cuyos móviles habían sido dianas de Pegasus en jornadas clave para el movimiento secesionista catalán

(Fuente el país 08/05/2022 https://elpais.com/espana/2022-05-08/pegasus-relato-de-un-rastreo-masivo.html?rel=buscador_noticias)

Este segundo caso, hace referencia al ciber-control aplicado a los separatistas catalanes en el contexto democrático español

Las diferencias más evidentes son que en China la represión contra los movimientos independentistas de la minoría étnica musulmana de los uigur de Xinjiang ha sido brutal como consecuencia de la aplicación de la doctrina de máxima seguridad, recluyendo a los sospechosos en campos de internamientos contemplados como centros de reeducación, sin ninguna garantía legal ni aplicación de la mínima expresión derechos humanos. En el caso español de los movimientos separatistas catalanistas el espionaje ha sido aplicado por una 'tecnología-espía' extranjera conocida como Pegasus, y los condenados han gozado de la defensa legal en todo momento. Estas cuestiones son puntos a explorar en ambos contextos, el autocrático chino y el democrático español.

Tras todo lo expuesto, investigamos la realidad actual en la República Popular China, apuntando hacia el tema discutido de la ciber-seguridad y la tecno-vigilancia como dispositivos digitales de control panóptico asociados a las prácticas de una política autocrática, y realizar una comparativa en relación al empleo de estos sistemas dentro de los cuerpos policiales españoles para estudiar su grado de penetración en el marco de una sociedad democrática. El objetivo de esta investigación será considerar en detalle el balance resultante del peso que juegan los platillos de la seguridad y de la libertad en el contexto de sociedades democráticas-liberales como pueda ser la española. Para ello se examinará el

marco legal de nuestro país, barajando las posibilidades y límites de la aplicación de estas medidas dentro del ámbito nacional.

INDICE.

1.APLICACIÓN DEL PANÓPTICO EN UN CONTEXTO AUTOCRÁTICO: EL CASO DE CHINA.

1.1. Preliminares teóricos sobre el concepto del Panóptico.

El panóptico era un tipo de edificación carcelaria ideada por el filósofo utilitarista Jeremy Bentham hacia fines del siglo XVIII. El objetivo de la organización panóptica era permitir a su guardián, guarecido en una torre central, observar a todos los prisioneros, recluidos en celdas propias alrededor de la torre, sin que estos puedan saber si son observados.

La consecuencia más importante del panóptico es inducir en el detenido un estado consciente y permanente de transparencia que garantizaría el funcionamiento automático del poder, sin que ese poder se esté ejerciendo de manera efectiva en cada momento, puesto que el prisionero no puede saber cuándo se le vigila y cuándo no.

Este dispositivo debía crear así un «sentimiento de omnisciencia invisible» sobre los detenidos. El filósofo e historiador Michel Foucault, en su obra *Vigilar y castigar* (1975), experimentó el modelo abstracto de una sociedad disciplinaria, inaugurando una larga serie de estudios sobre el dispositivo panóptico. «La moral reformada, la salud preservada, la industria vigorizada, la instrucción difundida, los cargos públicos disminuidos, la economía fortificada, todo gracias a una simple idea arquitectónica». Jeremy Bentham, *Le Panoptique*, 1780. (La obra, de 56 páginas, fue traducida del inglés e impresa por orden de la Asamblea Legislativa del año 1791.)

En la actualidad, es un tipo de distribución que tiene como fin ejercitar la disciplina; se trata de los nuevos mecanismos de vigilancia para la canalización productora y autocoaccionadora de la conducta social programada. Por medio de las nuevas tecnologías de la información, se convierte en un estado de vigilancia permanente, controlando de maneras diversas al individuo sin que este lo sepa.

Foucault planteaba que antes el poder se hallaba en una sola persona; esta era la única encargada de ejercer las leyes y hacerlas cumplir. Se encontraba bajo el mando de un monarca o de un rey. «En este modelo disciplinario moderno, el ejercicio del poder no tiene rostro, porque cualquier persona puede ser un representante del poder central para vigilar a los demás». No importa quién vigile. Todos pueden ser vigilantes porque los vigilantes, a su vez, serán siempre vigilados por otros superiores, y así sucesivamente hasta llegar a quienes encabezan el mantenimiento del orden.

Las nuevas tecnologías de la información y de la comunicación, junto con la activa presencia de las cámaras de vigilancia, se convierten en complejos y poderosos

aparatos de vigilancia panóptica; en vías de flujo del comportamiento de las personas.

Gracias al panoptismo, las fronteras en el ciberespacio se diluyen formando un nuevo modelo de estado. Un estado mundial con su propia policía y con su propio tiempo, ya que se convierte en algo relativo y virtual, deja de ser real. Se pierde la noción de qué es real y qué no, donde la red posibilita la interconexión entre millones de personas, sea cual sea su origen, sexo, etnia o nación. Este modelo de vigilancia toma fuerza en el mundo desde los acontecimientos del 11 de septiembre de 2001.

(fuente https://es.wikipedia.org/wiki/Pan%C3%B3ptico#Ejemplos_de_pan%C3%B3ptico)

1.2. Breve introducción a la realidad china actual.

Mientras son vigilados permanentemente por cámaras inteligentes de reconocimiento facial, capaces de establecer una identidad en tiempo real, ahora los chinos son calificados: 778 sobre 950, 548 no tan bueno, 548 es una buena calificación, por el momento se trata de una calificación bancaria que certifica el buen manejo de las cuentas y que aquí todo el mundo conoce. "*Me parece bien ser calificado, es necesario que haya reglas en una sociedad"* Dice uno de los entrevistados. "*Estas calificaciones, nos obligan comportarnos bien" "Puede asustar, pero en china eso sí estamos acostumbrados. De todas formas, no tenemos opción"* son algunas de las opiniones de los entrevistados. Beijing quiere poner a marchar todo el mundo, e incluso llegar más lejos de aquí al 2020, habrá buenos y malos ciudadanos gracias a la recolección de centenares de datos provenientes de bancos, compañías privadas, y las autoridades.

"*Utilizando la mayor cantidad de datos posible, es decir, el Big Data, este sistema jugará un papel importante en la reconstrucción de la sociedad"* comenta Lin Junyue, diseñador del "crédito social".

Para ello, todo será estudiado, la situación financiera, los hábitos de consumo, la carrera profesional e incluso el comportamiento en las redes sociales. Criticar el gobierno en internet o exhibir signos exteriores de riqueza, conllevará a una mala calificación, por su parte, elogiar al partido o donar sangre, aumenta el crédito social.

Xiao Wen Wang, es una ciudadana modelo. Vive en Nankin, ciudad que ha servido de prueba, tiene el perfil perfecto. Es madre de un niño de cinco años, trabaja en una residencia para jubilados, no tiene deudas, y por ejemplo, siempre espera pacientemente para cruzar una calle: "*Como buena ciudadana que soy, respeto el código de tránsito; si no lo hiciera perdería puntos en mi crédito social".*

En teoría, todo puede ser tomado en cuenta para una calificación social, incluso los gestos más anodinos, como por ejemplo, las compras en un supermercado. En esta era de los pagos electrónicos, las compras de Yao Weng One, podrían inclinar la balanza: comprar cigarrillos no está bien visto, pero pañales sí, porque

denotan atención para un menor. Comprar cerveza puede ser sinónimo de dependencia al alcohol, mientras que comprar agua es mejor.
En esta ciudad piloto de ocho millones de habitantes tan sólo hay 18.000 ciudadanos “modelos”; para Yao Weng One eso trae beneficios, cuando toma el bus por ejemplo, paga medio ticket: *“Cuento con descuentos en todos los servicios públicos, también en los museos, y en la biblioteca; gracias a mi carnet, puedo leer gratuitamente”.*
Un buen puntaje otorga ventajas, mientras que un mal puntaje quita derechos
“Es un asunto de principios, hay que denunciar a esta gente” “No *son honestos, deben de pagar el precio” “No reembolsar, es normal pagar las deudas, de lo contrario, deben de ser expuestos en la lista negra”* son algunas de las manifestaciones de ciudadanos de HengShui entrevistados.
Al día de hoy, la lista negra contiene veintitrés millones de individuos, entre ellos, un periodista Liu Hu, el cual parece que se interesó demasiado en asuntos de corrupción relacionados con un alto cargo del partido. Fue condenado por un tribunal por difamación; es por ello, según el que su nombre fue registrado en la lista negra de la noche a la mañana; se dio cuenta cuando fue a comprar un ticket de tren. Entendió que ya no lo dejarían viajar. Lo juzgan por indigno de confianza, razón por la cual lo castigan. En palabras de Liu Hu: “*Una vez que uno se encuentra en la lista negra, no puede obtener un crédito bancário ni crear una empresa, comprar un apartamento e incluso inscribir a sus hijos a una escuela privada. Me preocupa, porque mucha gente perderá sus libertades individuales tal como yo. Todos viviremos con restricciones”*
Son pocos, los que como Liu HU, critican este sistema, que algunos catalogan como dictadura digital.

(Fuente https://www.france24.com/es/20190508-en-foco-china-reconocimiento-facial)

La República Popular China mayormente conocida como **China** es un país soberano de Asia Oriental. Es el país más poblado del mundo, con más de 1400 millones de habitantes, y la primera potencia económica mundial por PIB en términos de paridad de poder adquisitivo. La República Popular China es, después de Rusia, el segundo país más grande de Asia. La República Popular China es un Estado socialista gobernado por el Partido Comunista de China desde 1949 y tiene la sede de su Gobierno en la capital del país, Pekín.

Geográficamente, china está dividida en veintidós provincias, cinco regiones autónomas, contando con una extensión total de 9596960 km^2. Es el tercer país más extenso del planeta por superficie terrestre detrás de Rusia y Canadá y el cuarto si se cuentan las masas de agua, detrás de Rusia, Canadá y los Estados Unidos. El paisaje chino es vasto y diverso, desde las estepas y los desiertos

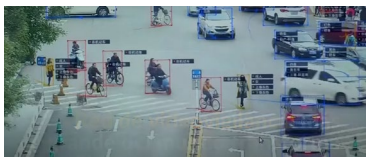
del Gobi y Taklamakán en el árido norte hasta los bosques subtropicales en el húmedo sur.

es la segunda economía del mundo en términos de PIB nominal, con un total aproximado de 15,66 billones de dólares (101,6 billones de yuanes) hasta 2020. Desde que se iniciaron las reformas económicas en 1978, China se ha convertido en una economía muy diversificada y en uno de los actores más importantes del comercio internacional. A principios de la década de 2000, China ha sufrido el deterioro y la contaminación del medio ambiente debido a su rápido ritmo de industrialización. Aunque la normativa, como la Ley de Protección del Medio Ambiente de 1979, es bastante estricta, su aplicación es escasa, ya que las comunidades locales y los funcionarios del gobierno suelen ignorarla en favor del rápido desarrollo económico. China es el segundo país con más muertes por contaminación atmosférica, después de India. Hay aproximadamente un millón de muertes anuales causadas por la exposición a la contaminación atmosférica. En los últimos años, China ha tomado medidas drásticas contra la contaminación. En 2020, el secretario general del PCCh, Xi Jinping, anunció que China pretende alcanzar un pico de emisiones antes de 2030 y lograr la neutralidad de carbono en 2060, de acuerdo con el acuerdo climático de París.

Dado las características geográficas y socioeconómicas de china citadas, por parte de sus dirigentes se utilizan se utilizan las técnicas que hemos avanzado y más adelante desarrollamos, con el fin de tener un control total de la población en todos los aspectos.

1.3 Desvelando los sistemas de Tecno- Vigilancia y Ciber – Control en la R.P.CH.

La red de videovigilancia más grande del mundo transforma a china en un gran hermano. Decenas de millones de cámaras, han sido instaladas en distintas ciudades chinas, con el objetivo de reconocer la fisonomía de las personas, a través de tecnologías de reconocimiento facial. Las compañías chinas están sacando ventaja en la carrera global, y los avances son impulsados por una generación de jóvenes emprendedores. Aunque la discusión por el derecho a la privacidad continúa vigente, muchas personas en china, presentan cierta



ambivalencia respecto de ser vigiladas. En palabras de Wang Shengjin, docente universitário: "*Creo que en la vida de las personas hay problemas de seguridad y problemas de privacidad. Creo, que cuando estas dos cuestiones entran en conflicto, la gente de China, quizás se preocupe más por la seguridad; cuando no tienes seguridad, no tienes nada"*.

El estado, es un cliente importante para las empresas del sector, en tiempos en los que el Gobierno de Xi Jinping, fomenta el desarrollo tecnológico mientras crea una enorme base de datos para identificar a cualquier ciudadano en segundos. Los departamentos de Policía Locales, compran los dispositivos para "prevenir el delito", y ya se trabaja con patrones para reconocer personas por su forma de hablar y caminar. ¿será así el escenario de futuro que nos espera a miles de kilómetros del país más vigilado del mundo?

Esta puerta abierta a la sociedad de la Hiper – Vigilancia, es uno de los posibles escenarios de futuro por dónde podría recorrer el destino de nuestros países, probablemente en menos de una década, si no existe una decidida discusión acerca del destino al que queremos encaminarnos, apostando por modelos que prosperen en la seguridad, pero retrocedan en la libertad, o bien al contrario, preferenciando el amparo de los derechos civiles frente a la progresiva inseguridad ciudadana. Cabría incluso cuestionarse sobre la posibilidad de si existen sistemas combinados o intermedios a este planteamiento binario.

a. **Videocámaras de vigilancia > tecno-vigilancia.**

   Sofisticado sistema, incluyendo aproximadamente 20 millones de cámaras, repartidas por la ciudad, interconectadas entre sí, incluso en establecimientos públicos, tales como restaurantes, observan a los ciudadanos chinos, incorporándole tecnologia de reconocimiento. La red, conocida como SkyNet, es la mayor red de videovigilancia del mundo y sus cámaras, son capaces de distinguir y realizar un seguimento a vehículos particulares, ciclistas y peatones. Estas cámaras, no son solo utilizadas para cometidos como la seguridad, sino tambien, como ejemplo, el centro

de personas perdidas en China, le da uso al sistema para sus cometidos, realizando fotografías para pasarlo al sistema de reconocimiento facial.

La Skynet, ya citada, ojos de lince, Operación llamando a las puertas, *Soldado de Limpieza de la Red*, estos son solo algunos de los términos utilizados por la seguridad de estado de China para describir los severos sistemas de vigilancia usados para identificar, monitorear, rastrear y perseguir, desde cada esquina parque o edificio, a decenas de millones de ciudadanos chinos, especialmente a minorías étnicas y grupos religiosos. Lo graba todo, desde la hora que finalizas tu jornada laboral, si te entretienes o no, si vas al domicilio de un familiar o si te diriges a realizar la compra semanal.

Están conectadas a la base de datos de la policía, que dispone de miles de criminales registrados. Para localizar a alguno, solo hay que buscarle en el sistema y pulsar "Enter". El sistema de hipervigilancia hará el resto. Están equipadas con machine learning y un sistema de reconocimiento facial, que les permite primero diferenciar entre una vehículo, cosa o humano, y en el caso de que se trate de una persona, lo pasa al dispositivo de reconocimiento facial.

«China ha adoptado el sistema de vigilancia más invasivo del mundo, y no solo utiliza nuevas tecnologías para vigilar, sino también para vincular a las personas con su registro policial, su información social, su nombre y su número de identidad», afirmó James Andrew Lewis, un experto en tecnología del Centro de Estudios Estratégicos e Internacionales (CSIS, por sus siglas en inglés). «Es la combinación de macrodatos, reconocimiento facial y vigilancia generalizada lo que hace que el mismo sea la cosa más intrusiva que alguien haya visto»

Este sistema, se instaló en Beijing, uno de los primeros lugares en terminar de instalar las cámaras de seguridad, concretamente en octubre de 2015, 7 meses después del nacimiento de SkyNet. Según el diario del pueblo, el

periódico del partido, “cada esquina de la capital, quedó cubierta con cámaras”.

b. Dispositivos de reconocimiento facial > tecno-vigilancia

Sistema utilizado, conjuntamente con las cámaras de videovigilancia, se utiliza para monitorizar a los ciudadanos, detectando su edad, género, vestimenta.

En determinadas ciudades chinas, por ejemplo, en Shanghái, este sistema es utilizado, para identificar a los ciudadanos que infringen las normas de circulación. En el caso de cometer cualquier infracción, sus rostros son captados y reconocidos por el sistema apareciendo en una pantalla, a la que llaman de la “vergüenza”. Así mismo, puede ser utilizado para prevenir robos.

Del mismo modo, cualquier persona desaparecida, normalmente anciana o con cualquier tipo de discapacidad cognitiva, son identificados, pudiendo contactar son su familia. Según los usuarios del sistema en cuanto a búsqueda de personas desaparecidas, aseguran que ha reducido de manera considerable el tiempo de búsqueda, reduciendo la carga de trabajo de los empleados, dotando de eficiencia a las búsquedas.

A nivel particular, este mecanismo ha proliferado, por ejemplo, en restaurantes de comida rápida, donde simplemente con el rostro del usuario se puede hacer efectivo el pago.

Cuando se empezó a usar el reconocimiento facial para prácticamente todo

(seguridad, salud, actividades bancarias, etc.), casi todo el mundo lo aceptó sin rechistar. Había cierto entusiasmo por una idea que demostraba el progreso tecnológico chino. Eso se vincula también con algunas concepciones filosóficas hace años arraigadas en China que dificultan la formación de barreras éticas al impacto de la tecnología en la

vida cotidiana. Mientras que en Occidente siempre hemos separado lo humano de lo técnico (religión y ciencia, por ejemplo), los chinos han creado una especie de «cosmotecnia» como la llama el filósofo Yuk Hui, los dos elementos han existido siempre juntos. Hui se refiere a los ritos confucianos: los objetos (la tekné como la llamaríamos en Occidente) son tan parte del proceso ritual como los propios ritos. Todo esto permite que China avance mucho más rápido que nuestras sociedades en este terreno. Los ciudadanos, lo utilizan para realizar transacciones comerciales a diario. Otro uso reciente, es que el gobierno chino recientemente ha obligado a todos los usuarios de celulares a utilizar el reconocimiento facial para su identificación. Uno de sus usos más controvertidos, siendo rechazado en varios países de la comunidad internacional, es, conjuntamente con el sistema de videovigilancia, rastrear a los uigures, una minoría étnica predominantemente musulmana, según su apariencia, para ser internados en “campos de reeducación”.

c. Sistema ‘Nube policial’ (*Police Cloud*) > ciber-seguridad

Procedimiento, que usa los datos aprovechables de un ciudadano en la red, desde el historial médico, uso de redes sociales o del terminal móvil, para confeccionar un historial, que marca donde y con quien ha estado cada ciudadano y qué ha estado realizando. El objetivo de esta técnica, es comparar las relaciones entre personas, sucesos y zonas para mostrar actividades o relaciones inusuales o comprometidas para el sistema. Esta plataforma, como es el caso de XinJiang, no es otra cosa que una gran base de datos que integra una gran cantidad de información del ciudadano, que la digitalización ofrece: desde datos básicos como la dirección o edad, que ya están en manos de la policía, relaciones familiares, así como registro de hoteles, vuelos y trenes, datos biométricos, imágenes de CCTV, o la información recopilada por las empresas tecnológicas derivada del uso de las TIC. Un ingente volumen de información, que la computación en la nube, la inteligencia artificial, el big data, y los algoritmos permiten convertir

en un pormenorizado análisis del pasado y el presente, que los ciudadanos ofrecen la posibilidad de predecir o alertar de posibles actividades o actitudes conflictivas del individuo.

En 2015, el *Humans Rights Watch*, señaló que “el gobierno chino debería dejar de construir plataformas policiales de macrodatos que agregan y analizan cantidades masivas de información personal de los ciudadanos”.

Este sistema, según ellos, abusivo, de “nube policial”, está diseñado para rastrear y predecir actividades de activistas, disidentes y minorías étnicas, incluidos aquellos que las autoridades gubernativas opinan que poseen “pensamientos extremos”.

Esto permite que la policía en China, obtenga información sin precedentes sobre la vida de la gente común, incluidos aquellos que no tienen conexión con las malas acciones. Por ejemplo, el sistema obtiene información del historial médico de las personas, sus preferencias en el supermercado, etc.

Todos esos datos, permiten que el Police Cloud, rastree donde han estado las personas, y sus actos, así como el realizar predicciones sobre sus actividades en el futuro.

Al ser diseñados, en parte, para rastrear y localizar a grupos que las autoridades consideran política o socialmente amenazantes, plantea serias preocupaciones sobre el perfilado social y racial. A medida que esta Police Cloud, está más alimentada, en palabras de Richardson, la directora de China en Observación de Derechos Humanos, las autoridades cada vez tienen más fuerza para rastrear los movimientos de todos, estando en juego no solo la privacidad, sino muchos de los derechos que tienen.

d. Sistema de rastreos a través de dispositivos móviles.

Como ejemplo, el gobierno chino, durante la pandemia por COVID-19, creó una aplicación, basada en los datos de geolocalización de los operadores móviles, y analizando los desplazamientos del usuario en los 14 días

anteriores, para saber si estuvo en una zona de riesgo o se cruzó con alguien enfermo por COVID-19.

El sistema Health Kit, utilizado en Pekín, utiliza, como fuentes de información billetes de tren o de avión, controles de identidad en la entrada a la capital, o resultados de los test. Tienen en común, que el usuario debe e introducir su nombre, número de identidad, teléfono y en ocasiones su foto. El sistema, genera un “código de salud”, en función de la peligrosidad. Según el ayuntamiento de Pekín, los datos personales “solo se utilizan para luchar contra la pandemia, teniendo acceso solo al apellido de la persona y a las dos últimas cifras del número de identidad.

También durante la pandemia, concretamente en Singapur, se puso en funcionamiento una controvertida aplicación, llamada TraceTogether. Los contagios, se rastrean con la tecnología BlueTooth. Los teléfonos, van reconociendo códigos que corresponden a otros teléfonos, con los que el interesado tiene un contacto significativo.

Este sistema, tiene dos formatos con diferencias para la privacidad: En el agrupado, las autoridades puedan indagar las identidades, hay que confiar en que solo lo usen para luchar contra la enfermedad, y se encargan de avisar a los contactos de quien ha dado positivo. Y el descentralizado, en el que el interesado comunica en su aplicación que ha sido infectado y sus contactos recientes se enteran por un signo que reciben en sus móviles. Estos se conectarán periódicamente con un servidor donde se registren los códigos de quienes han dado positivo.

En la entrevista realizada por el diario el País en abril del 2020, a la abogada experta en privacidad Paloma Llaneza, le suscita muchas dudas: *“En las tecnologías de contacto y trazabilidad, la implantación lo es todo. No es lo mismo un sistema descentralizado, en el que depende de la buena fe del infectado notificar su estado, que otro centralizado, que supondría subir datos de identificación a las autoridades sanitarias. el problema está en que*

estas soluciones de emergencia llegan para quedarse y pueden afectar a medio plazo a nuestra privacidad"

e. Internet de las cosas.

Es un término muy amplio, que el cual se utiliza para la interconexión de objetos cotidianos con internet o entre sí, contemplado en los estudios en informática. Estos dispositivos, incluyen teléfonos inteligentes, automóviles, televisores, relojes, electrodomésticos, y muchos más. Esta tecnología, ha ido transformando la forma en que las personas viven y trabajan. Se refiere a una red creciente de objetos físicos, conectados a internet. Estos dispositivos son cada vez más frecuentes en la vida cotidiana, ya que pueden ayudar a administrar el tiempo, la energía, recursos, bienes servicios y mucho más. Por ejemplo, zapatillas inteligentes, las cuales se pueden cargar de forma inalámbrica, y transmiten información al dispositivo al que se conectan como puede ser distancia recorrida o frecuencia cardíaca; o el caso de una aplicación para puertas de garajes inteligentes, permitiendo monitorizar y controlar el garaje desde casa para conectarse a la aplicación.

El término Internet de las Cosas, también denominado con sus siglas en inglés IoT (Internet of Things) ha permeado nuestra sociedad en los últimos años de manera especialmente intensa en los medios de comunicación. Si bien el término no es nuevo, también es cierto que las capacidades tecnológicas para implementarlo de manera más efectiva son más recientes. La masificación de dispositivos electrónicos, la posibilidad real de analizar grandes cantidades de datos a través del Big Data y de extraer conclusiones útiles de ellos parecen haber abierto definitivamente la puerta para una explosión del IoT. El término IoT está en desarrollo y por ende aún no tiene una definición aceptada universalmente. Se podría definirlo como un concepto que se

refiere a la interconexión digital de objetos cotidianos con internet. Por un lado, las bondades que traerá poder controlar todos estos dispositivos y como ello facilitará la vida cotidiana; y por el otro, los peligros implícitos de tanto control. Estos últimos básicamente agrupados en torno a la pérdida de privacidad y a la posibilidad de que un hacker se haga del control de nuestros objetos, y por extensión de nuestra vida. Un ataque realizado con éxito puede afectar a la integridad de la información que dispone el dispositivo, a la accesibilidad y la identidad del propio usuario provocando una suplantación de la identidad. En cuanto a los principales riesgos, según los expertos de la Comisión Europea, podemos enumerar:

- Asegurar la continuidad y la disponibilidad en la provisión de servicios basados en el internet de las cosas, intentando evitar posibles fallos y cortes en el funcionamiento.
- Consideraciones en el diseño de tecnologías del internet de las cosas. Es adecuado tener en cuenta las cuestiones de seguridad y privacidad en su diseño.
- La gran cantidad de datos que recopilan estos dispositivos plantea un gran problema de autentificación y confianza en dichos dispositivos.
- Ejercicio de los derechos de protección de datos para las personas y el cumplimiento de la legislación para las organizaciones.
- Pérdida o violación de la privacidad y protección de datos de los usuarios. Como ejemplo de este riesgo vamos a poner las nuevas tarjetas de crédito contactless.

f. ‘Comunidades de puertas cerradas’ (‘gated communities’): urbanizaciones cerradas.

Las *gated communities* o urbanizaciones cerradas son un fenómeno que se ha desarrollado a lo largo y ancho del planeta con gran rapidez. Su comienzo está en la segunda mitad del siglo XX, a pesar de que puede hablarse de una celeridad del proceso desde los años 80 de la centuria pasada. Siguiendo a Edward Soja podemos delimitar las *gated communities*

o comunidades cerradas como: Áreas residenciales con acceso restringido en las que normalmente los espacios públicos están privatizados. Son urbanizaciones de seguridad con perímetros marcados, habitualmente con muros o vallas y con entradas controladas que intentan prevenir su penetración por parte de los no residentes. Estas áreas residenciales reciben nombres muy diferentes: gated communities en Estados Unidos, fraccionamiento cerrado en Méjico, barrio privado en Argentina, condominio fechado en Brasil, urbanizaciones o comunidades cerradas en España, villes privées o privatisées en Francia, etc. (Capron 2006).

g. Métodos de etiquetación social (De mayor a menor: AAA hasta la D).

El gobierno chino ha diseñado un método para examinar el valor social de una persona según su conducta, llamado crédito social. Se empezó a desarrollar un sistema de crédito social, asignando a los ciudadanos puntuaciones desde la AAA, hasta la D, siendo la "AAA" el mayor nivel y el "D" el que menos, en la cual, un particular puntuado con AAA, sería la puntuación más alta gozando con todos los privilegios que considere el sistema, y a medida que no se cumplan o se transgredan las especificaciones del sistema se irá bajando la etiqueta, pudiendo y perdiendo privilegios. Es un uso cada vez más implantado en china, y aunque el gobierno asegure que se utiliza para controlar las malas conductas ciudadanas, es un medio más inculcar el régimen actual.

H. Sistema de créditos sociales > técnicas ingeniería social basada en la aplicación de la psico-sociología conductista o behaviorista.

El ideólogo de este sistema de evaluación ciudadana, es un investigador miembro de la academia de ciencias sociales, Lin Junyue, cuyos trabajos sobre el crédito social han servido de inspiración al gobierno chino. Para este científico social una educación pedagógica implica transmitir una instrucción en donde los ciudadanos deban tratarse como niños a educar, siendo el sistema de creditaje social la mejor manera de gestionar los

conflictos de una manera eficaz, restituyendo la educación moral, la honestidad y las conductas íntegras. En las tesis declaradas por este reconocido investigador chino se formula el objetivo de que la resolución de los problemas sociales mediante el crédito social no pretende tanto enviar a la gente a la cárcel cuando infringe la Ley, sino el señalamiento público de ciertos comportamientos que no son buenos para el conjunto de la sociedad. Una vez detectados los denominados como “malos” ciudadanos son desterrados de las urbes y señalados de manera humillante. En algunos centros comerciales su rostro aparece en paneles luminosos la finalidad de ser avergonzados públicamente. Más de veinte millones de ciudadanos chinos, se encuentran anotados en la lista negra, teniendo prohibido viajar por su mala calificación.

Ante el miedo a ser desaprobados y el temor al ostracismo, los ciudadanos se encuentran obligados a una ‘obediencia debida’, que por otra parte tiene su recompensa. Así, aquellos que alcanzan las mejores puntuaciones tienen derecho a ocupar las mejores posiciones en la sociedad, convirtiéndose en el orgullo de la nación. En este modelo diseñado por Lin Junyue, prima la búsqueda política de la paz y la estabilidad del país a través de un régimen policial en donde los conflictos se reduzcan a su mínima expresión. Solo a partir de este punto de aceptación del poder aparece la defensa de los derechos humanos

1.4 Casos de experiencias piloto en china.

En la ciudad de Roncheng, primer núcleo urbano en cual se puso en práctica el conocido como ‘crédito social’, en donde el baremo de puntos se exhibe en el centro de cada barrio para informar a los habitantes de las normas a seguir. Por

ejemplo, cinco puntos de deducción por la tala ilegal de árboles y el secado de alimentos, cinco puntos por la quema de residuos domésticos, etc. En este municipio, este sistema de control social es bien recibido, donde, se valoran los intereses colectivos frente a las desviaciones individuales, tradicionalmente contempladas como amorales.

Otros ejemplos, son las ciudades de Shanghai y Shenzhen, donde durante la crisis del Covid, se les pidió a las personas que viajaban entre su hogar y trabajo que se registrasen, antes de utilizar el transporte público, pudiendo solo utilizarlo las personas que declaren su identidad ante una aplicación móvil. La idea era saber si se ha viajado con personas sospechosas de estar infectadas, con el fin de realizar un seguimiento posterior.

La aplicación que se desarrolló por una empresa de aparatos electrónicos para el ejército controlada por el Estado, sirvió para que los ciudadanos chinos ingresasen su nombre y su número de identificación nacional, y supiensen si era probable que hubiesen estado en contacto con algún portador del virus. *(fuente https://www.amnesty.org/es/latest/news/2020/04/how-china-used-technology-to-combat-covid-19-and-tighten-its-grip-on-citizens/)*

1.5 Pros y contras de la ciber-seguridad en el contexto del "gigante-asiático"

Como aspecto positivo, con todos los sistemas implantados por parte de las autoridades poseen una tecnología altamente avanzada para realizar un control exhaustivo y generalizado del conjunto de la población, identificando en décimas de segundos cualquier tipo de infracción ya sea de índole penal o administrativo.

Del mismo modo, se crea la sensación de un entorno seguridad a la ciudadanía en donde impera el orden y la ley. Además, para los gobernantes constituye un

instrumento para dirigir la gestión política del modo más óptimo en el contexto de un país superpoblado y un vasto territorio a controlar.

Al entenderse la interacción humana como fuente de cualquier conflicto social, y siendo los conflictos sociales contemplados como generadores de problemas políticos, el gobierno aplica para evitarlos una tecno-estructura para primar la estabilidad social desactivando o disolviendo cualquier conato de contagio de resistencia entre la población que alimenten la disidencia contra las imposiciones del régimen comunista.

Como contraparte, se puede dar una extralimitación del poder del Estado, y una supresión total de la privacidad, y de los derechos individuales de los ciudadanos, que por otra parte en China no tienen una tradición como la que cobró en Occidente una vez superado el feudalismo medieval en donde las revoluciones burguesas rompieron con el pasado de un Estado absolutista para apostar por las democracias liberales construidas en Europa y EEUU apostando por las libertades ciudadanas, mientras que las revoluciones comunistas perseveraron en el fortalecimiento del Estado basado en la partitocracia propia del partido único optando por los criterios de seguridad y vigilancia total.

Durante la pandemia por Covid-19, la aplicación de estas tecnologías-espías ha sido un instrumento muy eficaz para el aseguramiento del cumplimiento de las medidas de contención y prevención de propagación del virus, si bien su aplicación extrema ha aplicado resistencias sobre ciertos sectores de la población, como se ha demostrado en el caso de la ciudad de Shanghái.

Mas allá de los límites nacionales chinos, todo el mundo que interactúe con el sistema chino, comprando o viajando productos chinos, corre el riesgo de que el gobierno recopile la información que le interese, con el fin de alimentar el sistema de crédito social. Si el gobierno chino tiene un buen resultado en el empleo de

estas técnicas de ciberseguridad es probable que otros países intenten implementar esas políticas en contextos de creciente inseguridad ciudadana.

Un uso inadecuado de estos datos, puede generar una amenaza al resto de países, concretamente al tratamiento de sus datos y a su seguridad.

Este conjunto de técnicas-espías, puede ser manipulada por el crimen organizado y hackers, para perfeccionar ataques, escoger un mayor número de objetivos de modo más óptimo y menos discriminada y mejorar su eficiencia

1.6 Balances entre el binomio de seguridad y privacidad, en el *Big Brother Chino.*

Una vez explorado el terreno, toca entender la noción de seguridad en relación a la concepción de privacidad/libertad individual en el contexto chino, en donde la balanza se inclina hacia el primero de los platillos por su peso desproporcionado

En la historia moderna de china, ante la preponderancia del partido comunista, siendo este una variante política de la autocracia de las dinastías imperiales de origen milenario, el poder omnímodo de las altas instancias estatales ha gobernado con mano dura los destinos de una inmensa población en un amplio territorio difícil de gestionar por otros medios democráticos.

Al igual que china, Rusia es otro claro ejemplo de la autocracia asiática, basada en una construcción estatalista de la nación, gobernadas en ambos casos por una cúspide oligárquica que culmina en la figura del emperador o del Zar.

La desoccidentalización de rusia avanza a una velocidad impresionante a medida que avanza el clima bélico actual para regresar al modelo de estado fuertemente gestionado desde arriba a partir de la represión política y policial. En el caso chino, la doble aplicación de los principios comunistas y capitalistas han reforzado

el poder de un estado que, por un lado, establece un control estricto en lo político y una expansión sin precedentes en lo económico.

2. EL EMPLEO DEL PANÓPTICO EN EL MARCO DEMOCRÁCTICO: EL CASO DE ESPAÑA.

2.1. Sistemas de vigilancia masiva en el contexto occidental.

A miles de kilómetros de la R.P. China, en el contexto de la UE la cuestión de la seguridad ha ido cobrando mayor relevancia a medida que la inseguridad ciudadana ha ido ganando terreno, fomentada sobre todo por unos medios de información que transmiten a diario imaginarios de descontrol de las realidades social, política y económica, un campo de reflexión que ha entrado de lleno en académica desde que el sociólogo Ulrich Beck introdujera el concepto de la 'sociología del riesgo'. Beck, sociólogo alemán, hace referencia a un estado de las cosas de las sociedades de la modernidad avanzada. Pensando en el *locus* de la realidad de la Alemania contemporánea, se orienta a vislumbrar las consecuencias del desarrollo tecnológico de sociedades caracterizadas por el prefijo "post", en el sentido de más allá, más allá de la modernidad, de la sociedad industrial o de clases. Para Beck, las sociedades contemporáneas, atraviesan un momento de transformaciones, similar en profundidad, al que observaron los padres de la sociología, cuando pensaron por detrás de las ruinas del régimen feudal, los rasgos de una sociedad industrial, en parte aún desconocida.

A pesar de cualquier aparente contradicción, la sociedad del siglo XXI transita hacia lo que Mattelart y Vitalis (2000) definen como un "mundo vigilado", una sociedad bajo el control de las nuevas tecnologías que hacen que nuestra intimidad o privacidad cobre la mayor transparencia posible, en donde cada vez se asiente más el principio del control cibernético.

La vertiginosa adopción de dispositivos tecnológicos que nos mantienen persistentemente conectados y que llevamos en nuestros bolsillos y mochilas, así

como la creciente presencia de cada vez un mayor número de accesorios, dispositivos e interfaces digitales incorporados como objetos en un creciente número de sujetos, ofrecen un sistema general que permite procesar ingentes cantidades de información dando muestras de un enorme salto cualitativo en nuestra nueva forma de entender los conceptos de la intimidad y la privacidad.

De este modo, en nuestra vida diaria se asiste a la creciente colonización de dispositivos incorporados a nuestras vidas de forma voluntaria que permiten informar de nuestras acciones a instancias desconocidas que acaban tomando decisiones sobre los comportamientos de los actores sociales, en muchas ocasiones de manera subrepticia y de manera ajena a nuestra voluntad. Desde cámaras de reconocimiento facial situadas en las esquinas de nuestras calles hasta dispositivos adheridos a las farolas que detectan la presencia de personas en la acera. Nuevas tecnologías como puedan ser la realidad aumentada, o los dispositivos de control automático de las funciones de los servicios urbanos, hasta automatismos que captan constantemente y registran nuestra posición etc., están poblando nuestras ciudades inteligentes enviando miles datos hacia la nube que como una esponja absorbe una ingente cantidad de información bruta a procesar a través de los avanzados sistemas de inteligencia artificial.

PEGASUS

Recientemente conocido a nivel nacional, por su escándalo político, tenemos el Spyware Pegasus. El software espía, se instala en dispositivos que ejecutan ciertas versiones de iOS (Sistema de Apple) y Android desarrollado por la firma cibernética israelí, NSO. Fue descubierta por primera vez, en agosto de 2016, después de un intento fallido de instalarlo en un iPhone perteneciente a un activista de derechos humanos, una investigación reveló detalles sobre el software espía, sus capacidades y las vulnerabilidades de seguridad que explotó. Es capaz de leer mensajes de texto, rastrear llamadas, recopilar contraseñas, rastrear la ubicación del teléfono y recopilar información de las aplicaciones.

Benjamín Netanyahu facultó recientemente la expansión por parte del Servicio de Seguridad General, tecnología de vigilancia habitualmente utilizada para la lucha contra el terrorismo, para realizar un seguimiento de personas positivas. En un primer momento, hubo negación por parte del parlamento, si bien el primer ministro la impuso con un “decreto de emergencia”. Recientemente, decenas de políticos, catalanes y españoles, han sido espiados con Pegasus. El caso, ha provocado un gran escándalo, y ha puesto sobre la mesa el debate sobre los límites de la seguridad tecnológica y el ataque de los servicios de inteligencia. En un principio, los políticos catalanes acusaron al gobierno español de utilizar Pegasus como parte de una guerra sucia para perjudicar al movimiento independentista catalán, que tiene mayoría parlamentaria en Catalunya y reclama su independencia de España. Entre los políticos espiados por el software, según los informes del Centro Criptológico, hubo dos intrusiones del programa espía Pegasus en el teléfono móvil del presidente del Gobierno, Pedro Sánchez, en mayo de 2021, y una en el de la ministra de Defensa, Margarita Robles, en junio de ese mismo año.

PRISM

Es el nombre que recibe un programa clandestino de vigilancia electrónica operado por la Agencia de Seguridad Nacional de los Estados Unidos para la recogida masiva de comunicaciones procedentes de al menos nueve grandes compañías estadounidenses de Internet. Este programa secreto, filtrado a la opinión pública en 2013, fue puesto en marcha en 2007, en el marco de la expansión de los servicios de inteligencia de Estados Unidos iniciada en 2001 tras los atentados del 11 de septiembre y el comienzo de la “guerra contra el terrorismo”. También aplica a Europa, esta herramienta de monitorización está implementada en Android y Apple. Con su uso es posible acceder al contenido de

teléfonos de forma remota, micrófono, cámara y localización sin necesidad de instalar nada, por ejemplo, en Android está implementada la puerta trasera en el Kernel y el socket de salida es el 443.

La existencia de PRISM se filtró seis años más tarde gracias al antiguo contratista de la NSA, Edward Snowden, quien advirtió que el alcance de la recopilación masiva de datos era mucho mayor de lo que la población conocía, al incluirse en el programa actividades «criminales y peligrosas». Las revelaciones empezaron a ser publicadas por *The Guardian* y *The Washington Post* el 6 de junio de 2013.[14] Los documentos posteriormente publicados demostraron los acuerdos financieros que existían entre la Special Source Operations, la división de la NSA responsable de PRISM, y las empresas estadounidenses de las que se extraían datos, que entregaban los datos a cambio de millones de dólares

C2PA

Al principio del año 2021, se anuncia por parte de Microsoft de la creación del C2PA, una red de vigilancia gigante en Internet. La definen como una alianza de empresas de tecnología y grandes medios de comunicación declarando por su parte, que su objetivo es “combatir la desinformación en las redes”.

Con esto, sería la entidad con mayor poder sobre la opinión pública que haya existido jamás.

El proyecto C2PA, como una red gigantesca de vigilancia en internet, la cual, según varios analistas, nadie podría huir a su revisión, una especie de gran “ojo” al servicio de la tecno élite. C2PA, se define como la red de certificadores de la veracidad, donde, según una publicación Microsoft del 22 de febrero de 2021, entre sus fundadores se encuentran el New York Times, la Cadena BBC, Adobe, Intel, ARM, etc. Este método de inteligencia artificial, podrá investigar la red de una forma muy poderosa, leyendo y revisando escritos, audios, fotos, pdfs, y documentos en cualquier formato; investiga las fotos y los vídeos, identifica los objetos que aparecen ahí, y también a las personas, mediante el reconocimiento facial. Podrá revisar una información y rastrear todo su recorrido, desde su origen

hasta el receptor final, así como evaluar tu escrito antes de que lo publiques, cuando todavía lo estamos tecleando en nuestras casas, leerá el recorrido de una foto o vídeo, desde el momento en el cual se toma la foto en el terminal, hasta el dispositivo receptor de la misma, rastreando todo el camino. Se identificará al autor, y a todos los consumidores de esa foto, noticia, o post, y a su vez a todos los que la hayan reenviado, quedando todos de una forma etiquetados y marcados. Unos creen que esto es bueno, que estamos ante un "buen filtro de garantía"; otros creen que será la "nueva Inquisición" condenando a la hoguera digital a los medios alternativos

2.2. Marco Legal Nacional sobre el uso de dispositivos de vigilancia digital.

La vídeo vigilancia, forma ya parte del paisaje urbano de la contemporaneidad, llenando el mercado de multitud de modelos y soluciones aplicadas tanto por las empresas privadas de seguridad como por los cuerpos públicos de seguridad, a través de cámaras de video-vigilancia, sistemas de reconocimiento de rostro, iris y voz, uso de drones, … Como se ha mencionado anteriormente, es cada vez más normal localizarlas en aeropuertos, calles céntricas, centros comerciales, o en cualquier edificio con actividad pública.

En el contexto nacional, la Agencia Española de Protección de datos, publicó, con fecha de última revisión el 12 de Julio de 2021, la Guía sobre el uso de Video Cámaras para seguridad y otras finalidades. En un apartado de su página web que clarifica las dudas que puedan surgir de la legislación aplicable, y aquellas existentes respecto a al Reglamento General de Protección de Datos y la videovigilancia, por ejemplo:

- El tratamiento de las imágenes con fines de seguridad, su legitimación y proporcionalidad.
- Supuestos específicos de tratamiento de imágenes con fines de seguridad: Fuerza y cuerpos de seguridad, Infraestructuras críticas,

Espectáculos deportivos, etc.

- Tratamiento de imágenes con fines diferentes a la seguridad: Control del tráfico, control de zonas con acceso restringido al tráfico, Sanidad y Centros educativos, etc.

- Tratamiento de imágenes a través de tecnologías emergentes: Cámaras “On Board”, Drones.

- Supuestos de no aplicación de la normativa de protección de datos: Tratamiento de imágenes en el ámbito personal y doméstico, tratamiento de imágenes por los medios de comunicación, Cámaras simuladas, etc.

La legislación española, en cuanto a videovigilancia, así como los ámbitos que pretenden regular son:

- **LO 4/1997 de 4 de agosto, regula la Videovigilancia para las Fuerzas y Cuerpos de Seguridad del Estado**. La prevención de hechos delictivos, la protección de personas y custodia de bienes, lleva a los miembros de las Fuerzas y Cuerpos de Seguridad, al empleo de medios cada vez mas sofisticados. Es oportuno regular el uso de los medios de grabación de imágenes y sonidos que vienen utilizando los miembros de las FFCCSS, introduciendo las garantías que son precisas para que el ejercicio de los derechos y libertades reconocidos en la constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública.

- **Real Decreto 596/1999, de 16 de abril, que aprueba el Reglamento de desarrollo y ejecución de la LO 4/1997**. Tras la aprobación de la LO 4/1997, es necesario dictar el presente Real Decreto, con el fin de poder desarrollar y elaborar los criterios de ejecución.

- Ley 19/2007 de 11 de junio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, en la cual se regula el uso de videovigilancia en eventos deportivos. Por medio de la contextualización histórica, se realiza un

enfoque práctico sobre la situación de violencia vivida en torno al deporte durante décadas. Dicha violencia pretende ser paliada por medio de distintas medidas preventivas y de disuasión. Aquí entra en juego la videovigilancia, sistema mediante el cual se intenta prevenir este tipo de conductas, o en su caso, localizar e identificar a sus autores.

- Real Decreto 203/2010 de 26 de febrero, que aprueba el desarrollo y ejecución de la Ley 19/2007. Debido a las diversas novedades existentes en la materia, ha sido necesario desarrollar un reglamento que contribuya a erradicar la violencia en el deporte. Este Real Decreto incorpora las modificaciones, inclusiones y adaptaciones necesarias para desarrollar la nueva ley y hacer así efectivas sus novedosas previsiones.

- Ley 5/2014, de 4 de abril de Seguridad Privada. La ley representa un tratamiento total y sistemático de la seguridad privada en su conjunto, que pretende abarcar toda la realidad del sector existente en España, al tiempo que lo prepara para el futuro. La regulación contempla, entre otros objetivos, la mejora de la eficacia en la prestación de los servicios de seguridad privada en lo relativo a organización y planificación, formación y motivación del personal de seguridad; la eliminación de las situaciones que dan lugar al intrusismo tanto de las empresas como del personal; la dotación al personal de seguridad privada del respaldo jurídico necesario para el ejercicio de sus funciones legales, y los elementos de colaboración entre la seguridad privada y la seguridad pública.

- **Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los derechos digitales**. La presente ley orgánica tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales,

amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica; y garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

2.3 Empleo de la tecnología de ciber-control, en el espacio público – privado.

	USO PÚBLICO	USO PRIVADO
VIDEOCÁMARAS	- Parkings Públicos. - Zona de tránsito - Eventos - Protección de edificios Públicos. - Control del Tránsito	- Control seguridad de empresa. - Seguridad doméstica. - Seguridad de Vehículos privados.
RECONOCIMIENTO FACIAL	- Control de personas - Realizar embarque en aeropuertos	- Sistema de pago.
DRONES	- Eventos. - Emergencias. - Búsqueda de Personas. - Vigilancia fronteriza. - Aproximación en emergencias	- Cinematografía. - Inspección de infraestructuras y construcciones. - Mapeo de zonas y vigilancia.
BIG DATA	- Salud. - Ciberseguridad. - Transporte público. - Sondeos Públicos.	- Optimización de procesos. - Control de Calidad. - Análisis de Mercado.
CIBERPATRULLAS	- Detección de actividad ilegal en la red. - Fraudes cibernéticos.	

El uso de los presentes avances tecnológicos, en cuanto a investigación, por parte de las Fuerzas y Cuerpos de Seguridad, es básico para la perseguir y resolver ilícitos, sobre todo, en los que las Tecnologías de Información y Comunicación de

importancia, por lo cual, su uso forma parte del presente y del futuro policialmente hablando.

Antiguamente, para realizar la labor policial, no se requería mucho más que un arma de fuego, sentidos, linterna y papel y boli, pero las técnicas policiales se han ido desarrollando al nivel del desarrollo de la humanidad y de la delincuencia, valiéndose actualmente de tecnología y material informático sofisticados.

La Dirección General de la Policía ha adaptado su estructura interna para responder mejor a los nuevos retos de la criminalidad, e destaca la lucha contra el cibercrimen y la innovación tecnológica a través de la creación de la Unidad de Investigación Tecnológica asumirá la investigación y persecución de los delitos a través de las tecnologías de la información y comunicación y actuará como Centro de Prevención y Respuesta del E-Crime de la Policía Nacional

En palabras de Silvia Barrera, Inspectora de la Unidad de Investigación Tecnológica de la Policía Nacional (https://www.youtube.com/watch?v=ijjBiSu57SE): "*Sin duda, internet ha marcado un antes y un después en nuestras vidas. Es maravilloso el acceso a la información. El problema es que, hay que saber usarla, la información es poder y lo que está pasando con internet, es que le estás dando a la gente mucho poder, mucha capacidad de comunicación, de llegar a la gente, y no es capaz y no sabe cómo manejar ese poder. El lado negativo no es la tecnología que se ha creado, que es maravillosa, sino en el uso que hacen de ellas ciertas personas*".

"*La Policía, utiliza herramientas, como cualquier otra persona en la red, herramientas OpenSource, que sirven para hacer búsquedas, identificaciones, monitorizaciones de perfil, de personas, de eventos, y por otra parte, otras herramientas de búsqueda más especializadas*".

Una técnica de ciber control, es el ciberpatrullaje. Se trata de un conjunto de técnicas, en su mayoría preventiva, con la finalidad de encontrar actividad ilegal en la red y descubrir a los delincuentes. No consiste solo en el monitoreo de la red, sino también en la obtención y la recolección de información el almacenamiento y el análisis del contenido que existe en la red. Se puede dividir en una observación de las redes sociales, también un rastreo de la dark net y en comprobaciones que se realizan en la web.

Hay que diferenciar, entre el ciberpatrullaje que se produce en las redes abiertas, y el que se produce en las redes privadas. En las redes abiertas, habilita a la Policía para que, al igual que se patrulla en la calle con un vehículo policial y con los distintivos, en la red se habilita de igual forma, incluso está reconocido judicialmente que el simple hecho de la Policía rastrear las redes, sin necesidad de una identificación como Policías, está también admitido. Sin embargo, en las redes privadas, en España, ya se requiere de una serie de medidas, de identificación, o de utilización de ciertos Nicks, que permite a la Policía acceder a determinados sitios privados. En ese caso, sí que judicialmente, precisamos de una autorización, que además recientemente en 2015, con la reforma de la LeCrim, se estableció el agente encubierto virtual que es una herramienta muy útil y que está siendo utilizada muchas veces en investigaciones concretas.

En el ciberpatrullaje, se pueden encontrar Fake News que son comprobadas, también grupos radicales, y todo tipo de fraudes. Una de las técnicas que más se utilizan son los esquemas de phishing. Muchas veces, se van buscando, otras veces se reciben denuncias, y otras veces la participación ciudadana que resulta fundamental.

Otro uso público del cibercontrol público, es la monitorización y reconocimiento de matrículas.

Este tipo de sistemas, cuentan con cámaras LPR (“License Plate Recognition”) cámaras ANPR (“Automátic Number Plate Recognition”). La primea de ellas, tiene la capacidad de leer la placa de matrículas, y la segunda además de ello, tiene la capacidad de ejecutar acciones cuando una de las matrículas está asociada a un listado que anteriormente hemos diseñado. El listado puede ser un listado “Blanco”, como ejemplo, los propietarios de una comunidad de vecinos, para los vehículos autorizados para acceder a un determinado lugar, o un listado “Negro”, que cuando detecte una matrícula en concreto, se genere una alarma, enviando una notificación al administrador. Un ejemplo de uso de esta tecnología, es en los parkings públicos, donde tienen la obligatoriedad de tener un registro de los vehículos que acceden asociando el número de matrícula, la hora de entrada y la hora de salida. Un ejemplo real en cuanto a uso de sistemas de reconocimiento de matrículas, fue el ocurrido en La Nucía (Alicante), en Marzo de 2008, donde fue clave para la investigación de un atropello mortal a un menor de 17 años, dada la detección de la matrícula y el dispositivo posterior, posibilitó a la Policía la detención de sus autores.

En el plano privado, a día de hoy, todas las empresas poseen asuntos confidenciales, siendo la ciberseguridad un factor crucial para cualquier empresa que quiera protegerse de la ciberdelincuencia.

En cuanto a sus usos, podemos resumir:

- Reducir peligros ante ataques: Ayuda a las empresas a prevenir un ciberataque, o a disminuir sus consecuencias. Son múltiples los ejemplos, en los cuales, hackers, acceden a registros personales, chantajeando a los interesados en difundir los datos, a cambio de una contraprestación económica.
- Detectar comentarios de la empresa en la Red: Se puede realizar un análisis de la opinión generalizada de un determinado sector de la sociedad. Por ejemplo, ver las fortalezas de la misma y ampliarlas, o detectar críticas, evitan la mala reputación de la misma.

- Prever amenazas futuras: se podría realizar un adelanto al ataque, y neutralizarlo o minimizarlo.
- Prevención del espionaje industrial: Ante la competencia desleal en cuanto a tener información confidencial de otras empresas, se pueden proteger datos sensibles de la organización o empresa. Como ejemplo el caso Huawei, donde la organización se le atribuyó la apropiación de patentes.
- Localización de fugas de información: Se pueden localizar casos, donde se transfiere de manera ilegal información de la organización. En el tema Huawei, también se mencionó, que otros trabajadores habían facilitado de forma ilegal información confidencial a
Huawei.
- Acelerar toma de decisiones.

2.4 CIBERSEGURIDAD PÚBLICA SOBRE LA CIUDADANÍA Y TECNOVIGILANCIA SOBRE LA CLIENTELA.

2.4.1. Empleo de la ciberseguridad en los cuerpos y fuerzas de seguridad pública sobre la ciudadanía.

A modo de ejemplos, en el Aeropuerto de Menorca, se utiliza un método de reconocimiento facial tanto en la zona de embarque como para acceder a los aviones. En el aeropuerto del Prat de Barcelona, a finales del 2021, puso en marcha una prueba piloto, de en principio seis meses de duración, de reconocimiento facial del pasajero, la primera de este tipo en toda Europa.

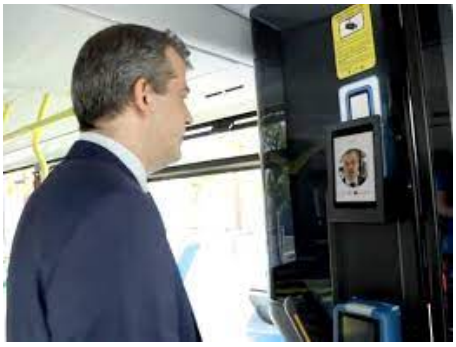
El aplicativo en cuestión, permite realizar todo el proceso de facturación y embarque, sin necesidad de mostrar documentación alguna, utilizando la biometría para asociar el rostro del

viajero a un documento de identidad y a la tarjeta de embarque.

Según unos de los precursores del proyecto "*su finalidad es viajar de modo más sencillo, ágil y eficiente, sin necesidad de dejar la maleta, ni pasar por la zona de embarque, ni entablar conversación con personal alguno, ya que al realizar el registro biométrico, se pasarán todos los registros de seguridad, almacenando los datos por parte de AENA, según el RGPD, siendo un proceso voluntario, existiendo el método tradicional, siendo esto una oferta más para mejorar la experiencia del pasajero, aprovechando la experiencia*".

Un proyecto parecido, se puso en marcha en el Aeropuerto Adolfo Suárez Madrid Barajas, a finales del 2019.

También en Madrid, concretamente la Empresa de Municipal de Transporte Público, dentro del Proyecto Madrid Mobility Movement, modernizó los sistemas de pago con el fin de facilitar a los ciudadanos el acceso al transporte público, haciendo la que movilidad urbana pueda resultar inteligente, sostenible, y conectada de una manera sencilla implementando el pago mediante reconocimiento facial, en sus líneas urbanas, convirtiéndola, en la primera ciudad europea en utiliza este sistema de pago.



En palabras del director de tecnología de la empresa, "*El hecho de poder entrar en un autobús sin tener que llevar ni tarjeta, ni teléfono ni cualquier otro medio de pago, sino que pasas con tu rostro, es una experiencia muy buena. Únicamente se tiene que registrar en una aplicación, que el usuario se tiene que hacer una foto, y registrarse con su rostro y un medio de pago, de modo que automáticamente pueda acceder a la flota de autobuses*".

En la ciudad de Madrid, se realizan anualmente más de cuatrocientos veinte millones de desplazamientos en los autobuses municipales. Varios usuarios encuestados, indican que "*Por un lado lo ven bien, porque tecnológicamente es un avance muy importante, si bien dependiendo de lo fiable que sea el uso del rostro, y de los algoritmos*".

Por parte de los responsables, se hace hincapié que todos los procesos de pago con reconocimiento facial, están amparados por la normativa europea, que revoca la existente en cada país miembro, definiendo los datos biométricos, como categorías especiales de datos personales y prohíbe su procesamiento, haciendo que las personas estén protegidas para que su información no sea compartida sin su consentimiento

En cuanto a vigilancia pública, uno de los lugares donde se utiliza el reconocimiento facial, es en la Estación Sur de Madrid. Gran estación de la capital, desde la cual se realizan traslado a todo el territorio nacional.

Los responsables de la empresa aseguran, que "*ha servido para identificar a carteristas o delincuentes habituales y reducir de manera importante el número de incidentes en el entorno*". En momentos puntuales, en el lugar se pueden congregar multitud de usuarios y viandantes, con cierto grado de dificultad desplazarse a pie en determinados momentos.

El año de implantación de la citada red, fue el 2016 y por aquel entonces, ya existían más de un centenar de cámaras, siendo 12, las que concretamente estaban destinadas a este servicio. Sus encargados, indican que ha sido un gran éxito, reduciendo de forma considerable los incidentes, pasando de cinco incidentes diarios en 2010 a uno por mes en el primer semestre de 2019.

2.4.2 Uso de la tecnovigilancia en las empresas privadas de seguridad sobre la clientela.

En cuanto al ámbito privado, en la empresa de supermercados Mercadona, instaló un sistema de reconocimiento facial en al menos cuarenta de sus establecimientos, con el fin de localizar a individuos con antecedentes por robo en sus establecimientos, o que tengan prohibido el acceso a los mismos.

Con este asunto, se ha suscitado una polémica bastante considerable, creando muchas dudas no solo en su uso, sino también en la información traslada que crea muchas dudas, como, por ejemplo, el desconocimiento, de cómo la empresa, se ha hecho con estas bases de datos que contenga la información biométrica de estos individuos ya registrados.

2.5 BENEFICIOS Y PERJUICIOS DE LAS TECNOLOGÍAS-ESPÍAS EN EL CONTEXTO DE UNA SOCIEDAD DEMOCRÁTICA.

2.5.1. De los beneficios del uso de las nuevas tecnologías de control

La política en general, se encuentra inmersa en una automatización constante, siendo ansiado que la citada automatización se incremente en el futuro. Es un asunto que suscita muchas variables en relación a como se puede ver la democracia actual.

Como aspecto positivo de estas tecnologías en la política democrática, nos encontramos por un lado la valoración de las políticas públicas y por otro ser mas conscientes de las preferencias de la sociedad.

A día de hoy, los estados, cuentan con tecnología muy potente para realizar un seguimiento exhaustivo de sus políticas. No es necesaria una organización concentrada, dirigida por expertos y burócratas, si bien, este tipo de técnicas permite examinar fuentes más diseminadas y competitivas, y en principio menos arraigadas.

Se afianza la idea de que los sistemas que deciden sin influencias humanas, son más neutrales y objetivos.

La segunda parte, sería tener constancia del deseo auténtico de la sociedad, a la que el ejecutivo debe de atender, siendo conscientes de las necesidades reales, mediante los cuales se puede constituir la intención popular. Con la tecnología, se puede individualizar la salud, energía o el transporte. Gracias a todo ello, se desmenuzan las interacciones individuales, existiendo sistemas capaces de dar respuesta a las demandas individuales. Las pretensiones de la sociedad, se pueden conocer con un alto grado de precisión, diseñando servicios de manera anticipada.

2.5.2 De los perjuicios del empleo de la innovación en ciberseguridad.

En cuanto a la problemática que se puede suscitar con estas técnicas en la democracia, es la duda que se origina de que, si estas sociedades tecnológicamente tan desarrolladas practican un paternalismo tecnológico, en virtud del cual, en el fondo “nos dicen lo que queremos oír”,
pudiendo haber una cierta manipulación, que, aunque todo esto satisfaga mucho de los deseos y necesidades, se puede estar sacrificando la capacidad de reflexionar sobre ello.

Otro problema que puede ser de importancia, es que los algoritmos que realizan predicciones, a partir de los patrones del pasado, es decir, los datos con los que se alimentan toda esta tecnología, son los datos de una sociedad actual, incluyendo toda la problemática y las desigualdades actuales, y generalmente, las predicciones se realizan sobre la base de que nuestro comportamiento en el futuro va a ser muy similar al del pasado, es decir, los algoritmos introducidos en toda esta tecnología realiza una hipótesis en función del pasado y el presente, teniendo en cuenta de que el comportamiento va a continuar siendo el mismo.

Y un problema, con todo esto, que puede ser grave en democráticamente hablando, es que la política no es una actividad que releja la realidad, es decir, los sistemas de predicción e inteligencia artificial, prestan más atención a voluntades más consumistas y débiles, en donde la extrapolación del pasado, es completamente insuficiente, y gran parte de la política es una apertura hacia el futuro, y donde los algoritmos, no pueden predecir el futuro, dado que es indeterminado, siendo los algoritmo conservadores, sin posibilidad de ruptura no valorando futuros alternativos, sino en posibilidades continuistas

Todo este tipo de tecnología, está llega de sesgos discriminatorios, es decir, satisfacer el patrón en el que encaja un individuo, no es lo mismo, que satisfacer al individuo, así como examinar a grupos poblaciones en función de las trazas o huellas que se dejan en el espacio digital, da pie a muchas posibilidades de exclusión y de manipulación

2.6. El dilema de la seguridad y la libertad en el contexto nacional.

Existe una amplia doctrina del Tribunal Constitucional referente a la protección de los Derechos fundamentales, con específica atención al Derecho a la intimidad, frente a los continuos progresos tecnológicos, pues el Tribunal Constitucional ha asegurado de forma insistente que el derecho a la intimidad ha adquirido también una dimensión positiva en relación con el libre desarrollo de la personalidad, encaminada a su plena efectividad, "*razón por la que se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada"* (STC 119/2001, de 29 de mayo).

El principal exponente de la ponderación elaborada por nuestro Tribunal Constitucional entre la defensa de los derechos fundamentales de la persona y el empleo de la tecnología, cuando se persigue un fin legítimo como es la

investigación criminal por parte de las autoridades judiciales y policiales, lo simboliza la STC 173/2011, de 7 de noviembre, en donde expresamente se pronuncia sobre la necesidad de establecer una serie de garantías frente a los peligros que existen para los derechos y libertades públicas -en particular, la intimidad personal- a causa del uso ilícito de la información así como de las TIC durante la investigación criminal. Una de las mayores preocupaciones del intérprete español también gira en torno a la viable eliminación de cualquier foco de privacidad de los individuos con motivo del depósito y cruce masivo de datos gracias a las posibilidades que ofrece la informática, con el riesgo de crear «perfiles integrales de la personalidad» de los ciudadanos. Por lo tanto, el Tribunal Constitucional considera preciso establecer una serie de garantías frente a los peligros que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información, y dispone que cualquier indiscreción en el contenido de un computador personal deberá venir legitimada, en principio, por el aprobación de su titular, o bien por una previa resolución judicial, salvo en los casos en los que se valore necesaria y urgente la actuación policial, porque entiende que “el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.), no sólo forma parte de este mismo ámbito, sino que además, a través de su observación por los demás, pueden descubrirse aspectos de la esfera más íntima del ser humano.

Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico (…), está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad, por referirse a pensamientos, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente

descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona".

(fuente: *La investigación del delito en la era digital (https://eprints.ucm.es/id/eprint/64640/1/ORTIZ%20PRADILLO%202013%20la%20investigacion%20del%20delito%20en%20la%20era%20digital.pdf)*

3. RESULTADOS DE LA APLICACIÓN DE UNA ENCUESTA EN TORNO A LA PROBLEMÁTICA.

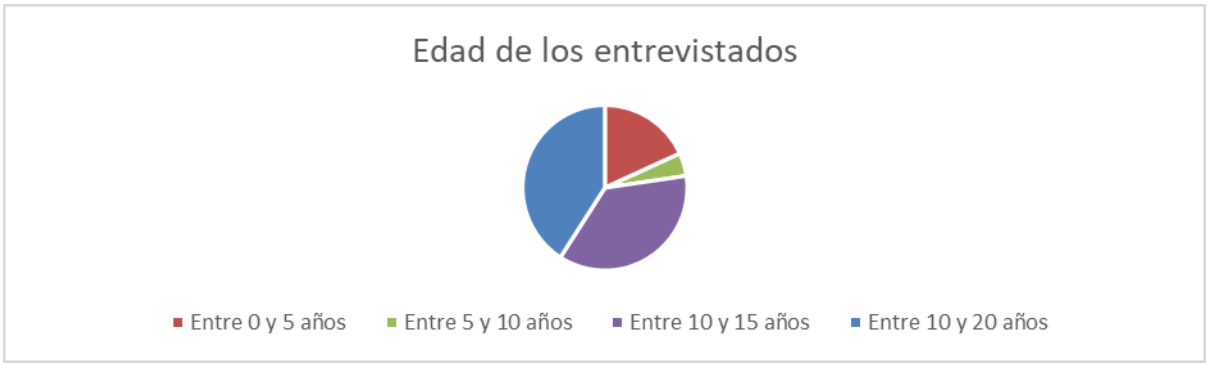
La encuesta realizada estuvo dirigida a una muestra de 50 personas, todas ellas trabajadores integrantes de los Cuerpos de Seguridad Pública, que se desglosan por distintos criterios a efectos clasificatorios:

a. Por Cuerpos Policiales.

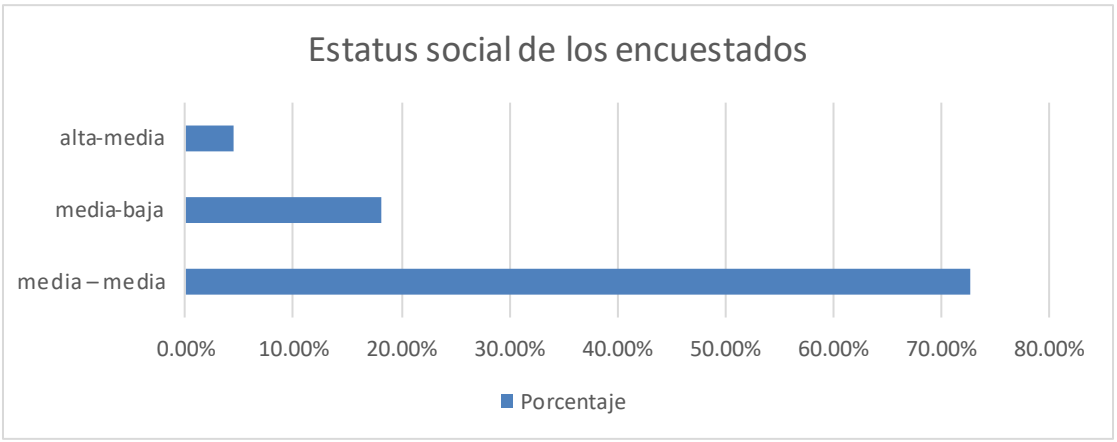
De los sondeados, un 81% pertenecen a los Cuerpos de la Policía Local, un 9.1% a la Policía Nacional y un 9,1 % a la Guardia Civil.

b. Por años en activo:

Del conjunto de los encuestados, un 40’9 % lleva entre 10 y 20 años ejerciendo de agente de seguridad, un 36’4% lleva un 18’2% entre 0 y 5 años, y un 4’5% entre 5 y 10 años.



c. Por estatus social percibido, un 72,7% se identifica con la clase social media – media, un 18,2% con media-baja, un 4,5% con alta-media, y un 4,5% con media-alta.



El objetivo de la encuesta apunta a la diana de captar cuál es la percepción que tienen actualmente los cuerpos policiales de seguridad españoles en relación al conocimiento de los nuevos dispositivos de ciber-seguridad y tecno-control, aplicados en contextos nacionales como España y China con regímenes políticos tan distintos como puedan ser una democracia y una autocracia, respectivamente a fin de ofrecer un contrapunteo entre ambos marcos.

1ª PREGUNTA: ¿CONOCES LA SEGURIDAD PREVENTIVA? EN CASO AFIRMATIVO, MOTIVE SU RESPUESTA.

A tenor de la primera pregunta planteada del conocimiento de la seguridad predictiva, un 63% ha respondido que no la conoce, siendo una cuestión que aun parece no haber permeado con la suficiente profundidad en los diversos cuerpos policiales españoles. El 17% restante, afirma saber, que, mediante la seguridad, se realiza un análisis con la intención de conocer eventuales situaciones críticas o de seguridad, con el fin de poder prevenir situaciones reales críticas en lo que a seguridad pública se refiere, de tal modo que predecir se asocia con la idea funcional de prevenir el delito.

2ª PREGUNTA: EN CASO AFIRMATIVO, ¿QUÉ ASPECTOS POSITIVOS PODRÍA APORTAR AL PANORAMA ACTUAL O FUTURO EN NUESTRO PAÍS?

En cuanto a los aspectos positivos a introducir con tales dispositivos en el panorama actual o futuro, los encuestados responden con una doble afirmación que se niega en su contradicción por parte de un 17% de los sondeados. Por un lado se alude al hecho de que la incorporación de la nueva tecnología supondría una notable mejora de la gestión policial para reducir el índice delincuencia, pero por otro lado se expresa la dificultad de la implantación de estas novedosas medidas de seguridad debido a la escasa inversión pública en este tipo de concepto por lo que en nuestro país sería muy complicada su implantación y/o desarrollo.

3ª PREGUNTA: ¿QUÉ CONOCIMIENTOS TIENE USTED ACERCA DE LOS SISTEMAS DE CIBER-VIGILANCIA EN CHINA? ¿QUÉ INFORMACIÓN TIENE AL RESPECTO?

En relación a la tercera de las cuestiones planteadas se advierte el amplio desconocimiento de la aplicación de estos dispositivos de tecno-control en contextos autocráticos como la República Popular China, dado que un 72% de los encuestados reconoce no tener ningún tipo de conocimientos sobre el uso y abuso de tales medidas, mientras que el resto afirma tener muy poca información al respecto.

4ª PREGUNTA: ¿CONOCE USTED DE LA EXISTENCIA DE UN SISTEMA DE INTELIGENCIA ESPAÑOL? EN CASO AFIRMATIVO, ¿QUÉ INSTITUCIONES CONOCE EN NUESTRO PAÍS QUE SE ENCARGEN DE ESTE COMETIDO?

En este punto las respuestas son más variopintas. El 36,5 % del conjunto de los interrogados no conoce ningún sistema de inteligencia nacional, mientras que un 59% de quienes responden a esta encuesta afirman conocer la existencia del Sistema de Inteligencia Español (CNI). Más allá, un 4,5% es capaz de reconocer además otros servicios de inteligencia como puedan ser los de las FFCCSS.

5ª PREGUNTA: ¿QUÉ OPINAS DEL USO DEL BIG DATA EN EL SECTOR PÚBLICO?

Los encuestados, opinan del uso del Big Data en el sector público que su implementación debería ser prioritaria para mejorar la gestión de las políticas públicas de seguridad, tanto en la toma de decisiones como en la gestión con criterios de eficiencia, así como que su uso puede ayudar a los ciudadanos, siempre que se garantice la seguridad de sus datos. Ello exige tener un control externo y una fiscalización auditora con el fin de evitar abusos o excesos por parte del Estado.

6ª PREGUNTA: ¿QUÉ OPINIÓN TIENES DE LA TECNOLOGÍA EN LA SEGURIDAD DIGITAL/ELECTRÓNICA EN EL PLANO NACIONAL?

Acerca de la tecnología en seguridad digital/electrónica en el plano nacional, los encuestados relatan que se trata de un reto tecnológico a afrontar pese a que en la actualidad se halla muy lejos de alcanzar a un nivel óptimo. En este sentido, se trata de una debilidad fácilmente aprovechable para quienes se quieran beneficiar de tales déficits para cometer ciber-delitos , siendo una materia imprescindible, en donde aún queda mucho por hacer.

7ª PREGUNTA: ¿CONOCES EL POLICE CLOUD?. EN CASO AFIRMATIVO…

En cuanto al Police Cloud o nube policial, el 100% de los encuestados desconoce su existencia, así como su funcionamiento, lo cual vuelve a confirmar el grado de desconocimiento de los agentes policiales en la materia estudiada.

8ª PREGUNTA: ¿CONOCES EL INTERNET DE LAS COSAS?...

Del total de los agentes encuestados el 56% carece de conocimiento alguno del internet de las cosas. El resto de los sondeados opina que son dispositivos, que poseen la capacidad de conectarse a internet, e interactuar con otros dispositivos similares, siendo válidos para facilitar las tareas cotidianas, poseyendo sensores, memorias, permitiéndoles tener determinada autonomía. El conocimiento de esta tecnología procede básicamente del ámbito doméstico más que del policial.

9ª PREGUNTA. DE LAS SIGUIENTES TECNOLOGÍAS, ¿USAS ALGUNA DE ELLAS A NIVEL PROFESIONAL? ¿QUÉ USO LE DAS? ¿QUÉ PROS Y CONTRAS OBSERVAS EN ELLAS? A). VIDEOCÁMARAS B) RECONOCIMIENTO FACIAL, VOZ, IRIS. C) DRONES. D) BIG DATA E) CIBERPATRULLAJE:

El 26% ni las utiliza, ni tiene conocimiento acerca de ellas, pues tal como dice la una herramienta fantástica para ejercer la labor policial. En el caso de las videocámaras para grabar las actuaciones policiales con el fin de aportar un elemento para consabida máxima 'ni están, ni se las espera'. En cambio, el resto de los sondeados piensan que permiten objetivar cualquier proceso, valorando la eficacia de las videocámaras a la hora de aplicarla sobre el ámbito de la vigilancia del tráfico; o el uso de los drones como dispositivos útiles para el intensificar el control y salvamento en zonas y lugares poco accesibles para mejorar la efectividad de las patrullas, si bien todas estas tecnologías deberían adecuarse al marco normativo al respecto.

10ª PREGUNTA: ¿PIENSA QUE TIENEN CABIDA EN LA ACTUALIDAD Y EN EL FUTURO ESTE TIPO DE TECNOLOGÍAS EN EL PANORAMA MARCO LEGAL NACIOANL? TANTO EN CASO NEGATIVO COMO POSITIVO, MOTIVE SU RESPUESTA:

Si tienen cabida o no en la actualidad y en el futuro este tipo de tecnologías en el panorama marca legal nacional, los sondeados manifiestan su acuerdo en el uso de las mismas, al servicio de las fuerzas y cuerpos de seguridad, facilitando buenos resultados dando celeridad a la resolución de problemas como tecno-estrategia en la lucha e investigación de la criminalidad, siempre y cuando se apliquen dentro de la legalidad.

CONCLUSIONES.

La primera conclusión a entresacar se refiere al alto grado de desconocimiento por parte de las Cuerpos y Fuerzas de Seguridad Pública sobre la cuestión de la seguridad predictiva y su aplicación en términos lesivos contra los derechos ciudadanos en contextos internacionales asociados a regímenes autocráticos, como pueda ser la R.P. China como ejemplo paradigmático.

La segunda cuestión a extraer de este sondeo se refiere a la escasa información que los agentes de los diferentes cuerpos de seguridad tienen sobre los servicios nacionales de inteligencia, detectándose un bajo nivel de penetración de estas instancias en las actividades policiales actuales.

La tercera y última reflexión resalta el interés por incorporar tales dispositivos electrónicos de ciber-vigilancia y tecno-control por parte de los encuestados, siempre y cuando se apliquen dentro del orden legal establecido a fin de evitar todo tipo de abusos y excesos al desplegarse sobre un país como España dentro de un contexto democrático.

4. CONCLUSIONES FINALES

4.1. Sobre los imaginarios del panóptico en China y España: Datos y Relatos.

A día de hoy, seis universidades chinas están entre las 100 principales del mundo, clasificación realizada por Times Higher Education. Con este potencial intelectual y científico, China ya no solo es el laboratorio industrial del planeta, un sino que ambiciona ser el número uno tecnológico del capitalismo cognitivo, por supuesto siempre bajo la dirección vigilante del Partido Comunista.

El nivel de inversión e innovación planificada por las empresas chinas y por el aparato político en esferas como la inteligencia artificial, el 5g, el Big Data, las tecnologías de reconocimiento facial o el potencial vertiginoso de la informática cuántica podría ser incuantificable.

Por todo ello, se plantean incógnitas complejas, sobre las interacciones y las posibles asociaciones entre un sistema especializado futurista y un modelo político-civilizacional sui generis, que armoniza hiperdesarrollo y arraigos milenarios.

Los proyectos de ciudades inteligentes abarcan todas las características de los varios sistemas de vigilancia y permiten a China resolver una serie de problemas, en primer lugar, el control de la población. Se supone que estas" ciudades inteligentes" tendrán un alto nivel de sustentabilidad ambiental.

En la última Asamblea General de las Naciones Unidas, celebrada el 22 de septiembre, el presidente Xi Jinping anunció que China quiere alcanzar un equilibrio entre las emisiones y la absorción de dióxido de carbono en 2060. Un "compromiso", que puede ayudar a todo el planeta reducir las emisiones y a iniciar unas intenciones energéticas realmente alternativas

A través del crédito social, comportamiento social y la confianza en la ciudadanía, se realizará una selección social a través de los precios de la vivienda y del costo de vida en general.

Existirán nuevos sistemas de planificación urbana, y de nuevos modelos de ciudadanía, donde solo los más ricos podrán vivir en ciudades inteligentes, solo teniendo acceso a ellas los que tengan mejor “puntuaje”.

Aquí en España, parece alarmante, pero si recapacitamos en todas las ocasiones en que somos valorados y examinamos a los demás con sistemas de categorización, no estamos tan lejos del modelo chino. Por el momento, en Occidente, nos valoramos entre ciudadanos; en China, es un proceso que viene de arriba.

4.2. Sobre el marco legal y la aplicación de los distintos tipos de dispositivos utilizados en ambos países.

En China, el 20 de julio de 2017 el Consejo de Estado arrojó el Plan de desarrollo de Inteligencia Artificial de futura generación, donde crearon objetivos estratégicos a largo plazo (2030) el cual contiene medidas de garantía, como el progreso de un sistema regulador y el fortalecimiento de la defensa intelectual, que permita iniciar el progreso de la Inteligencia Artificial.

Actualmente, la oficina de patentes ha esbozado una normativa que esclarezca asuntos como la elaboración de reclamaciones, la propaganda de los inventos y la posibilidad de negocio de patentes registradas. Además, China ha entrado en la cuestión de la Inteligencia Artificial, elaborando 15 puntos llamado los “principios de Pekín de Inteligencia Artificial” por la Academia de Pekín de Inteligencia Artificial (BAAI), apoyada por el Ministerio de Ciencia y Tecnología y el ayuntamiento de la capital, en colaboración con los principales centros y empresas de IA, publicado a mediado de 2019 donde trata algunos principios para la

investigación y el desarrollo de la Inteligencia Artificial, como: la privacidad, la libertad, autonomía, la dignidad y los derechos humanos, como referentes para la investigación y el desarrollo de la Inteligencia Artificial, afirmando, que "*El desarrollo de la Inteligencia Artificial, debe reflejar la diversidad y la inclusión, y debe de diseñarse para beneficiar a la mayor cantidad de personas posibles, especialmente a aquellos, que de lo contrario serían fácilmente descuidados o insuficientemente representados*".

La Declaración Universal de los Derechos Humanos determina, en el artículo 12, que "*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*"

En España hay un alto grado de europeización de sus políticas públicas, es decir, la estrategia sobre Inteligencia Artificial en el caso español se adhiere plenamente a los planteamientos de la UE. A nivel organizativo, destaca la creación de una Secretaría de Estado de Digitalización e Inteligencia Artificial, dentro del Ministerio de Asuntos Económicos y Transformación Digital. Este dato es clave, no solo por ser la primera vez que en España existe un órgano político de este nivel con la competencia directa de desarrollar la Inteligencia Artificial, sino también lo es por el hecho de conectar la Inteligencia Artificial desde los gobiernos y administraciones públicas. De hecho, será esencial la colaboración con la secretaria general de Administración Digital, tal y como se está mostrando con algunas de las medidas adoptadas durante la crisis del COVID -19 (incluyendo la app de trazado y rastreo Radar COVID) o la creación de la Oficina del Dato y sus proyectos asociados.

La publicación de la Estrategia Nacional de Inteligencia Artificial (ENIA) y su directo alineamiento con el marco europeo de Inteligencia Artificial, junto con algunas de las medidas ya puestas en marcha (carta de derechos digitales o la creación de un consejo asesor de IA) y otras que se mencionan (sandboxes,

gobtechlab, ecosistemas de datos para uso sectorial tanto público como privado, etc.) van en buena dirección.

Sin embargo, será necesario algo más de tiempo para caracterizar la política de Inteligencia Artificial en España, su alcance y, desde luego, los resultados de la misma. Finalmente, también es crítico conocer la visión de los actores impulsores, sobre todo, los responsables TIC ministeriales (CIOs) españoles. Como responsables de la definición e implantación de las políticas tecnológicas dentro de sus organizaciones, disponer de evidencia sobre sus percepciones es esencial para comprender las potenciales limitaciones y oportunidades de la IA en las administraciones públicas españolas.

4.3. Sobre los distintos puntos de equilibrio entre seguridad y libertad: "A la china" y "A la española".

4.3.1. La inclinación autocrática hacia la seguridad frente a la privacidad.

Las razones de seguridad son una de las razones habitualmente esgrimidas para limitar los derechos, lo cual suele estar previsto en el derecho positivo. Son múltiples las normas que citan la seguridad como justificación de posibles restricciones, también en el ámbito del Derecho Internacional de los derechos humanos.

En China, en la actualidad, con el fin de tener acceso a una vida digital, sus usuarios deben de aceptar una política de tratamiento de sus datos personales sobre la que no pueden negociar, supone ceder toda la información generada por los usuarios a las empresas de tecnología.

El 7 de noviembre de 2017, se promulgó la Ley de Ciberseguridad, dando soporte legal, a las medidas de monitorización y control de tráfico en internet con el que cuenta el gobierno chino.

A modo de ejemplo, en cuanto a los derechos de los cibernautas, la libertad de expresión se encuentra vetada ante la prohibición del tratamiento de ciertos temas, imponiéndose un sistema de monitorización, mediante el cual los registros de actividad en la red, deben de guardarse durante seis meses, por lo tanto, el Gobierno Chino cuenta con todos los mecanismos para investigar las actividades llevadas a cabo por sus ciudadanos.

A título comparativo, los contenidos de la normativa china, aparecen distribuidos en los articulados de las siguientes normas españolas: Ley Orgánica de protección de datos, Reglamento de desarrollo de la LOPD, Ley de servicios de la sociedad de la Información, Ley General de telecomunicaciones, Ley de protección de infraestructuras críticas, Código civil, Código penal, esquema nacional de seguridad y Estrategia nacional de ciberseguridad

4.3.2. La orientación democrática hacia la libertad frente a la seguridad.

En Europa, por tanto, en España, sería necesario establecer una política común y única sobre el Big Data, es decir, deberían de ser gestionados como un bien común.
En 1981, por parte de Alemania, España, Francia, Noruega y Suecia, se celebró el Convenio No. 108, “para la protección de las personas con respecto al tratamiento de datos automatizados de carácter personal”, mediante el cual se gestiona el respeto a la intimidad y a la vida privada de los ciudadanos a través de la protección de sus datos personales, y se crea a favor del ciudadano afectado la posibilidad de presentar un recurso como garantía de protección de esos derechos detallados en el Convenio.

La Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea (UE), la Agencia Espacial Europea (ESA) y la Organización Conjunta de Cooperación en materia de Armamento (OCCAR), de las cuales España forma parte desarrollaron

un esquema, y la normativa correspondiente, para la protección de la Información Clasificada, la cual se destina a las personas, las instalaciones, los sistemas de información y comunicación y las empresas que han de acceder, manipular o crear dicha Información Clasificada.

En la Ley 36/2015 de 28 de Septiembre, de Seguridad nacional, concretamente en su artículo 3, define a la Seguridad Nacional como: "*la acción del Estado dirigida a proteger la libertad, los derechos y el bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que hasta la fecha no había sido objeto de una regulación normativa integral*"

La entrada en vigor de la Estrategia de Seguridad Nacional 2017 estableció que "se abordará el diseño de la posición estratégica nacional respecto de la gobernanza y uso de los espacios comunes globales". Con este objetivo, se complementará, en primer lugar, la arquitectura orgánica y gobierno del Consejo de Seguridad Nacional con la génesis de un Consejo de Seguridad Aeroespacial. Y en segundo lugar, se ajustará el marco estratégico sectorial de los denominados espacios comunes a esta nueva Estrategia; supuesto que obligará tanto a revisar la vigente Estrategia de Seguridad Marítima Nacional y de Ciberseguridad Nacional como la Estrategia de Seguridad Energética Nacional, así como el desarrollo de una Estrategia de Seguridad Aeroespacial Nacional.

4.4. Sobre los escenarios de futuro ante el avance de la Ciber-Seguridad.

Muy posiblemente, el futuro se describa en China, es una especie de capitalismo de vigilancia bajo el control del Partido-Estado, con una forma sui generis de sinergia público-privada y un nivel relativamente alto de aceptación social, que tiene incluido un profundo arraigo histórico, en términos de la cultura del «buen gobierno» y las expectativas de los gobernados. Por ejemplo, durante la

pandemia, ha habido una manifestación concordando alta tecnología con congregación de aglomeraciones. Y ante esto, hay nuevas posibilidades para las empresas de alta tecnología, teniendo una oportunidad histórica de maximizar la primordial materia prima de sus creaciones: los datos.

Aquí en Occidente, en Europa, por lo tanto, correlativamente en España, se podría, establecer una política unitaria del Big Data, gestionando los datos como un bien común, de forma transparente, y por la colectividad, y evitar que Europa se encuentre en medio de la batalla entre China y Estados Unidos. Todas estas cuestiones, pueden ser motivo de desavenencias políticas.

Del mismo modo, un uso inadecuado de la Inteligencia Artificial, puede dar lugar a sentimiento de sentirse amenazado entre países, en lo que al ataque a su seguridad y sus datos se refiere, pudiendo dar lugar a ciberataques, o a una guerra, con el fin de ganar la batalla hacia la inteligencia artificial.

Otra cuestión a tener en cuenta, es que el uso excesivo de estos métodos puede crear inseguridad en la población y falta de ética por parte de los gobiernos de los países que las utilice, con el fin de tener control total sobre su población, siendo necesario que se apliquen límites en cuanto al uso y perfeccionamiento de la IA, para que el resto de países no puedan usar de manera desmedida esta tecnología, con el fin de desplegar sus fortalezas.

WEB- BIBLIOGRAFÍA.

- *Vulnerabilidad y Cultura Digital. Riesgos y Oportunidades de la Sociedad Hiperconectada*. (https://ebookcentral-proquest-

com.publicaciones.umh.es/lib/bibliotecaumh-ebooks/detail.action?docID=6484091&query=SEGURIDAD+AND+LIBERTAD+AND+CHINA+AND+CIBER+AND+TECNOLOG%C3%8DA)

- *Red Mirror ¿Qué futuro se escribe en china?* (https://static.nuso.org/media/articles/downloads/5.TC_Saint-Upery_290.pdf-)
- *Inteligencia Artificial y su afectación en China* (https://www.researchgate.net/profile/Shania-Leon-2/publication/344379536_INTELIGENCIA_ARTIFICIAL_Y_SU_AFECTACION_EN_CHINA/links/5f6e1c42299bf1b53ef151a3/INTELIGENCIA-ARTIFICIAL-Y-SU-AFECTACION-EN-CHINA.pdf).
- *La videovigilancia con reconocimiento facial en España tras la RGPD.* (http://openaccess.uoc.edu/webapps/o2/handle/10609/108826).
- *Big Data en China.* (file:///E:/Descargas/6485-Texto%20del%20art%C3%ADculo-6526-1-10-20181004.pdf)
- *Panóptico Digital. La falsa percepción de privacidad en Internet* (https://psicoeducativa.iztacala.unam.mx/revista/index.php/rpsicoedu/article/view/68)
- *Discriminación 4.0: una aproximación a los problemas que suscita la biometría y los sistemas de reconocimiento facial.* (https://201.131.47.130/index.php/ridh/article/view/670/986)

La pandemia COVID-19, distanciamiento social, el uso de tecnologías de la información y comunicación, y la falta de regulación internacional que proteja los datos personales. (https://repositorio.lasalle.mx/handle/lasalle/1695).

- *La privacidad en las ciudades inteligentes.* (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2145-77192019000200675)
- *El reto de proteger nuestros datos, aún no resuelto por las leyes.* (https://www.sport.es/es/noticias/economia/reto-proteger-datos-resuelto-leyes-13240802).

- *Ética e inteligencia artificial. Una discusión jurídica.* (https://idus.us.es/handle/11441/111541).
- *Dilemas éticos en el uso de la inteligencia artificial*. (https://www.scielo.sa.cr/scielo.php?pid=S2215-34032020000100093&script=sci_arttext)
- *Decálogo de la inteligencia artificial ética y responsable en la Unión Europea* (http://www.aidaargentina.com/wp-content/uploads/Dec%C3%A1logo_de_la_inteligen...-1.pdf).
- *El impacto de la inteligencia artificial en la democracia* https://cadmus.eui.eu/bitstream/handle/1814/69688/1526-Texto%20del%20art%C3%ADculo-1894-1-10-20201229.pdf?sequence=1
- *Ética de la inteligencia artificial.* https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-M-2019-10037900394
- *Hacia el Humanismo Digital. Desde un denominador común para la Ciber Ética y la Ética de la Inteligencia Artificial.* https://repositorio.comillas.edu/xmlui/handle/11531/61801
- *La Política Europea frente al desafía chino* https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/comentario-esteban-oteroiglesias-politica-europea-frente-al-desafio-chino.pdf

- *Rastreo de contagios: la controvertida aplicación que busca sacarnos del confinamiento*

https://elpais.com/tecnologia/2020-04-26/rastreo-de-contagios-la-controvertida-aplicacion-que-busca-sacarnos-del-confinamiento.html

- *Inteligencia Artificial como herramienta de estrategia de seguridad y seguridad para defensas de los Estados.* https://revista.esup.edu.pe/RESUP/article/view/67

- *Disrupción tecnológica y democracia en el siglo XXI.*

https://www.cuestionessociologia.fahce.unlp.edu.ar/article/download/cse125/14622?inline=1

- *FACEBOOK EN LA SOCIEDAD DE CONTROL Aplicación simultánea del panóptico y del sinóptico en un dispositivo de vigilancia y control social*

https://repository.eafit.edu.co/bitstream/handle/10784/12349/Emilio_ManjarresChavarriag_20 7.pdf?sequence=2

- *Sociedad de Control y Panóptico Electrónico. La Victima de la Videovigilancia*

http://repositorio.ucam.edu/bitstream/handle/10952/3839/Tesis.pdf?sequence=1&isAllowed=y

- *Los datos y la inteligencia artificial en la lucha contra el COVID-19*

http://www.sciencesecuritylab.com/publicaciones/previous/3

- *El proyecto C2PA y sus implicancias con el derecho a la libertad de pensamiento y expresión(*)*

https://www.derechoycambiosocial.com/anexos/MISCELANEA/2021/El_proyecto_C2PA.pdf

- *La investigación del delito en la era digital Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*

https://eprints.ucm.es/id/eprint/64640/1/ORTIZ%20PRADILLO%202013%20la%20investigacion%20del%20delito%20en%20la%20era%20digital.pdf

- *¿Qué es el ciberpatrullaje?*

https://www.youtube.com/watch?v=0fXVnfYtJSA

- *Cámaras de reconocimiento de matrículas*

https://www.youtube.com/watch?v=PkskYo9ZNSE

- Estudio Comparativo de un marco legal y normativas vigentes aplicadas en la inteligencia artificial dentro del panorama nacional e internacional.

https://repositorio.pucese.edu.ec/bitstream/123456789/2604/1/Maffare%20Corozo%20Joselyn%20Ivonne.pdf

- *Videovigilancia e inteligencia artificial: Entre la utopía y la distopía*. https://revistaciencias.inacipe.gob.mx/index.php/02/article/view/432/346

- *Ciberseguridad en China*
file:///E:/Descargas/Dialnet-CiberseguridadEnChina-6057663.pdf

- *El derecho de acceso a la Información Nacional y supranacional. Los casos de España y panamá y el difícil equilibrio entre lo Open y la salvaguarda de la seguridad.*
http://repositorio.ucam.edu/bitstream/handle/10952/4017/Tesis.pdf?sequence=1&isAllowed=y

- *BIG DATA, COMUNICACIÓN Y CONSUMO: DEL PANOPTISMO BENTHAMIANO AL PANOPTISMO DIGITAL.*

https://digibug.ugr.es/bitstream/handle/10481/66637/LIBRO-REFLEXIONES%20EN%20TORNO%20COMUNICACION.pdf?sequence=2&isAllowed=y#page=63

- *República Popular de China*
https://es.wikipedia.org/wiki/Rep%C3%BAblica_Popular_China#Problemas_sociopol%C3%ADticos_y_derechos_humanos

- *Las tic y la cibersoberanía en china: la base del presidente Xi Jinping para perfeccionar el control social*
http://openaccess.uoc.edu/webapps/o2/bitstream/10609/83827/6/oaribauTFM0618memoria.pdf

- *Las gated communities como expresión de los nuevos contextos urbanos y socioculturales: un estado de la cuestión*

file:///E:/Descargas/6924-Texto%20del%20art%C3%ADculo-7007-1-10-20110531.PDF

- *El urbanismo "antiurbano" maoísta en la China Popular 1949-1976*

https://revistaizquierda.com/images/easyblog_articles/415/izq0060_a08.pdf

- *El estado de vigilancia de alta tecnología de China: un «despotismo digital»*

https://es.bitterwinter.org/el-estado-de-vigilancia-de-alta-tecnologia-de-china/

- *Sky Net: el Gran Hermano chino que vigila con 20 millones de cámaras inteligentes*

https://www.eldiario.es/tecnologia/sky-net-gran-hermano-china_1_3173654.html

- Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana.
https://revistaseug.ugr.es/index.php/cridi/article/view/20899/20280.

- Los sistemas de reconocimiento facial, una mirada a la luz del examen de proporcionalidad.
https://ojs.austral.edu.ar/index.php/ridh/article/view/664/987

- China. Los sistemas de 'Big Data' de la policía viola la privacidad y apunta a la disidencia.

https://www-hrw-org.translate.goog/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc

- La sustentabilidad de Internet de las Cosas

http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1853-35232018000500004

- *INTERNET DE LAS COSAS. PRIVACIDAD Y SEGURIDAD*

https://tauja.ujaen.es/bitstream/10953.1/4008/1/TFG_G%c3%b3mez_Padilla%2c%20Lorenzo.pdf

- *La sociología de la sociedad del riesgo: Ulrick Beck y sus críticos.*

file:///E:/Descargas/Dialnet-LaSociologiaDeLaSociedadDelRiesgo-3288983.pdf

- ***¿Qué es Pegasus y a qué políticos ha espiado?***

https://www.elmundo.es/espana/2022/05/02/626f90fefdddffaba38b45b5.html

- *Pegasus: el programa que espía a políticos y gobiernos*

https://www.lavanguardia.com/vida/junior-report/20220509/8248278/pegasus-espionaje-politicos-gobiernos.html

- *PRISM*

https://es.wikipedia.org/wiki/PRISM

- *Análisis y desarrollo de la "Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la tolerancia en el deporte", con especial hincapié en la violencia en torno a los clubs de fútbol.*

https://repositorio.unican.es/xmlui/bitstream/handle/10902/18857/ARIZTEGUIHOYAJORGE.pdf?sequence=1&isAllowed=y