SCIO. Revista de Filosofía, n.º 20, Julio de 2021, 93-146, ISSN: 1887-9853

FUNDAMENTOS LEGALES DE LAS TÉCNICAS DE CONTROL POLÍTICO Y SOCIAL.
EL CAPITALISMO DE VIGILANCIA EN LA ERA POS-COVID

LEGAL FOUNDATIONS OF THE TECHNIQUES OF POLITICAL AND SOCIAL CONTROL.
SURVEILLANCE CAPITALISM IN THE POST-COVID ERA

Francisco J. Hernández Guerrero[a*]

Fecha de recepción y aceptación: 12 de febrero de 2021 y 11 de junio de 2021

DOI: https://doi.org/10.46583/scio_2021.20.806

A mi amigo Ángel Gómez de Ágreda, inspirador de muchas palabras de este estudio.

Resumen: La crisis sanitaria del SARS2-COVID ha traído a nuestra atención el conflicto permanente entre lo público y lo privado; entre los métodos de gestión abordados desde la perspectiva tecnológica sin concesiones a los derechos y libertades fundamentales, y las posiciones éticas que aún pretenden sostener su validez. Desde la aplicación de la tecnología en las mayores barbaries conocidas por la humanidad hasta el día de hoy, el ser humano se debate entre mayor seguridad o más libertad. El problema es que el individuo, o las organizaciones y empresas que crea, han visto incrementada su capacidad de obrar gracias a la tecnología informática, y esta nueva situación ha dado lugar a la ruptura del pacto social originado por la Revolución francesa, donde el

[a] Fiscal Delegado de Criminalidad Informática. Fiscalía Provincial de Granada

[*] Correspondencia: Juzgados La Caleta. Avenida del Sur 5, Ed. La Caleta, 7.ª planta. 18014 Granada. España.

E-mail: franciscojose.hernandez@fiscal.es

monopolio del poder se atribuía al Estado a cambio de que este se sometiera a la voluntad del pueblo expresada por medio de la ley. Hoy día, el individuo se ha vuelto más poderoso y el Estado se resiste a perder su papel. Entre esos dos polos navega la vida de miles de millones de personas, cuyas vidas se han vuelto transparentes a los ojos vigilantes de los Estados y de las grandes corporaciones empresariales.

Palabras clave: vigilancia masiva, algoritmos, comunicaciones electrónicas, protección de datos personales, capitalismo de la vigilancia.

Abstract: The SARS2-COVID health crisis has made evident the permanent conflict between what is public and what is private: on the one hand, there are the technological management methods without regard for fundamental rights and freedoms and, on the other, the ethical positions that still seek to defend them. Since the application of technology in the greatest barbarities carried out by Humanity until today, the human being is debated between more security or more freedom. The problem is that the individual, organizations and companies have seen their ability to act increased thanks to computer technology. This new situation has led to the breaking of the social pact originated by the French Revolution. In this pact, the monopoly of power was attributed to the State in exchange for its submitting to the will of the people expressed through the law. Today the individual has become more powerful and the state is reluctant to lose its role. Between these two poles navigate the lives of billions of people, whose lives have become transparent to the vigilant eyes of states and large business corporations.

Keywords: mass surveillance, algorithms, electronic communications, personal data protection, surveillance capitalism.

ABREVIATURAS EMPLEADAS

AEPD	Agencia Española de Protección de Datos
BOE	Boletín Oficial del Estado
CEDH	Convenio Europeo de Derechos Humanos
CERN	Oficina Europea para la Investigación Nuclear
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CP	Código Penal

DOCE	Diario Oficial de la Comunidad Europea
INE	Instituto Nacional de Estadística
LECr	Ley de Enjuiciamiento Criminal
LOPDPGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
LOPJ	Ley Orgánica del Poder Judicial
OCDE	Organización para la Cooperación y el Desarrollo Europeo
PNR	Passenger Name Records: Registro de Nombres de Pasajeros
RGPD	Reglamento General de Protección de Datos
STS	Sentencia Tribunal Supremo
STC	Sentencia del Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
TEDH	Tribunal Europeo de Derechos Humanos
SCS	Sistema de Crédito Social (Chengxin wenhua)

§1. Introducción

Nuestra vida diaria discurre en esa transición entre los átomos y los *bytes*, como reflejara Nicholas Negroponte en el momento de la emergencia de las tecnologías informáticas. Pero esa modificación de la naturaleza de nuestra vida está permitiendo el control de las personas y de las almas de una forma mucho más fácil. Y si bien es cierto que existen razones sociológicas que permiten sostener la justificación del incremento de las medidas de control político, la más que acreditada desviación o ampliación desmesurada del uso de dichas técnicas por los poderes públicos y privados de las grandes compañías está llevando a la humanidad a una verdadera dictadura digital, referida con la más digerible denominación de "capitalismo de vigilancia".

A consecuencia de la revolución informática, reducidas todas las realidades a ceros y unos –el lenguaje digital–, desde el punto de vista político y

social la diferencia entre lo público y lo privado se diluye; la privacidad no es cosa de uno sino del grupo en el que vive y con el que se relaciona; los actos ilegales no son definidos por su estructura sino por su motivación. Frente a esta situación, las barreras entre la defensa nacional, la seguridad nacional y la seguridad ciudadana igualmente se emborronan, y con ellas se pierde el régimen tradicional de garantías que protegían al ciudadano. Hoy día vivimos en una única realidad digital donde todos los elementos, toda la información, todas las conductas, tienen una repercusión en lo pequeño y lo grande. Como diría un buen amigo, lo micro y lo macro –en términos de mundo digital– confluyen al igual que la física newtoniana y la cuántica. Nos falta, al igual que en ese mundo inextricable de la física teórica, una teoría del campo unificado que aúne nuestras facetas pública y privada. Eso nos proporcionaría seguridad jurídica y libertad.

El presente artículo tiene por objeto abordar, desde lo que consideramos los posibles comienzos de toda esta ola de imposición del control político y social, sus orígenes, su evolución, las razones, los mecanismos legales en que ahora se sustenta, su posible justificación y las eventuales consecuencias de su abrazo incondicional.

§2. Unos cuantos acontecimientos históricos

Aunque hablemos de tecnologías que parecen futuristas –falsa apreciación de la realidad actual–, lo cierto es que los fundamentos de las herramientas actuales se hallan en los albores del siglo xx, caminando algunos de ellas de la mano de los propios protagonistas.

2.1 *Los censos de población*

Hermann Hollerich, un ingeniero norteamericano de origen alemán, empleó por primera vez la tecnología de tarjetas perforadas en la elaboración del censo de población de Estados Unidos, reduciendo drásticamente el tiempo necesario –de cinco años a dos– y el coste, una quinta parte del hasta entonces necesitado.

La empresa fundada por Hollerith –la Tabuling Machine Company– se fusionó con otras para fundar en 1911 la Computing Tabuling Recording Company (CTR), que en 1924 cambió su nombre por el de International Business Machine Corporation (IBM).

El empleo de las máquinas de tarjetas perforadas cruzó el Atlántico y llegó a la Alemania de entreguerras. IBM fundó una filial, la Deutsche Hollerith Maschinen GmbH (Dehomag) para el desempeño de su labor empresarial en Europa. Sin embargo, su empleo por los jerarcas nazis se desvió pronto hacia la identificación de los que se consideraban enemigos del Reich por razón de etnia, raza o religión. La misma política se empleó en los territorios ocupados, especialmente en los Países Bajos, lo que dio pie a la localización, detención, deportación y exterminio de las personas de raza judía y gitana.

Qué duda cabe que, si bien su uso no fue tan determinante del resultado de la solución final, como expone Black en su obra *IBM y el Holocausto* (Black, 2001), sí es cierto que puso de relieve –por vez primera– los peligros de la desviación en el uso de datos obtenidos con una originaria finalidad legítima. Por ello, en la mentalidad jurídica europea quedó grabado lo que denominamos *paradigma Auschwitz*: evitar, a cualquier precio, la desviación en las finalidades del uso de los datos personales. Más adelante veremos su vigencia actual.

2.2 *Enigma. Las matemáticas y la guerra*

Alan Turing, uno de los padres de la informática actual, fue reclutado para formar parte de los especialistas de la Escuela Gubernamental de Códigos y Cifras de Bletchley Park. Gran Bretaña sufría el acoso del régimen nazi por mar y aire, que pretendía doblegarla. La armada alemana comunicaba con su Alto Mando, mediante transmisiones cifradas con la máquina Enigma, sofisticado ingenio que permitía un cifrado casi inexpugnable de las comunicaciones. De este modo, se mantuvo un bloqueo naval que dificultaba el apoyo logístico de Estados Unidos a sus aliados europeos.

El descifrado de la máquina Enigma se logró mediante el empleo de uno de los primeros ordenadores mecánicos, la denominada Bomba, que realizaba el

cálculo de tres máquinas Enigma anulando sus efectos criptológicos. El empleo de esta tecnología matemática logró acelerar el final de la guerra al permitir la interceptación de comunicaciones de las "manadas de lobos" –escuadras de submarinos alemanes operando conjuntamente en un sector– con su mando, y así despejó de buques enemigos el Atlántico y permitió la llegada de los suministros bélicos y alimenticios desde Estados Unidos, lo que supuso el vuelco del signo de la contienda. Otro tanto sucedió en el frente del Pacífico, donde la aplicación de esta tecnología para la interceptación de las comunicaciones japonesas, unida al empleo del arma nuclear, aceleraron la rendición del Imperio japonés y con ello el fin de las hostilidades. Por primera vez, las matemáticas, y especialmente los algoritmos, se convertían en un arma de guerra.

2.3 *El tratado UKUSA. La vuelta a la diplomacia secreta*

Tras la colaboración sostenida por Estados Unidos y Gran Bretaña durante la Primera Guerra Mundial y sus fructíferos resultados, Norteamérica propuso en 1940 continuar la colaboración SIGNINT (Signal Intelligence/Inteligencia de señales). La colaboración se intensificó a partir de entonces para acabar con el bloqueo naval del Atlántico, actuando norteamericanos y británicos –a los que se unieron los canadienses en 1943– como una única unidad conjunta. Ese año vio la luz el acuerdo BRUSA-SIGNINT, cuyo propósito era –como describe el informe del Parlamento Europeo sobre el sistema de interceptación ECHELON– "el intercambio de toda información relativa al descubrimiento, identificación e interceptación de señales, así como el desciframiento de los códigos y claves". Tras el fin de la guerra, la iniciativa para el mantenimiento de la alianza partió del Reino Unido, sumando a sus componentes a Australia y Nueva Zelanda. De esta forma, la alianza contaba con base geográfica en todo el globo terrestre para establecer estaciones de escucha e interceptación, intercambiando toda la información obtenida entre sus miembros.

La existencia del acuerdo secreto fue revelada a la opinión pública por el periodista escocés Duncan Campbell en 1981, al publicar por primera vez un artículo donde hacía referencia a la existencia de ECHELON, un programa de interceptación global de comunicaciones, prolongación natural de dicho acuerdo.

El artículo fue censurado y sometido a las leyes de secretos oficiales del Reino Unido, si bien una segunda entrega sí pudo ver la luz en 1988. Lo relevante de la noticia no era simplemente dar a conocer la existencia de una red secreta de interceptación global de comunicaciones, sino el desvío de la información obtenida hacia finalidades de espionaje económico e industrial efectuado por las agencias de inteligencia en favor de sus empresas estratégicas como forma de pago de sus contribuciones tecnológicas a sus Gobiernos nacionales.

La recepción de estas noticias periodísticas por la opinión pública dio lugar a la apertura de una investigación en el panel de asesoramiento científico y técnico del Parlamento Europeo (STOA), en el que se presentó el informe *An Appraisal of Technologies Of Political Control* (1998), elaborado por la Fundación Omega. En dicho informe se hizo referencia a la existencia de redes de interceptación de comunicaciones nacionales e internacionales, especialmente la mencionada ECHELON. El hecho, por entonces motivo de escándalo en la opinión pública, fue digerido tras los acontecimientos del 11S hasta convertirlo en contenido de ocio. Véase el ejemplo de películas norteamericanas, como *Enemigo público* (*Enemy Of The State*), *La noche más oscura* (*Zero Dark Thirty*), o de series como *The Good Wife* (5.ª temporada) (Hancok, 2016).

El 24 de abril de 2001 el Parlamento Europeo consideró acreditada la existencia de dicho tratado secreto, y manifestó su preocupación por el empleo de este tipo de tecnología para el espionaje industrial por las implicaciones que supondrían en la vida de los ciudadanos, e instó a los países miembros del acuerdo a la suscripción de los oportunos convenios internacionales de protección de los derechos civiles.

2.4 *El terrorismo yihadista. Los atentados del 11 de septiembre de 2001 y de 8 de junio de 2005*

Osama bin Laden creó entre agosto de 1988 y finales de 1989 la organización terrorista Al Qaeda, un conjunto de militantes musulmanes de la guerra de Afganistán contra la Unión Soviética. Su oposición a la presencia norteamericana en la península arábiga tras la primera guerra del Golfo le hizo desvincularse de sus lazos norteamericanos para crear una de las primeras

experiencias del *terrorismo de franquicia*. Al Qaeda mantenía la estructura de una red, contando con un núcleo central formado por antiguos combatientes de la guerra afgana, que empleaba las comunicaciones en todos sus formatos para el mantenimiento de los contactos con las células dispersas en todos los países de Occidente. De hecho, Al Qaeda supuso la primera experiencia de terrorismo basado en comunicaciones, donde las redes de información y comunicaciones como internet fueron empleadas como recursos no solo de contacto entre sus miembros y de transmisión de órdenes, sino como herramienta para la obtención de información logística, propaganda y financiación.

El funcionamiento de Al Qaeda se basaba, además, en la construcción de un relato o discurso narrativo que servía de mecanismo de cohesión ideológica y personal entre personas con las mismas creencias religiosas radicales dispersas por todo el mundo, haciéndoles partícipes de una unidad construida a través de la generación de emociones y sentimientos de adhesión (reforzamiento del orgullo musulmán, guerra y odio al enemigo occidental, interpretación radical de un concepto de guerra santa o yihad).

El modelo terrorista fue llevado a un nivel superior por la organización ISIS o Dáesh (Estado islámico de Irak y del Oriente). La perfecta producción de sus vídeos sobre ejecuciones, tanto de civiles como de militares, así como de la destrucción de obras patrimonio de la humanidad –el caso de los Budas de Bamiyan–, son un claro ejemplo de la evolución del concepto de terrorismo de franquicia hacia una *organización basada en el relato*, donde la muerte de personas y el daño a bienes de incalculable valor se convierten en mero instrumento y escenario al servicio de la construcción de la narración que mueve las emociones y los sentimientos de odio, adhesión a la causa y lucha contra el infiel.

El clima de terror ocasionado en Estados Unidos tras el 11 de septiembre dio paso a la declaración de la «Guerra contra el Terror» por la Administración Bush, lo que tuvo importantes repercusiones en el ámbito normativo a nivel mundial. El enfoque adoptado de *paradigma de la prevención* supuso la aprobación de un importante paquete de medidas legislativas que afectaban a numerosos estatutos legales en vigor, de modo que se afrontó el nuevo escenario de guerra asimétrica con medidas de alcance transversal, aplicando tanto acciones militares como civiles (aplicación del derecho penal y procesal).

El modelo normativo fue acompañado de reformas equivalentes en los países de la Unión Europea y de los tradicionales aliados norteamericanos.

El concepto de guerra asimétrica hace referencia a un tipo de conflicto donde no existen frentes de combate y, por ello, no se pueden emplear ni el armamento ni las tácticas de guerra convencionales; afecta a toda la población civil, entre la que se hallan los propios contendientes, y donde tienen un papel relevante tanto el empleo de medios tecnológicos como los aspectos psicológicos de los adversarios, jugándose y manipulándose sus sentimientos y percepciones de la realidad para emplearlos como instrumentos de combate contra sus propios dirigentes (Fojón, 2006).

También tienen su importancia, en nuestra pequeña historia del avance del control político y social, los atentados en el metro londinense de 7 de julio de 2005. En el Consejo Europeo celebrado en Bruselas los días 17 y 18 de junio ya se habló de la necesidad de aprobación de la futura Directiva de retención de datos de las comunicaciones electrónicas, medida muy discutida en el seno de la Unión Europea por sus implicaciones en el derecho a la vida privada de los ciudadanos y su posible colusión con los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE). Los atentados facilitaron la rápida aprobación de la norma, al igual que sucediera en Estados Unidos después del atentado del 11 de septiembre. La Directiva ha sido considerada no conforme con la normativa comunitaria en varias resoluciones del Tribunal de Justicia de la Unión Europea.

§3. Tecnología y sociedad. cambio del equilibrio de poder

3.1 *Cambios tecnológicos*

La situación actual de control político y social no puede entenderse sin una referencia a los cambios operados en la sociedad y en la política gracias a la tecnología. Han sido diversos episodios de evolución los que han dado lugar a un aumento de la capacidad de obrar de los individuos, lo que ha ocasionado, a su vez, un intento de reequilibrio del poder mediante el incremento de las técnicas de control social.

El paso de la informática estática, basada en grandes computadoras ENIAC y UNIVAC I, a la informática doméstica gracias al IBM-PC modelo 5150 de 1981, unido a la aparición en enero de 2007 del primer teléfono móvil *iPhone*, de la marca Apple, ha dado lugar a la modificación de nuestra relación con la informática y el uso de la información.

Liberados de la necesidad de permanecer físicamente en un lugar para hacer uso de los medios informáticos, la informática móvil a que dio lugar la nueva generación de smartphones basados en los sistemas IOS de Apple y Android, de Google, dio pie a otro gran cambio: la Web 2.0, denominación popularizada por Tim O'Reilly en 2004 para referirse a una nueva forma de emplear internet basada en la inteligencia colectiva para generar servicios interactivos, donde la relación entre iguales es preferente y de más fiabilidad que la que se recibe de las organizaciones o instituciones propias de la Web 1.0. Internet pasa de ser vertical a horizontal, propiciada por la conjunción de *software* que permite esta interactividad (las redes sociales) y *hardware* que facilita la movilidad, ubicuidad y permanente conectividad para el tratamiento y generación de la información.

A su vez, la proliferación de dispositivos conectados permanentemente a internet llevó a adoptar un modelo de virtualización de la informática por medio de la denominada *cloud computing*, que permitía convertir los equipos informáticos en máquinas virtuales –equivalentes a programas informáticos– almacenados en servidores siempre disponibles. La información así tratada y los propios medios informáticos empleados para su gestión pasaban a tener una misma.

3.2 *Consecuencias en las capacidades de obrar*

La democratización de los medios informáticos por medio de su producción en masa, y su consiguiente reducción de precio de adquisición, permitió un trasvase de poder desde los Estados y las grandes corporaciones a los individuos, que podían desarrollar nuevas actividades en la sociedad, algunas de trascendencia política.

El individuo ganó capacidad económica al poder monetizar sus creaciones –e incluso su propia vida digital– a través de las redes de intercambio *peer to peer* (P2P). Inicialmente empleadas para el intercambio ilegal de obras audiovisuales, el avance tecnológico generó un verdadero paradigma de las relaciones económicas digitales, en las que los individuos se autoorganizan sin necesidad de intermediarios convencionales. Los individuos pasaron de ser consumidores a convertirse en *prosumidores*, productores de bienes digitales (Aparici, 2018: 72). Manifestaciones de ese nuevo paradigma fueron Blablacar, Airbnb o, de forma más radical, las criptomonedas.

En 2008, tras la crisis financiera mundial ocasionada por la caída de Lehman Brothers, surgió el proyecto, presentado bajo el seudónimo de Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", que –empleando técnicas de redes *peer to peer* con criptografía asimétrica de clave pública– generó un nuevo tipo de activo económico con propósito de convertirse en moneda no fiduciaria. La confianza del sistema estaba basada en un sistema de contabilidad distribuida mediante la tecnología *blockchain*, en virtud de la cual todas las transacciones realizadas son comunicadas a todos los usuarios, que mantienen un libro registro igual, evitando de esta forma las falsificaciones. Aunque con posterioridad surgieron otros proyectos de monedas, *bitcoin* sigue siendo la más conocida y extendida, funcionando como un activo financiero más que como una moneda no fiduciaria, empleado para realizar transacciones con cierto nivel de anonimato y con finalidad generalmente especulativa. Estas características han hecho de las criptomonedas un instrumento muy útil para el blanqueo de capitales procedentes de actividades ilícitas, de lo que ha surgido un propósito de regulación por parte de los países.

Pero los ciudadanos también alcanzaron una capacidad política antes desconocida. Actuando de forma concertada mediante el empleo cada vez mayor de las redes sociales, los individuos ganaron poder político mediante el ciberactivismo, a su vez desplegado en diversos niveles –desde la coordinación para campañas cívicas hasta el ciberhacktivismo de Anonymous–, y el proceso culminó con la denominada Primavera Árabe, que tuvo lugar entre los años 2010 y 2012 en los países africanos y de Oriente Medio del arco Mediterráneo, donde se sucedieron movimientos espontáneos de rebeldía frente a los Gobiernos autoritarios por los ciudadanos coordinados entre sí por

comunicaciones electrónicas. En el caso de la Primavera Árabe o "revolución de las redes sociales", estas pasaron de ser herramientas de entretenimiento a instrumentos de información (Carlini, 2018). Estamos, por tanto, ante un nuevo salto cualitativo en el uso de los instrumentos informáticos e informacionales que pone de relieve la pérdida del monopolio del poder por parte de los Gobiernos tradicionales en favor de los ciudadanos organizados por medios electrónicos, que de esta forma son capaces de convertirse en actores en el panorama nacional e internacional, algo hasta entonces reservado a las estructuras estatales y supranacionales.

3.3 *El lado oscuro del empoderamiento digital*

Ciertamente, todas las actividades descritas ponen de relieve el incremento de la capacidad de obrar que hemos obtenido gracias a la digitalización de nuestra sociedad. Sin embargo, esta mayor capacidad de obrar y algunas de sus características asociadas, como la capacidad de actuar anónimamente, ocultando el origen de nuestra conexión mediante el empleo de redes privadas virtuales (VPN) o *proxies* anonimizadores, o el empleo de criptografía para ocultar el contenido de nuestras comunicaciones, permiten a algunos usuarios la realización de comportamientos delictivos que antes era imposible imaginar. La capacidad de obrar digitalmente, unida a la sensación de impunidad por el empleo de medios tecnológicos de los que se cree en su capacidad para hacernos completamente anónimos, y la errónea consideración de legítimos de todos los instrumentos, programas e información que podemos encontrar en la red, hacen que muchas personas completamente insertadas en la sociedad lleven a cabo comportamientos ilícitos que –de tratarse de actividades materiales– nunca llevarían a cabo.

Dado que la velocidad de comisión de los delitos y estas características dificultan su perseguibilidad, los Estados se han dotado de mecanismos de inteligencia criminal que les permitan la localización e identificación de los autores de los hechos mediante la consulta de los metadatos de sus comunicaciones. Ello comporta la adopción de una política de retención de datos de tráfico relativos a comunicaciones electrónicas, un instrumento necesario

para la lucha contra la criminalidad informática y otras formas graves de delincuencia. Actualmente, la tensión existente en el plano legal radica –precisamente– en la legitimidad del establecimiento de estas grandes bases de datos indiscriminadas de metadatos de cualquier usuario de la red simplemente por haber realizado una comunicación electrónica, y el posible desvío en su uso para otras finalidades por parte de las autoridades gubernamentales. Nuevamente, se pretende evitar la aparición del *paradigma Auschwitz*.

La máxima manifestación de actuación criminal que es posible para el usuario normal de internet lo constituyen los actos de ciberguerra. En realidad, un delito informático común, un delito informático terrorista o un ataque a la seguridad nacional de otro Estado únicamente se diferencian en la motivación del autor, dado que su ejecución se lleva a cabo con las mismas herramientas informáticas. Incluso es posible la recuperación de vigencia de las antiguas actividades corsarias, por la que algunos Estados se valen de organizaciones criminales residentes en su territorio para la comisión de ataques contra la ciberseguridad de otras naciones, haciéndolos pasar por delitos informáticos comunes. Los Estados pueden así valerse de profesionales del crimen, altamente cualificados tecnológicamente, para la realización de *ataques de falsa bandera*, teniendo únicamente que protegerlos frente a intentos de reclamación policial o judicial internacional (Luna, 2012). Son las nuevas patentes de corso digitales.

§4. Inteligencia de comunicaciones

4.1 *Los sistemas de vigilancia global en las sociedades democráticas*

El panorama actual de conflictos asimétricos y amenazas híbridas, en donde lo civil y lo militar se entremezclan hasta confundirse, tiene –a nuestro juicio– dos causas de base. De una parte, el recurso al arma nuclear durante la Segunda Guerra Mundial convirtió en inoperante e inaplicable la doctrina del conflicto bélico tradicional –la doctrina de la Guerra Total, en palabras de Claustzwitch– desarrollado únicamente con armamento convencional. De otra, la extensión y la difusión de los medios informáticos entre todos los

individuos han roto el equilibrio de poder existente entre Estado y ciudadanos surgido tras la Revolución francesa, por el que se le otorgaba al primero el monopolio del ejercicio de la fuerza en beneficio del segundo, titular de la soberanía nacional, limitándose su uso por medio de la ley, expresión de la voluntad popular. En el panorama actual, esa fuerza también se manifiesta mediante la capacidad de procesamiento de información, que ya no está en manos exclusivas del poder público.

Sin embargo, en una situación así, de "frente de batalla" interior o civil y de oponentes confundidos entre la población no militar, empleando herramientas informáticas de propósito común pero usadas con fines de atentar contra la seguridad nacional, se hace sumamente difícil la localización de las amenazas y de sus autores. La única forma de localización de los atacantes es proveerse de un sistema global de interceptación de comunicaciones que capte toda señal electrónica de comunicaciones para proceder, posteriormente, a su filtrado por medio de términos clave.

Las medidas de esta naturaleza no son contrarias *per se* al régimen legal de los sistemas democráticos. Las medidas de inteligencia, en cuanto necesarias para la protección de la seguridad y defensa nacional, son compatibles con el derecho al respeto a la vida privada y familiar, tal y como lo contempla el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales (CEDH), suscrito en Roma el 4 de noviembre de 1950.

Sin embargo, como puso de relieve el Informe Final del Parlamento Europeo sobre el Sistema ECHELON y las redes globales de vigilancia (2001), además de la necesidad de estar prevista en una ley accesible (publicada), la medida ha de ser proporcional al riesgo que pretende afrontar, y el sistema debe contar con los oportunos mecanismos de control y supervisión de las posibles reclamaciones de los afectados. Por estos motivos consideró la Comisión que un sistema indiscriminado de escuchas como ECHELON no era compatible con el estándar de protección del Convenio Europeo, en la medida en que no se amparaba en una disposición normativa publicada y al alcance general, ni tenía previstos medios de control (Schmid, 2001).

Pero los acontecimientos derivados de los atentados de Al Qaeda y Dáesh modificaron la percepción de la amenaza, y con ello de los medios necesarios para prevenirla. El paradigma de prevención se ha ido imponiendo poco a poco,

permitiéndose a los Gobiernos nacionales el empleo de medios extraordinarios en materia de vigilancia de las comunicaciones electrónicas. Así, y sin oponerse a las conclusiones de la Comisión ECHELON, la vía empleada desde entonces ha sido la de optar por la retención masiva de los datos de tráfico de las comunicaciones electrónicas. Como se expuso anteriormente, los atentados en el metro londinense en 2005 aceleraron la puesta en vigor de la imposición a las operadoras de comunicaciones de diversas medidas de facilitación de las labores de las Fuerzas y Cuerpos de Seguridad, que analizaremos a continuación.

4.2 *Los sistemas de vigilancia electrónica de las comunicaciones con propósito de investigación criminal*

4.2.1 Requerimientos técnicos para la interceptación legal de las comunicaciones

La prohibición de uso de sistemas de vigilancia electrónica global llevó a la Unión Europea a formular su lucha contra el crimen desde otras perspectivas.

Tras la apertura de internet al público en abril de 1993, los Gobiernos fueron conscientes de la necesidad de controlar el tráfico de comunicaciones. Por ello, en noviembre de ese año se celebró un Seminario ILET (*International Law Enforcement Telecommunications*) en Quantico (Virginia-EE. UU.), sede del FBI, en el que participaron unidades policiales y servicios de inteligencia del Consejo de Europa y de la Commonwealth, estableciendo una serie de requisitos técnicos que reclamar a las operadoras de telecomunicaciones para hacer posibles las intervenciones legales de comunicaciones. A partir de esa fecha fueron modificándose las legislaciones procesales de intervención de comunicaciones.

En el seno de la Unión Europea, los requerimientos fueron recogidos en la Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones. A nivel nacional, los requerimientos técnicos fueron adoptados en la Ley General de Telecomunicaciones de 2003, particularmente en su desarrollo reglamentario plasmado en el Real Decreto 425/2005, de abril, que contenía una pormenorizada regulación del sistema

SITEL, plataforma de intervención de comunicaciones y acceso a datos de tráfico por las Fuerzas y Cuerpos de Seguridad del Estado.

4.2.2 La conservación de datos de tráfico de las comunicaciones electrónicas

La segunda vía desarrollada por los integrantes de la Unión Europea para dotarse de un sistema de vigilancia electrónica fue la de regular, como nueva obligación de los operadores, la conservación de los datos de tráfico asociados a las comunicaciones electrónicas.

La digitalización de las comunicaciones ha permitido asociarles etiquetas de datos –metadatos– que proporcionan información relevante tanto para la realización de los procesos de conexión a las redes de comunicación y de comunicación en sí, como de facturación y otros usos comerciales posteriores. Estos datos de tráfico pueden proporcionar una información muy precisa sobre la vida privada de los usuarios de las comunicaciones a las que se refieren, como puso de relieve el Tribunal de Justicia de la Unión Europea en su Sentencia de 8 de abril de 2014 (*Digital Rights Ireland*; asuntos C-293/12 y C-593/12).

La norma europea que dio fundamento a esta obligación de conservación fue la Directiva 2006/24/CE, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Su contenido tenía soporte en el art. 15.1 de la Directiva 2002/58/CE, que prevé la restricción de los derechos allí recogidos en términos parecidos al del artículo 8 CEDH.

Los atentados de Londres de 2005 aceleraron el proceso de adopción de la normativa; pero, además, introdujeron un cambio en el ámbito de aplicación (la lucha contra los delitos graves, además de contra amenazas a la seguridad nacional), siendo a la postre fundamental para el cuestionamiento de la validez de la disposición.

El Tribunal de Justicia de la Unión Europea (TJUE) se ha pronunciado en diversas ocasiones en sentido negativo sobre la validez y compatibilidad de la normativa de conservación y retención de datos europea con los derechos

fundamentales reconocidos en la Unión. Su doctrina se puede sintetizar en los siguientes puntos:

- Los sistemas de almacenamiento de datos relativos a las comunicaciones electrónicas suponen una injerencia al derecho a la vida privada, al generar en el ciudadano un sentimiento de vigilancia constante.
- No obstante, se considera una medida razonable y proporcionada la adopción de una medida de tal alcance para fines de lucha contra las amenazas a la seguridad nacional, para lo que requiere una precisión normativa de las condiciones de conservación y acceso a los datos conservados, particularmente cuando se trataba de perseguir o enjuiciar delitos; y contar con los suficientes mecanismos de control, de modo que no puede concluirse si la medida es o no necesaria en el seno de una sociedad democrática.
- La determinación de las obligaciones de conservación y acceso por motivos de seguridad nacional o seguridad pública constituye una materia comunitaria, por más que la Unión Europea careciera de competencias para regular asuntos relacionados con Justicia y Asuntos de Interior. La Directiva, al determinar por esta vía el alcance de la garantía de la confidencialidad de los datos, incide en el régimen de protección diseñado para los operadores de telecomunicaciones a los que se le impone esta obligación adicional de orden público.
- Se acepta la existencia de sistemas de conservación y retención de datos, si las normas -comunitarias o nacionales- establecen las garantías adecuadas, asumiendo la posibilidad de existencia de algunos regímenes especiales siempre que obedecieran a algunos de los fines previstos en el art. 15.1 de la Directiva 2002/58/CE; que los datos fueran objeto de acotación en función de criterios espaciales, temporales o personales; y que los sistemas legales diseñados contuvieran normas de procedimiento que garantizaran el control judicial o administrativo independiente, así como la correcta conservación para garantizar el derecho a la confidencialidad de los datos manejados, referido en el art. 5.1. de la Directiva. No obstante, los regímenes de conservación de datos que podrían admitirse tendrían siempre un carácter selectivo, debiendo ser acotados –en el caso de ser preservados con la finalidad de lucha contra

la delincuencia grave– con arreglo a criterios objetivos que acrediten la relación entre los datos y el objetivo de la investigación.

- No todas las medidas de investigación tienen la misma naturaleza de injerencia grave en la vida privada. La medida de investigación no se considerará grave, si únicamente se accede a los datos de abonado o titularidad de las tarjetas SIM, dado que no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se vean afectados.

4.3 *Conclusiones*

Como puede observarse, el recurso a los datos de tráfico y de localización de terminales de comunicaciones electrónicas es un tema aún candente en el panorama europeo. La fuerza de los hechos lleva a los tribunales a la matización de sus pronunciamientos anteriores en orden a admitir –aunque con serias limitaciones– distintas soluciones que permiten el equilibrio entre la disponibilidad de medidas eficaces de investigación criminal y la necesaria preservación del derecho a la vida privada y a la protección de datos en toda sociedad democrática.

Este debate está llevando a la necesaria distinción entre datos de abonado, datos de conexión y datos de tráfico, para entender que solo estos últimos –relacionados con una comunicación concreta– deben ser objeto de especial protección por su carga de contenido informacional de carácter personal, pues una extralimitación en su uso originario mediante la elaboración de perfiles personales puede suponer una violación del derecho a la vida privada.

Con todo, el panorama de decisiones judiciales no tiene en consideración el estado actual de la tecnología y de las amenazas híbridas, donde la identificación a priori de una persona implicada en un ataque a la seguridad nacional o a la seguridad pública no aparece claramente deslindada, y es precisamente el recurso a las bases de datos de tráfico de las conexiones empleadas –junto a otros datos de inteligencia– lo que permite su identificación y la concreción de su verdadero designio criminal. El sistema diseñado por la jurisprudencia europea es, ciertamente, necesario para evitar el abuso desde los poderes públicos. Y, con independencia de su efectividad, parece un buen punto de partida para que –en

sucesivos pronunciamientos judiciales– se permita su ampliación en función de las necesidades de las sociedades a las que han de servir como garantía.

§5. Inteligencia criminal y vigilancia policial

5.1 *Inteligencia criminal*

En los tiempos en que no se contaba con medios tecnológicos la comisión de un delito requería, en muchas ocasiones, un contacto o proximidad física entre agresor y víctima. Esa circunstancia espacial ha desaparecido –salvo en los delitos contra las personas– en nuestra sociedad actual, permitiendo que agresor y víctima estén ubicados en localizaciones distintas, incluso en países distintos. Además, la disponibilidad de recursos informáticos a través de la red ha dado lugar a una especie de legitimación de hecho a todo aquello que puede ser realizado mediante herramientas informáticas o información hallada en la red.

La ampliación del número de autores de hechos delictivos, la desubicación con relación al hecho y a la víctima, el incremento en la movilidad geográfica por el fenómeno de la globalización, así como la complejidad de los instrumentos tecnológicos empleados en algunas ocasiones, han hecho necesaria la utilización cada vez más intensa de recursos de inteligencia criminal por parte de las fuerzas y cuerpos de seguridad (OSCE, 2017).

La inteligencia criminal puede ser definida como "cualquier tipo de información con valor adicional que puede ser utilizado por los agentes del orden para combatir la delincuencia" (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2010). Gracias a ella, tanto de tipo operacional –destinada a las investigaciones particulares– como estratégica –definición de objetivos o líneas de actuación en política criminal– las decisiones policiales se hacen más eficaces y exactas.

Si antes la base de la inteligencia criminal se asentaba en los datos e información recopiladas por la policía de seguridad ciudadana, en la actualidad son las bases de datos y ficheros policiales, asociados a programas informáticos de *data mining,* los que aportan los *inputs* para la toma de decisiones. Para ello se precisa una ingente cantidad de información proveniente tanto de la propia organización

policial como de otros organismos públicos o privados. Además, el incremento de la gravedad de los ataques a la seguridad ciudadana –en muchas ocasiones, de naturaleza híbrida, sin definir su propósito final– lleva a la necesidad de actuar con carácter cada vez más predictivo del peligro que evitar, dado que el resultado lesivo puede ser de incalculable gravedad. La actividad desplegada en control de fronteras, ciberpatrullas, crimen organizado y formas graves de delincuencia se basa, en gran parte, en la denominada *Policía Predictiva* (Kostopoulos, 2019), la puesta en práctica del escenario ideado por Phillip K. Dick en *The Minority Report* (1956), después convertido en una inquietante película distópica (Spielberg, 2002), donde la Policía puede anticiparse a la comisión de graves crímenes en tiempo real por lectura remota del pensamiento del criminal.

Sin embargo, esta actividad predictiva supone un serio peligro para los ciudadanos. La búsqueda de patrones de comportamiento basados en hechos anteriores, muchas veces inconexos entre sí, genera una apariencia de presunción de culpabilidad en todos los individuos, que pueden verse sometidos a una decisión algorítmica difícilmente controlable y cuestionable, pero que limita decididamente su capacidad de actuación. Para ello, deben verse sometidos a una continua recopilación de datos de su vida privada, cedidos o comunicados con finalidades distintas a las de seguridad ciudadana. Si bien dichas medidas pueden estar amparadas en la ley, el conjunto de obligaciones y escrutinios a que nos vemos sometidos sí genera una sensación de vivir en una sociedad vigilada. Y el peligro de desviación de su uso está siempre presente, como la Historia y los acontecimientos diarios nos van demostrando.

5.2 *Bases de datos policiales*

Los pilares de la Policía Predictiva son, como hemos anticipado, las bases de datos policiales y los algoritmos que permiten la *Machine Intelligence*, la inteligencia de las máquinas que –al fin y a la postre– toman las decisiones en materia de seguridad pública actualmente, quiérase o no.

Los sistemas de información policial han evolucionado desde los archivos en fichas y papel hasta los actuales bancos de datos que hoy conocemos. Y especial relevancia tiene en esa evolución el modelo europeo.

La constitución de un espacio único europeo para la libre circulación de personas y mercancías comportó la necesidad de sustituir los controles fronterizos por un sofisticado sistema de vigilancia electrónica. Había nacido el *Territorio Schengen*.

En virtud del Convenio de Aplicación del Acuerdo de Schengen de 14 de junio de 1985, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, se estableció un sistema de información común a todos los países firmantes en estructura de estrella, con una unidad central (C-SIS) a la que se hallaban conectados los sistemas nacionales (N-SIS), a cargo de una oficina de enlace (SIRENE). La información o *descripciones Schengen* que se introducían en el sistema eran compartidas por todos los miembros, basándose en el nuevo principio de disponibilidad de la información policial. Dichas descripciones estaban perfectamente definidas en el Convenio, así como las garantías y plazos para su cancelación. El sistema Schengen se acomodaba, en materia de protección de datos, a la normativa del Consejo de Europa, si bien contenía importantes previsiones en materia de protección de datos personales y garantías institucionales. Pero establecía métodos de vigilancia electrónica novedosos, como la *vigilancia discreta*, por la que podía introducirse una descripción del conductor, vehículo y ocupantes, trayecto, destino, equipaje y circunstancias de sospecha, basado en un perfil de peligrosidad sobre los afectados, quienes no tendrían conocimiento de estar siendo sometidos a control policial durante el trayecto.

Schengen supuso un avance sobre los sistemas policiales anteriores, cuya información pertenecía a cada país y únicamente podía ser transmitido por los canales de cooperación policial –la Oficina Interpol–. El nuevo principio de disponibilidad permitía el acceso a información de dichos ficheros nacionales, que eran puestos en común en la unidad central C-SIS.

Un avance polémico en esta línea de interconexión de bases de datos policiales lo constituyó el denominado Tratado de Prüm. Negociado casi en secreto, sin supervisión parlamentaria nacional ni europea, Alemania, España, Francia, Bélgica, Austria, Luxemburgo y Países Bajos, decidieron reforzar y ampliar el Sistema Schengen en dos sentidos: de una parte, ampliando el tipo de descripciones o información que compartir, pues abarcaba perfiles de ADN, matrículas de vehículos y embarcaciones, huellas dactilares y armas; de otra, estableciendo

un sistema de registros indexados que aceleraba las búsquedas y permitía la recepción automatizada de la información. El sistema suponía, por ello, una posibilidad de recepción directa de la información de los propios sistemas policiales nacionales, sin sistemas intermediarios distintos de los registros índices.

Una limitación fundamental al régimen de tratamiento de datos policiales lo constituye el carácter necesario de la información almacenada; en particular, su dimensión temporal.

Los datos policiales únicamente pueden mantenerse el tiempo imprescindible para permitir el cumplimiento de su finalidad. Un mantenimiento más allá del precisado supone una injerencia en la vida privada de las personas afectadas no permitida por la legislación de protección de datos. Por ello, la revisión de dichas decisiones de mantenimiento, al modo del sistema Schengen, son absolutamente precisas para mantener el equilibrio entre intereses públicos y limitaciones a las libertades fundamentales justificadas por ello. Eso fue lo resuelto por el Tribunal Europeo de Derechos Humanos en *Marper vs. UK*, donde el Tribunal Europeo dictaminó la existencia de vulneración al derecho a la vida privada por haberse mantenido las reseñas dactiloscópicas de los demandantes –absueltos en sus respectivos procesos penales– más allá del tiempo necesario para la tramitación de las actuaciones. Este fallo es de especial trascendencia para la futura (o ya presente) situación de juicios algorítmicos, donde las decisiones judiciales podrán ser asistidas por sistemas de inteligencia artificial.

5.3 *Las nuevas tecnologías de vigilancia electrónica. Especial mención de la videovigilancia*

5.3.1 La eficacia irrenunciable de la videovigilancia

Nos vigilan. Constantemente caminamos por calles y plazas en las que nos percatamos de la existencia de cámaras – instaladas de forma consciente con ese propósito– que continuamente nos siguen. Quizá las más peligrosas sean aquellas cuya instalación no permite ser vistas puesto que no anuncian la existencia de una limitación a nuestros derechos en dicha zona. Pero el

objetivo fundamental de las videocámaras es disuadirnos de actuar ante la amenaza de estar siendo vigilados.

Qué duda cabe de que la videovigilancia es un instrumento muy útil –casi irrenunciable– para el mantenimiento de la seguridad ciudadana. Pero llenar nuestras vías públicas de ojos orwellianos conectados a un *Big Brother* policial restringe de forma considerable, intolerable, nuestro nivel de libertad. La persona no se comporta igual sabiendo que está siendo observada. No solo es nuestra vida privada la que resulta afectada; es nuestra propia libertad la que resulta limitada por mor de la seguridad ciudadana.

La Fundación Omega puso de relieve –en su informe sobre las tecnologías de control político para el Panel STOA del Parlamento Europeo– su posible papel como instrumento sustitutivo de otras técnicas o armas de control de multitudes, especialmente si eran apoyadas por algoritmos de reconocimiento facial. Sin embargo, llegaba a la conclusión negativa sobre su extensión, ya que no impedía la actuación de los radicales en la calle y, más preocupantemente, generaba por contra una red de supervisión en masa que podía ser usada para diferentes propósitos de los originalmente previstos (Omega Research Foundation, 2000).

Si las conclusiones eran estas a mitad de 2000, en 2020, con una tecnología de reconocimiento facial apoyado en inteligencia artificial como soporte de un tratamiento masivo de datos, la realidad ha superado con creces las expectativas. En 2007, un reportero de la BBC, John Sudwoth, realizó la experiencia en la ciudad china de Guiyang, de comprobar en cuánto tiempo sería localizado por el sistema de videovigilancia instalado por las autoridades chinas (BBC News / Mundo, 2017). Fueron siete minutos los que tardaron los dispositivos de vigilancia electrónica en dar con el periodista británico. El sistema de videovigilancia chino se basa en una instalación de 200 millones de cámaras por todo el país, conectadas a bases de datos policiales y administrativas, y apoyadas por un sistema de reconocimiento facial e inteligencia artificial. Como reflejaba la noticia, el sistema no solo pretende evitar el delito sino también predecirlo (Mendiola, 2017). Ciertamente, es el modelo más eficaz de seguridad ciudadana existente en el mundo; pero a costa de carecer de protección de la privacidad. Sin duda, George Orwell no imaginó un desarrollo tan eficaz de su crítica al sistema comunista que se ha convertido en el paradigma de las distopías tecnológicas actuales.

5.3.2 Garantías frente a la videovigilancia

Conscientes de la efectividad en la persecución del delito, e incluso en su prevención, pero también de los riesgos que comportaba su generalización, en el ordenamiento jurídico español se adoptó en 1997 la normativa actual reguladora de la videovigilancia con fines de seguridad pública. La norma tuvo su origen en la necesidad de lucha contra el fenómeno de la *kale borroka* en Euskadi, ante los dubitativos pronunciamientos judiciales que generaba la aportación de imágenes de las videocámaras por las fuerzas y cuerpos de seguridad para identificar a los responsables de los actos de disturbios públicos. El cuadro normativo se completa con la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras; así como de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Dado que una videocámara es, desde el punto de vista de protección de datos, un sensor que capta imágenes y sonidos, su empleo desde el momento de la captación hasta otros tratamientos posteriores (almacenamiento, cesión, bloqueo…) queda sometido igualmente a la normativa de protección de datos.

La labor de los tribunales también ha sido muy relevante para la configuración del contenido y límites al uso de la videovigilancia en nuestra sociedad. A este respecto deben reseñarse tres aspectos delimitados por la jurisprudencia:

- El reconocimiento de la existencia de espacios en la vía pública donde se desarrolla la intimidad personal. Es el supuesto, por ejemplo, de los aseos públicos, donde se ha diferenciado entre las zonas comunes y las cabinas individuales. La jurisprudencia penal ha tenido en cuenta esta diferencia para excluir como pruebas, por vulneración de derechos fundamentales, las imágenes captadas en dichas zonas sin autorización judicial.
- En cuanto a los métodos de captación, el empleo de cámaras ocultas –especialmente por medios de comunicación– ha sido igualmente objeto de diversos pronunciamientos en sede constitucional y civil. Aunque en estos casos el conflicto se plantea entre los derechos a la intimidad personal y la libertad de expresión, dado que es un método comúnmente empleado por los medios de comunicación en la realización de reportajes televisivos, los fallos son relevantes por cuanto que excluyen la

posibilidad de empleo de cámaras ocultas por la vinculación y efecto de la grabación en la libertad personal y dignidad del sujeto grabado, dado que este no se comportaría con igual naturalidad en caso de conocer que está siendo grabado. Sin embargo, en el último pronunciamiento del Tribunal Constitucional sobre la materia, y con base en la jurisprudencia del TEDH, ha matizado su doctrina para aceptar este método de investigación periodística siempre que se aprecie la necesidad del empleo de este por razón de las circunstancias de obtención de la noticia, su relevancia pública y su veracidad.

- Por último –y lo más relevante, si cabe– hemos de referirnos al planteamiento judicial sobre las nuevas tecnologías de vigilancia.

En la STS (2) 329/2016, de 20 de abril, la Sala Penal del Tribunal Supremo restringió su doctrina sobre la legalidad del empleo de dispositivos de observación y grabación de imágenes y sonidos por las Fuerzas y Cuerpos de Seguridad. En un caso de tráfico de drogas en el que los implicados realizaban sus operaciones en un piso ubicado en la décima planta de un edificio –con las ventanas abiertas– que estaba siendo sometido a observación visual por la Policía Judicial mediante el empleo de prismáticos de amplia potencia, el Tribunal revisa y adapta su anterior doctrina a la nueva situación tecnológica, manifestando una clara vocación de delimitación de los nuevos criterios frente a los nuevos peligros. De esta forma, considera que, frente a lo que denomina *injerencias virtuales en el domicilio* la tutela de este otorgada por el art. 18.2 de la Constitución Española "protege, tanto frente la irrupción inconsentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artilugio técnico de grabación o aproximación de las imágenes". Lo relevante no es si el sujeto ha establecido medios de protección adicional a su domicilio, sino si se emplean instrumentos técnicos que ponen al observante en posición de ventaja respecto del observado. La Sala está pensando en los nuevos métodos de invasión del domicilio, mucho más eficientes, insidiosos e indetectables, como es el caso de los drones –que especialmente menciona–, y traza una línea clara de protección de los ámbitos físicos de libertad del ciudadano: si es necesario hacer uso de un medio tecnológico que dota de una

capacidad de percepción no natural al ser humano, de modo que no es posible prever la invasión y –en consecuencia– evitarla, se estará produciendo una injerencia no consentida en la intimidad del sujeto.

La sentencia ahora comentada permite abordar la evolución que pueden sufrir las técnicas de videovigilancia en poco tiempo.

En 1987 la ciencia-ficción anticipaba, una vez más, nuestro futuro distópico. En un panorama social donde la seguridad pública se hallaba contratada con empresas privadas, la robótica y la videovigilancia se hacían presentes como técnicas de lucha contra la delincuencia. El personaje principal de la mítica película de Paul Verhoeven, Robocop, primer cíborg conocido en la historia del cine, nos traía consigo el empleo de gafas o visores que permitían la identificación de los delincuentes y el contraste de la imagen con las bases de datos policiales. Hoy día, 30 años después, en la estación de ferrocarril de Zhenzhou (China) los agentes policiales usan gafas de identificación visual tipo *Google Glasses* para realizar las mismas identificaciones (Rodríguez, 2019).

Este tipo de tecnología de investigación no podría estar amparada en la ley en España. La Ley de Videovigilancia somete al requisito del empleo de las videocámaras móviles –este sería el caso– a la captación conjunta de imagen y sonido; pero además es preciso que exista un peligro concreto que justifique su uso y que se dicte una decisión de autorización por el máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad, que será revisada por una comisión de garantías en el plazo máximo de 72 horas posteriores a la toma de las imágenes.

5.4 *Un paso adelante: inteligencia artificial y seguridad pública*

El 11S lo cambió todo.

Hasta entonces, la sociedad occidental tenía puestas sus miras en el progreso económico y el Estado del bienestar, apoyado por una política internacional que había dado lugar a la neutralización del peligro de guerra nuclear con la caída del Muro de Berlín y la práctica anulación de la Unión Soviética como amenaza mundial.

Sin embargo, el mayor atentado terrorista de la Historia, convenientemente diseñado por sus autores para alcanzar el máximo impacto mediático, unido a varios atentados más en 2004 y 2005, trastocaron la sensación de seguridad en el panorama mundial. La prevención era ahora el paradigma básico de actuación pública, y a ella iban dirigidas todas las políticas en materia de seguridad pública. Estados Unidos, el mayor afectado por este conflicto asimétrico, exportó a todo el mundo una nueva economía del control social –la que ahora conocemos como *capitalismo de vigilancia* (Zuboff, 2020: a)–.

El riesgo sufrió una transformación en su concepto. A partir de entonces, proviene de enfermedades o epidemias a gran escala, del crimen organizado y las mafias, de la corrupción o del terrorismo (Faraldo y Brandariz, 2004). Y para hacer frente a estas nuevas amenazas generadas por enemigos a los que les falta la *seguridad cognitiva*, cuya identidad se desconoce por habitar en la sociedad a la que atacan, surgió la doctrina del *Derecho Penal de Enemigos* (Jakobs y Cancio, 2003). Bajo este nuevo prisma, quienes actúan en contra del Estado no tienen por qué disfrutar de los derechos que el Estado concede a sus ciudadanos, puesto que se enfrenta a aquel.

El paradigma de la prevención ha llevado a la maximización de los intentos por predecir –más incluso que prevenir– los delitos. La imagen de las Torres Gemelas cayendo en llamas evoca el miedo al daño irreparable que cualquier atentado puede generar y que la respuesta penal no evita. Esto justifica los intentos desde entonces de incrementar la vigilancia electrónica y la búsqueda de patrones de conducta que permitan la identificación de los terroristas o grandes delincuentes. Deseamos Precrimen.

El nuevo frente de batalla entre el poder público y los ciudadanos lo constituyen las decisiones automatizadas, las decisiones adoptadas por máquinas dotadas de inteligencia artificial, apoyándose en los datos obtenidos por los sensores instalados en el mundo exterior (videocámaras, señales de geolocalización, drones…) y en las bases de datos propias o privadas mantenidas con propósito de seguridad pública (metadatos de comunicaciones electrónicas). La elaboración de los perfiles de criminalidad, obtenidos por estos mecanismos, gozan psicológicamente de mayor fundamento ante el ciudadano que las propias conclusiones de los investigadores humanos. Sin embargo, las decisiones algorítmicas comportan muchos riesgos para el ciudadano de a pie.

Es de cita obligada al hablar de decisiones algorítmicas y justicia penal la sentencia del caso Loomis vs. Wisconsin (*State of Wisconsin vs. Eric L. Loomis. 2015AP157-CR*, 2016). En este fallo, el tribunal aceptó la validez del uso de sistemas asistidos a la toma de decisiones por los tribunales de justicia, si bien proscribió que los algoritmos en los que se fundaban fueran desconocidos a la opinión pública, dado que no podría conocerse la mecánica y fundamentos de la decisión, vulnerándose el derecho proceso debido, que incluye el derecho a la motivación de las sentencias.

El sistema de decisiones asistidas por inteligencia artificial se basa en dos elementos no suficientemente controlados.

De una parte, el algoritmo o conjunto de instrucciones dadas a la máquina para realizar una tarea, en este caso la evaluación de la peligrosidad criminal de un sujeto. Estos algoritmos son frecuentemente opacos al constituir secretos empresariales protegidos por la ley. Eso ha llevado a más de un autor a considerar que los algoritmos empleados en sectores de alta intensidad o peligrosidad por la Administración (como es el caso de Justicia o de Sanidad) no pueden ser del tipo *blackbox*, es decir, carentes de cualquier sistema de auditoría y trazabilidad interna del proceso decisorio, debiendo pasar un proceso de autorización previa como el de los medicamentos (Fernández, 2017).

De otra, es muy importante en materia de seguridad pública la base o bases de datos empleadas para la obtención de la decisión automatizada. En efecto, tratándose de decisiones de valoración de la peligrosidad criminal del sujeto, los datos base de la decisión automatizada deberían cumplir el principio de calidad reclamado por el artículo 4.1.d) de La Directiva (UE) 2016/680, que exige que sean exactos y debidamente actualizados.

Unos algoritmos cuyos códigos fuente no son conocidos, y por tanto no pueden ser evaluados desde punto de vista de la ética y el marco jurídico aplicable, unido a unas bases de datos de suministro de su materia prima que cuentan con una información que no cumple los principios de calidad exigidos por la legislación de protección de datos, pueden dar lugar a una decisión basada en un sesgo de discriminación.

Por todo esto, quizá fuera conveniente establecer normas específicas para el diseño y uso de algoritmos en sectores estratégicos del Estado, como es el

caso de la Administración de Justicia, basados en los protocolos de código abierto, de forma que todos pudieran conocer y auditar el conjunto de reglas y lógica subyacente al sistema de toma de decisiones –o de asistencia a la toma de decisiones– en el ámbito judicial, al modo en que lo ha realizado Francia, estableciendo una obligación de empleo de algoritmos abiertos en la Administración Pública.

§6. Aplicando el control político y social

6.1 *Verdad y posverdad. Los nuevos mecanismos de control político y social*

Todo cuanto llevamos expuesto sirve para comprobar cómo, con un marco regulatorio adecuado, la existencia de mecanismos de control político y social por medio de técnicas invasivas de la intimidad y la privacidad puede justificarse en un Estado de Derecho siempre que nos enfrentemos a un riesgo real y concreto a su propia existencia o integridad.

Ahora bien, también hemos comprobado cómo el acaecimiento de episodios disruptores –los atentados del 11S– han producido cambios radicales en nuestra forma de estar en la sociedad. El 11S supuso la modificación del relato social sustentado por el poder desde la caída del Muro de Berlín en 1989. Del *paradigma Austchwitz* de proscripción de cualquier exceso en el uso de información por el poder público, hemos pasado al *paradigma de la prevención total*, por el que se prefiere la seguridad a la libertad si el resultado es una mayor seguridad física.

Gómez de Ágreda (2019) remite a la obra de Orwell, *1984*, para encontrar precedentes de la labor política de control del relato, donde un Ministerio de la Verdad cambiaba constantemente el contenido de la hemeroteca para que el presente –así justificado y legitimado por la Historia modificada– conformara el futuro. La verdad es construible, es el producto de un acuerdo que cuente con mayoría suficiente; algo que puede realizarse al haberse introducido, desde la filosofía del s. xx, el factor de la subjetividad. Esta plasticidad de la verdad puede llevarse a cabo mediante

el control del relato, la narración de los hechos desde la perspectiva que interesa al poder del momento. Como refiere muy acertadamente Gómez de Ágreda (2020):

> El control del relato se vuelve, por lo tanto, fundamental. No el control de la información, sino el de la conformación de las noticias en relatos. La iniciativa en este caso es requisito ineludible porque, en los cortos plazos que se manejan, las contranarrativas pierden toda credibilidad y utilidad. Lo importante es sentar las bases sobre las que se asienta la verdad y dejar luego que el público vaya encajando las piezas que se le vayan sirviendo sobre esa base sesgada.

La renovación del debate sobre las técnicas de control político social ha llevado a una reactualización del pensamiento de filósofos como Foucault o Bentham. La visión de este último del panóptico como paradigma del estado de vigilancia se ha adaptado a la nueva realidad tecnológica de modo que puede hablarse hoy día de un concepto de *postpanopticismo*, en el que la vigilancia no se ejerce desde el exterior sino que es sustituida por una autovigilancia o censura; un sistema en el que la anticipación –no prevención– es preferente a la corrección; un sistema, además, en el que el colectivo controla al individuo (Martínez, Tudela y Alegre, 2018: 141-142).

Esta convivencia con el enemigo, en esta visión paranoica de la realidad social, lleva al poder político a considerar a sus ciudadanos como sujetos susceptibles de control. De ahí que el debate sobre las técnicas de control político y social vuelva a estar sobre la mesa, máxime cuando estamos viviendo la puesta en práctica del mayor experimento de ingeniería social en la humanidad, el sistema de crédito social chino (*Chengxin wenhua*).

Como se recordaba en el informe elaborado por la Omega Research Foundation para el Panel STOA del Parlamento Europeo (Omega Research Foundation y European Parliament, 1999) las tecnologías de control político eran un *nuevo tipo de arma*:

> Es el producto de la aplicación de la ciencia y la tecnología al problema de neutralizar a los enemigos internos del Estado. Está dirigido principalmente a poblaciones civiles, y no está destinado a matar (y sólo rara vez lo

> hace). Está dirigido tanto a los corazones y las mentes como a los cuerpos. [...] Este nuevo armamento va desde los medios de monitoreo de la disidencia interna a los dispositivos para controlar las manifestaciones; desde nuevas técnicas de interrogatorio hasta métodos de control de prisioneros. Los efectos previstos y reales de estas nuevas ayudas tecnológicas son más amplios y complejos que el armamento más letal que complementan.

6.3 *El perfilado político: Cambridge Analytica*

En las democracias occidentales también se han producido episodios de manipulación de masas. Cambridge Analytica ha sido, por el momento, el más relevante.

Según De La Sancha (2019) la empresa accedió por medio del psicólogo Alexander Kogan, profesor en la Universidad de Cambridge, a los datos de casi 50 millones de perfiles de usuarios de Facebook. Para ello, Kogan replicó una aplicación empleada en sus investigaciones académicas –*thisisyourdigitallife*– que los usuarios de Facebook podían descargarse para realizar un exhaustivo test de personalidad político a cambio de una remuneración de 2 a 5 dólares. La *app* recogía datos no solo de los usuarios que habían autorizado participar en una investigación académica, sino en la de todos los perfiles de usuarios que interactuarán con ellos, con independencia de que hubieran dado su consentimiento a participar en la misma investigación. Con esta información Cambridge Analytica desarrolló un programa que le permitía predecir el comportamiento político de los usuarios, producto que puso a disposición de su cliente, Trump, para mejorar los objetivos de su campaña electoral.

El 17 de marzo de 2018 una investigación conjunta por los rotativos The New York Times, The Observer y The Guardian (Rosenberg, Confessore y Cadwalladr, 2018) hizo pública la filtración de datos llevada a cabo por la empresa británica en la multinacional norteamericana.

La estrategia empleada por la empresa consultora consistía en la realización de una campaña de *microtargeting* político con el propósito de influir, y no solo persuadir. En este sentido, autores científicos ponen de relieve el

empleo de técnicas militares de operaciones de información (PsysOps), orientadas a propósitos manipulativos llevadas a cabo sobre objetivos especialmente vulnerables, con el propósito de modificar sus sentimientos y moverlos hacia los intereses u objetivos fijados (Suárez-Gonzalo, 2018: 27).

De acuerdo con el autor que acabamos de mencionar, el escándalo Cambridge Analytica pone de relieve la insuficiencia del marco regulatorio actual, dado que el daño generado por el acceso no consentido a datos personales de individuos que habían comunicado con miembros del conjunto de control –que sí habían otorgado su consentimiento– no se cubre por el consentimiento informado de estos. Nuestro consentimiento tiene por ello una dimensión social que no es abarcada por nuestra declaración positiva de tratamiento, dejándola sin cobertura legal ni garantía.

§7. Control sanitario epidemiológico

7.1 *La situación de pandemia ocasionada por la COVID-19*

La pandemia ocasionada por la COVID-19 parece una prueba de concepto en toda regla. La idea de prueba de concepto es muy empleada en ciberseguridad, y se refiere a ataques desplegados para comprobar la capacidad de reacción del enemigo, como sucedió con el virus informático Wannacry (Rodríguez, 2017), que afectó a un innumerable conjunto de redes informáticas en todo el mundo –especialmente al Servicio de Salud británico–, creando la primera oleada mundial de ciberataques conocida.

Tras un período de confusión y opacidad en la región de Hubei, donde se halla la ciudad china de Wuhan, en diciembre de 2019 el Gobierno de Xinping decidió hacer pública la enfermedad. La Organización Mundial de la Salud la declaró pandemia el 11 de marzo de 2020.

Frente a la nueva plaga surgieron dos formas de lucha: la asiática, intensamente basada en el control de población y el empleo de tecnología de rastreo para la localización y aislamiento de los contagiados; y la occidental, basada en un cierre de fronteras (De Miguel, 2020) y aislamiento físico, primero internacional,

y luego domiciliario de su población hasta mediados de 2020. Las consecuencias económicas de ambos modelos son de todos conocidas (Deloitte España, 2020).

Conscientes de los resultados logrados en Asia, aunque en la ignorancia de calibrar hasta qué punto había sido efectiva la medida, los países europeos imitaron el modelo de gestión de crisis sanitaria de los asiáticos y comenzaron a proponer soluciones tecnológicas.

En primer término, las soluciones consistían en el desarrollo de *apps* para teléfonos móviles que permitieran el autodiagnóstico, descongestionadoras de los servicios de atención primaria. En segundo lugar, se desarrollaron estudios de movilidad contando con los datos de tráfico puestos a disposición de los respectivos gobiernos por las operadoras de telefonía móvil. Por último, y para la fase de desescalada, se diseñaron *apps* de rastreo para la localización de casos positivos y su aislamiento, a fin de frenar el contagio, elevadamente alto en este virus.

El desarrollo de las aplicaciones de rastreo evidenció diferencias de enfoque, particularmente en cuanto a la protección de la privacidad de los usuarios. Así, mientras que los países asiáticos (China, Corea, Taiwan y Japón), así como Israel, emplearon la señal GPS de geolocalización de los teléfonos móviles para realizar la identificación de todos los ciudadanos; en los países europeos se optó por el modelo de Singapur de uso de la señal Bluetooth. Aun así, fue de apreciar diferencias entre los socios europeos. Polonia, por ejemplo, requiere al usuario que envíe su señal GPS en un plazo máximo de 20 minutos, so pena de tener que presentarse en una comisaría policial para su identificación; además, obliga a los enfermos a realizarse y enviar un *selfie* que podrá conservarse durante seis años (Alarcón, 2020).

En el caso europeo se constituyó en abril de 2020 un consorcio denominado Pan-European-Privacy-Preserving Proximity Tracing, PEPP-PT), que pretendía el desarrollo de un modelo único de intercambio de datos basada en la tecnología Bluetooth. Sin embargo, el proyecto generó una gran desconfianza pública al diseñar un sistema centralizado de recogida de los códigos aleatorios generados por los teléfonos móviles, pues permitía a los gobiernos realizar actividades de cruce de datos con otros que ya tuviera en su poder (Pérez, 2020). Por ello, se constituyó un nuevo grupo de trabajo formado por 26 ingenieros bajo el auspicio del Instituto Federal Suizo de Tecnología (EPFL)

bajo la dirección de la española Carmela Troncoso. El nuevo modelo desarrollado denominado Decentralized Privacy-Preserving Proximity Tracing (DP-3T), al contrario del anterior, se basaba en un sistema descentralizado de almacenamiento de datos en los dispositivos de los usuarios, que únicamente transmitían a una base central los códigos aleatorios y efímeros. Los datos son remitidos voluntariamente por los usuarios, que únicamente reciben una señal de alerta si en el sistema central se cruzan dos códigos aleatorios que demuestran un contacto a menos de dos metros por más de quince minutos. El gobierno español, pese a que inicialmente adoptó la iniciativa alemana del consorcio PEPP-PT, tras la Recomendación del Parlamento Europeo sobre diseño de las *apps*, se adscribió al modelo suizo.

El último factor de incidencia en el panorama generado por la pandemia y su control informático en Europa vino de la mano de las multinacionales norteamericanas Google y Apple. En una unión sin precedentes, ambas ofrecieron el 10 de abril a los países europeos un diseño de *app* muy similar al modelo DPP-3T, pero resolviendo los defectos de funcionamiento como el de la *app* TraceTogether –ejecución en segundo plano, con menor consumo de batería– al estar integrada la aplicación dentro de los propios sistemas operativos IOS y Android.

7.2 *Tecnologías de lucha contra la pandemia. Implicaciones en la privacidad*

Como ya decíamos, parece que la pandemia ocasionada por el virus SARS-2 parece una prueba de concepto para comprobar el estado de funcionamiento y la capacidad de respuesta de las naciones frente a una crisis de naturaleza mundial y multicapa.

El hecho de que se viniera advirtiendo de esta posibilidad –algo muy factible, dadas las anteriores epidemias de Zica, SARS-1, Ébola y otras– así como el clima de creciente tensión internacional entre EE. UU. y China, hace pensar que las consecuencias de esta pandemia irán más allá de las sanitarias y económicas.

La diferente forma y grado de éxito en la gestión de la crisis ha dado ventaja propagandística al modelo de Estado vigilante chino. Al igual que su

población está convencida de la efectividad del sistema de crédito social, pese a lo que signifique de dilución de las barreras entre lo público y lo privado, en Europa y en el resto del mundo se comienza a ver el modelo desde otra perspectiva mucho más favorable. Privacidad a cambio de salud comienza a ser una opción razonable (Alarcón, 2020). Basta ver la complejidad del modelo de toma de decisiones europeo para adoptar medidas de trazado digital o de estudios de movilidad personal o colectiva y sus resultados en el número de fallecidos, para comprobar las bondades de la efectividad digital asiática. Esta efectividad por el acceso sin restricciones de privacidad a datos médicos es, precisamente, la reclamación que se realiza en Occidente por las grandes operadoras del *Big Data* (Varsavsky, 2020); necesitan acceso irrestricto a datos sanitarios de calidad para poder competir con el gigante chino, algo que no se logrará con los actuales estatutos de privacidad (Foroohar, 2020).

Puede decirse que, desde el punto de vista geoestratégico, la COVID-19 no va a producir –por sí misma– un cambio mundial, pero sí va a acelerar procesos que ya se estaban produciendo (Melvin, 2020), programas de control social que ya se estaban desarrollando. Y, en este sentido, China aparece como el nuevo modelo hegemónico que viene a poner en evidencia la incapacidad del orden mundial actual para hacer frente a desafíos de esta escala. Daniel Innerarity, citado por Munárriz (2020), manifiesta sobre el proceso actual: "La amenaza es la tentación de ese autoritarismo benevolente, que ahora se observa en esa versión china, con imagen de eficacia ganada gracias a que no pierden el tiempo con formalidades democráticas y atención a derechos humanos". Como señala el mencionado autor, la epidemia lanza al mundo frente a una pinza entre políticos y tecnólogos por el control mundial.

No solo vamos a vivir un cambio de poderes hegemónicos; el alcance de la privacidad y la protección de datos también van a cambiar. Como refleja García Mexía (Alarcón, 2020), tanto las grandes empresas como los Gobiernos saldrán más poderosos de esta crisis: las empresas, porque habrán aumentado su nivel de influencia en el panorama estatal –la alianza Apple-Google es un ejemplo–; los gobiernos, porque habrán acostumbrado a sus ciudadanos a nuevos instrumentos de control social, suministrados por las grandes empresas tecnológicas, que se incorporarán a sus dispositivos para esta o para la siguiente ocasión. Hemos podido comprobar, una y otra vez, cómo los poderes

de excepción entregados al Estado para la resolución de determinadas crisis (guerra fría, terrorismo, lucha contra el crimen organizado, crisis económicas…) nunca han sido devueltos: se han reconvertido, se han ampliado temporal o directamente se han mantenido sin fundamento legal y desviados para fines no propuestos inicialmente.

Una prueba de este cambio de mentalidad y preocupación por nuestra privacidad la constituye la alianza Apple-Google. Aparte de haber servido de campaña de propaganda para ambas empresas, su colaboración en un momento de impotencia de las cancillerías occidentales para hacer frente a la pandemia ha dado lugar a cambiar el estado de opinión sobre el acceso al mercado de los datos de salud. Antes, lo que hubiera ocasionado una repulsa pública sin precedentes (pese al cada vez más extendido empleo de dispositivos que captan datos de esta naturaleza: relojes inteligentes, pulseras deportivas, *apps* de *personal sport training*...) se ha aceptado con total naturalidad (Foroorhar, 2020).

Que las aplicaciones generadas, con todo el buen propósito, para rastrear a personas asintomáticas puedan albergar ese doble uso –sanitario y comercial– es un hecho; cuando menos, existen elementos de sospecha para creer en su realidad. La participación de la alianza Apple-Google ha traído como consecuencia que las aplicaciones tipo Radar COVID alberguen partes del código fuente no relacionadas con el funcionamiento de la *app*; y que, según su configuración –controlada por las empresas citadas– puedan transmitir datos a sus servidores. Al hacerse público el código fuente abierto de la aplicación los analistas observaron la presencia de la librería Firebase, empleada por los desarrolladores para su prueba y control. Como han puesto de relieve los técnicos, la aplicación no solo tiene funcionalidades de desarrollo, sino también de comunicación de datos tanto a las autoridades sanitarias como a las empresas que suministran la *app* (Colomé, 2020): "Es una navaja suiza para desarrolladores". De esta funcionalidad nadie ha sido informado, pudiendo dar lugar a transferencias internacionales de datos no consentidas ni –lo que es peor– autorizadas tras la declaración de nulidad del acuerdo UE-EE. UU. "Escudo de Privacidad", que declaró la compatibilidad del sistema de protección de datos estadounidense y europeo.

La crisis sanitaria de la COVID-19 y sus instrumentos informáticos de gestión son el último episodio en el avance del sistema de control político y social. Como pone de relieve Foorhar (2020) los países tendrán que optar entre uno de los tres modelos de gestión de la privacidad existentes: el chino, de control total por el Estado; el norteamericano, de predominio de las grandes corporaciones; y el europeo, anclado en unos principios éticos que son atacados por los dos anteriores. El *soft-power* chino parece que ha ganado la presente partida con actividades como las de la asistencia sanitaria a Europa, la Iniciativa Belt and Road y el ejemplo de gestión ofrecido. Pero la contienda por el dominio del orden mundial continúa.

§8. Conclusiones

Cuanto mayor poder tiene el individuo –y más aumenta su capacidad de hacer el mal– más poder reclaman los Estados para mantener la seguridad de todos. Las situaciones de crisis generan, además, nuevos episodios que sirven de narración justificadora de las malas solicitudes de poderes de excepción; poderes que nunca se devuelven porque las amenazas se mantienen, o al menos así se narran. Los Estados evidencian una tendencia mantenida en el tiempo a prolongar sus poderes de excepción ampliando los supuestos de aplicación, las capacidades o facultades de intervención, o directamente desviando su uso hacia otras finalidades no contempladas inicialmente.

A este nuevo escenario de control se han sumado las operadoras de telecomunicaciones y servicios digitales. Los Estados se han asociado con ellas, o han mirado hacia otro lado cuando era conveniente, para establecer un nuevo orden económico que beneficia a ambas partes, el capitalismo de vigilancia. Esta nueva versión del capitalismo tradicional va un paso más allá de las limitaciones que se habían establecido al régimen de libertades. Ahora, con mayor crudeza, se refleja el sentido de la protección que querían conferir los derechos de protección de datos. No era realmente la información personal lo que contaba como objeto de protección, sino el daño que podía ocasionar su conocimiento y tratamiento a otros derechos fundamentales, particularmente al propio derecho a la libertad personal, a actuar en libertad y a decidir el futuro de cada uno.

Escándalos como el de Cambridge Analytica nos han puesto de relieve que la privacidad es un ecosistema y que tiene un componente colectivo. Describe Veliz que "La privacidad es colectiva, como el medioambiente. Si no cuidas tus datos, otros sufren las consecuencias". Sin una continua vigilancia de los propios titulares de los datos sobre las repercusiones de sus decisiones informacionales (*selfies*, publicaciones en redes sociales, revelación de comunicaciones privadas, configuraciones de privacidad de sus aplicaciones…) todos resultamos afectados. Que 44 ciudadanos españoles dieran lugar a la afectación en su privacidad a 136985 pone de relieve lo que se está diciendo.

Las técnicas de control político y social pueden ser legítimas si obedecen a una finalidad legítima, como el mantenimiento de las libertades y derechos de los ciudadanos, o el afrontamiento colectivo de una crisis sanitaria. La existencia de normas jurídicas habilitantes de excepciones a los derechos fundamentales es, pues, legítima. Por ello, su mera mención no implica una ilegalidad; será el abuso de su empleo o extensión indebida de su alcance lo que determine su ilegitimidad.

Contemplamos un escenario de contienda jurídica entre poderes ejecutivos y legislativos, de una parte, y judicial por otro, en el que este rechaza –una y otra vez– intentos técnicamente incorrectos de ampliar las restricciones a los derechos. Las empresas multinacionales y los *lobbies* de presión intentan influir en los representantes del poder judicial para lograr un control, o al menos una diferencia significativa, en las decisiones que afectan al nuevo orden económico mundial. Este debate está pasando desapercibido a la opinión pública, como es el caso del TJUE sobre la regulación de la conservación de datos personales o los acuerdos de privacidad con Estados Unidos, dado que los fallos judiciales están reflejando siempre la misma realidad: un intento continuado, aunque mal ejecutado, de reducir la incertidumbre que genera la libertad de los ciudadanos, sustituyéndola por predecibilidad e incluso modificación de su comportamiento.

Sirva como colofón de este análisis las palabras contenidas a modo de declaración de principios en el Considerando (4) del RGPD: "El tratamiento de datos personales debe estar concebido para servir a la humanidad".

Ojalá se pueda conseguir.

Referencias bibliográficas

A (FC) and Others (FC) (Appellants) v. Secretary of State for the Home Department (Respondent) & X (FC) and Another (FC) (Appellants) v. Secretary of State for the Home Department (Respondent). House of Lords, Great Britain (UK). 16 de diciembre de 2004.

Agencia EFE (2019). San Francisco prohíbe el uso del reconocimiento facial para identificar a criminales. lavanguardia.com, 17 de mayo. Disponible en: <https://www.lavanguardia.com/internacional/20190515/462256381193/san-francisco-reconocimiento-facial-prohibe.html> (consulta: 28-11-2020).

Agencia Española de Protección de Datos (2018). *A.E.P.D. ante CAMBRIDGE ANALYTICA, FACEBOOK INC., FACEBOOK IRELAND LIMITED, FACEBOOK SPAIN, S.L.* (Agencia Española de Protección de Datos, 29 de octubre). Procedimiento n.º E/01873/2018.

Agencia Española de Protección de Datos (2018b). Guía sobre el uso de videocámaras para seguridad y otras finalidades. aepd.es. Disponible en: <https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf>.

Agencia Española de Protección de Datos, Fiscalía General del Estado, y Ministerio de Trabajo, Migraciones y Seguridad Social (2019). Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles. aepd.es, 12 de septiembre. Disponible en: <https://www.aepd.es/sites/default/files/2019-12/consecuencias-administrativas-disciplinarias-civiles-penales.pdf> (consulta: 3-12-2020).

Alarcón, I. (2020). En la guerra contra el coronavirus, Europa está perdiendo la batalla de la privacidad. Elconfidencial.com, 17 de abril. Disponible en: <https://n9.cl/n9xa4> (consulta: 6-12-2020).

Álvarez, R. (2017). China implementará un sistema de puntaje ciudadano basado en la confiabilidad. Sí, "black mirror" se vuelve real. xataca.com, 28 de octubre. Disponible en: <https://n9.cl/oko1f> (consulta: 2-12-2020).

Aparici, R., García-Marín, D. (2018). Prosumers and emirecs: Analysis of Two Confronted Theories. *Comunicar* 26(55), 71-79. Disponible en: <https://doi.org/10.3916/c55-2018-07>.

Arana, I. (2019). La inquietante apuesta china por el reconocimiento facial. *La Vanguardia*, 17 de mayo. Disponible en: <https://n9.cl/c1kk> (consulta: 2-12-2020).

Arquilla, J., Ronfeldt, D., Rand Corporation (2001). Networks and Netwars: the Future of Terror, Crime, and Militancy. Rand.org. Disponible en: <https://www.rand.org/pubs/monograph_reports/MR1382.html> (consulta: 20-11-2019).

Article 29 Data Protection Working Party (2018). ARTICLE 29 DATA PROTECTION WORKING PARTY. https://ec.europa.eu/newsroom/article29. Disponible en: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826>

Ballester, J. M. (2020). Soros controla a 12 de los 100 jueces del Tribunal Europeo de Derechos Humanos. abc.es, 23 de febrero. Disponible en: <https://n9.cl/nmh12> (consulta: 4-12-2020).

Basilon (2012). IBM y el Holocausto. *La Segunda Guerra*, 19 de septiembre. Disponible en: <https://www.lasegundaguerra.com/viewtopic.php?t=11768> (consulta: 14-11-2020).

BBC News/Mundo (2017). El asombroso sistema de videovigilancia en China que detectó a un reportero de la BBC en tan solo 7 minutos. *BBC News Mund*o, 26 de diciembre. Disponible en: <https://www.bbc.com/mundo/media-42358019> (consulta: 28-11-2020).

Bigelow, K. (Dir.). (2012). *La noche más oscura (Zero Dark Thirty)* [film]. EE. UU: Columbia Pictures.

Campbell, D. (1988, 12 de agosto). Somebody's Listening. cryptome.org, 12 de agosto. Disponible en: <http://cryptome.org/jya/echelon-dc.htm> (consulta: 15-11-2020).

Campbell, D. (1999). Part 2/5:The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ultilanguage leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition. duncancampbell.org. Disponible en: <https://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf>. Parlamento Europeo - STOA (Ed.).

Campbell, D. (n.d.). Echelon. duncancampbell.org. Disponible en: <https://www.duncancampbell.org/content/echelon >(consulta: 14-11-2020).

Carlini, A. (2018). Las Redes Sociales Como Factor De Desestabilización (Ed.). *ieee.es*, 2 de julio. Disponible en: <https://n9.cl/jqoxm> (consulta: 15-11-2020).

Castells, M., Hernández, M.ª (2014). *Comunicación y poder*. Madrid: Alianza Editorial.

Chandor, J. C. (Dir.) (2011). *Margin Call* [film]. EE. UU.: Before the Door Pictures.

Cilevics, B. (2018). Legal challenges related to hybrid war and human rights obligations. En Comité de Asuntos Legales y Derechos Humanos & a Parlamentaria del Consejo de Europa (eds.), *Parlamentary Assembly C - Council of Europe*. Disponible en: <https://pace.coe.int/en/>.

Colaboradores de los proyectos de Wikimedia (2020a). S and Marper v United Kingdom. *wikipedia.org*, 16 de septiembre. Disponible en: <https://n9.cl/jyjn6> (consulta: 27-11-2020).

Colaboradores de los proyectos Wikimedia (2003). Alan Turing. *wikipedia.org*, 4 de agosto. Disponible en: <https://es.wikipedia.org/wiki/Alan_Turing> (consulta: 14-11-2020).

Colaboradores de los proyectos Wikimedia (2005). Web 2.0. *wikipedia.org*, 5 de octubre. Disponible en: <https://es.wikipedia.org/wiki/Web_2.0> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2008a). Computación en la nube. *wikipedia.org*, 13 de septiembre. Disponible en: <https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia. (2008b). Ejecución de un test aplicado a una tarea. *wikipedia.org*, 10 de octubre. Disponible en: <https://es.wikipedia.org/wiki/Prueba_de_concepto> (consulta: 6-12-2020).

Colaboradores de los proyectos Wikimedia (2011). Primavera Árabe (2010-2012). *wikipedia.org*, 29 de enero. Disponible en: <https://es.wikipedia.org/wiki/Primavera_%C3%81rabe_(2010-2012)> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia. (2018). Islamic State of Iraq and the Levant. *wikipedia.org*, 9 de diciembre. Disponible en: <https://en.wikipedia.org/wiki/Islamic_State_of_Iraq_and_the_Levant> (consulta: 14-11-2020).

Colaboradores de los proyectos Wikimedia (2020b). Russian Business Network. *wikipedia.org*, 27 de junio. Disponible en: <https://es.wikipedia.org/wiki/Russian_Business_Network> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020c). BlaBlaCar. *wikipedia.org*, 9 de julio. Disponible en: <https://es.wikipedia.org/wiki/BlaBlaCar> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020d). Iniciativa de la Franja y la Ruta. *wikipedia.org*, 1 de agosto. Disponible en: <https://es.wikipedia.org/wiki/Iniciativa_de_la_Franja_y_la_Ruta> (consulta: 3-12-2020).

Colaboradores de los proyectos Wikimedia (2020e). Ecoterrorismo. *wikipedia.org*, 8 de septiembre. Disponible en: <https://es.wikipedia.org/wiki/Ecoterrorismo> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020f). Prosumidor. *wikipedia.org*, 20 de septiembre. Disponible en: <https://es.wikipedia.org/wiki/Prosumidor> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020g). Herman Hollerith. *wikipedia.org*, 24 de septiembre. Disponible en: <https://es.wikipedia.org/wiki/Herman_Hollerith> (consulta: 14-11-2020).

Colaboradores de los proyectos Wikimedia (2020h). ENIAC. *wikipedia.org*, 14 de octubre. Disponible en: <https://es.wikipedia.org/wiki/ENIAC> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020i, 3 de noviembre). Megaupload. *wikipedia.org*. Disponible en: <https://es.wikipedia.org/wiki/Megaupload> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020j). Criptomoneda. *wikipedia.org*, 8 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/Criptomoneda> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020k). Bitcoin. *wikipedia.org*, 12 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/Bitcoin> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (202l). Internet. *wikipedia.org*, 13 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/Internet#Origen> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020). Al Qaeda. *wikipedia.org*, 14 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/Al_Qaeda> (consulta: 14-11-2020).

Colaboradores de los proyectos Wikimedia (2020). Iphone. *wikipedia.org*, 14 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/IPhone> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020n). Osama bin Laden. *wikipedia.org*, 14 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/Osama_bin_Laden#cite_note-bergen75-38> (consulta: 14-11-2020).

Colaboradores de los proyectos Wikimedia (2020o). Patriot Act. *wikipedia.org*, 15 de noviembre. Disponible en: <https://en.wikipedia.org/wiki/Patriot_Act#Title_V:_Removing_obstacles_to_investigating_terrorism> (consulta: 15-11-2020).

Colaboradores de los proyectos Wikimedia (2020p). Bogeyman. *wikipedia.org*, 19 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/Bogeyman> (consulta: 2-12-2020).

Colaboradores de los proyectos Wikimedia (2020q). Deng Xiaoping. *wikipedia.org*, 30 de noviembre. Disponible en: <https://es.wikipedia.org/wiki/Deng_Xiaoping#Ascenso_al_poder_y_reformas_econ> (consulta: 2-12-2020).

Colaboradores de proyectos Wikimedia (2020r). Cambridge Analytica. *wikipedia.org*, 24 de septiembre. Disponible en: <https://es.wikipedia.org/wiki/Cambridge_Analytica> (consulta: 3-12-2020).

Colom-Piella, G. (n.d.). La Gran Revolución. *dialnet/*unirioja.es. Disponible en: <https://dialnet.unirioja.es/servlet/extaut?codigo=1194473> (consulta: 17-11-2020).

Comunidad Autónoma de Madrid (2020). Coronavirus Comunidad de Madrid. Coronavirus Comunidad de Madrid. Disponible en: <https://coronavirus.comunidad.madrid/> (consulta: 6-12-2020).

Consejo de la Unión Europea (2004). Consejo Europeo de Bruselas 17 y 18 de junio de 2004. Conclusiones de la Presidencia. 10679/2/04 REV 2. https://www.consilium.europa.eu/. Disponible en: <https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/81750.pdf>.

Coppola, F. F. (Dir.) (1974). *TheGodfather II* [film]. EE. UU.: Coppola Co. Production. Productor: Francis Ford Coppola. Distribuida por Paramount Pictures.

Coppola, F. F. (Dir.) (1990). *The Godfather III* [film]. EE. UU.: Paramount Pictures.

Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. *SSRN Electronic Journal*. Disponible en: <https://doi.org/10.2139/ssrn.3175792>

De Diego Retuerta, J. (2020). Publicación de datos personales de terceros en redes sociales. *piconyasociados*, 17 de febrero. Disponible en: <https://n9.cl/cvho8> (consulta: 3-12-2020).

De Gorgot, E. (2012). Tony Soprano Vs Vito Corleone. *Jot Down Cultural Magazine*, 7 de agosto. Disponible en: <https://www.jotdown.es/2012/08/tony-soprano-vs-vito-corleone/> (consulta 25-11-2020).

De la Sancha, M. (2018). Claves para entender el escándalo que afecta a millones de usuarios de Facebook. *Huffpost*, 20 de marzo. Disponible en: <https://n9.cl/eci9u>.

De Miguel, B. (2020, 17 de marzo). La UE cierra sus fronteras por primera vez en su historia y no dejará entrar a ciudadanos de terceros países. *El País*. Disponible en: <https://n9.cl/qz4xq> (consulta: 6-12-2020).

Deloitte España (2020, March 24). El impacto económico del COVID-19. *Deloitte.com*. Disponible en: <https://www2.deloitte.com/es/es/pages/about-deloitte/articles/impacto-economico-del-covid19.html> (consulta: 6-12-2020).

European Commission For The Efficiency Of Justice (CEPEJ) (2018). European ethical charter on the use of artificial intelligence in judicial systems and their

environment.*rm.coe.int*. Counseil of Europe. Disponible en: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

European Court of Human Rights - Research Division (2013). Division de la recherche research division National security and European case-law. *www.echr.coe.int*. Disponible en: <https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf>.

European Parliamentary Research Service (2020). Disruption by technology [YouTube Video]. Disponible en: <https://www.youtube.com/watch?v=cAMKrMoYZ3U&feature=youtu.be>.

European Union Agency for Law Enforcement Cooperation (EUROPOL) (2020). Internet Organised Crime Threat Assessment (IOCTA). *www.europol.europa.eu/*. Disponible en: <https://n9.cl/iwsux>.

Faraldo Cabana, P., Brandariz García, J. Á., María, L. (2004). *Nuevos retos del derecho penal en la era de la globalización*. Valencia: Tirant Lo Blanch.

Fernández, C. B. (2017). ¿Deben someterse los sistemas de inteligencia artificial a un proceso de autorización como el de los medicamentos? *Diario La Ley Ciberderecho* (11).

Ferrer, I. (2020). Países Bajos veta un algoritmo acusado de estigmatizar a los más desfavorecidos. *El País*, 13 de febrero. Disponible en: <https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html>.

Financial Action Task Force (FATF). (2019). Virtual Assets and Virtual Asset Service Providers. *http://www.fatf-gafi.org/*. Disponible en: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.

Financial Action Task Force (FATF) (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. *fatf-gafi.org*. Disponible en: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf> (consulta: 11-2020).

Fojón, J. E. (2006). Vigencia y limitaciones de la guerra de cuarta generación, 27 de febrero. Real Instituto Elcano. Disponible en: <https://acortar.link/WmP0z> (consulta: 22-6-2021).

Foroohar, R. (2020, 16 de abril). Las grandes tecnológicas serán las ganadoras de esta crisis, y es un problema (E. Esteban, Interviewer). Disponible en: <https://n9.cl/fxq2z>.

Galán. (2018). Amenazas híbridas: nuevas herramientas para viejas aspiraciones. realinstitutoelcano.org, 13 de diciembre. Real Instituto Elcano Disponible en: <https://n9.cl/w1wfi> (consulta: 17-11-2020).

Godement, F., Przychodniak, M., Drinhausen, K., Knight, A., Kania, E. B., Stanzel, A. (2018). The china dream goes digital: Technology in the age of xi. *European Council on Foreign Relations*. Disponible en: <https://n9.cl/gs0h>.

Gómez de Ágreda, A. (2019). *Mundo orwell: Manual de supervivencia para un mundo hiperconectado*. Barcelona: Ariel.

Gómez de Ágreda, Á. (2020). Ética y límites de la libertad de opinión y de prensa. *Amenaza Híbrida. La Guerra Imprevisible*. Ministerio de Defensa pp. 19-26). Disponible en: <https://n9.cl/tlxob>.

González Álvarez, J. L., López Osorio, J. J., Muñoz Rivas, M. (2018, septiembre). La valoración policial del riesgo de violencia contra la mujer pareja en España – Sistema VioGén, septiembre. Disponible en: <https://cutt.ly/xnGovGW> (consulta: 29-11-2020).

González Pascual, M. I. (2020). El Tribunal Constitucional Federal Alemán ante la compatibilidad con los derechos fundamentales de la Normativa Nacional de Origen Europeo de Prevención de Delitos. *Revista De Derecho Comunitario Europeo* (34), 945-966. Disponible en: <https://recyt.fecyt.es/index.php/RDCE/article/view/46023/27524>.

Gonzalo, M. (2018, 25 de marzo). El día en que nos dimos cuenta de que teníamos un problema con Facebook. Huffingtonpost.com, 25 de marzo. Disponible en: <https://n9.cl/7aih> (consulta: 3-12-2020).

Han, B.-C. (2020, 21 de marzo). La emergencia viral y el mundo de mañana. Byung-Chul Han, el filósofo surcoreano que piensa desde Berlín. *El País*, 21 de marzo. Disponible en: <https://n9.cl/02nv> (consulta: 6-12-2020).

Hernández, J. C. (2020). Decisiones algorítmicas de perfilado: régimen y garantías jurídicas. *Revista Española De Derecho Administrativo* (203), 281-322.

Instituto Nacional de Estadistica (INE) (2019). Evolución de la movilidad por ámbito geográfico durante el estado de alarma por COVID-19. Gobierno de España. Disponible en: < https://www.ine.es/covid/covid_movilidad.htm> (consulta: 6-12- 2020).

Jakobs, G., Cancio Meliá, M. (2003). *Derecho penal del enemigo*. Disponible en: <https://lpderecho.pe/descargue-pdf-derecho-penal-enemigo-gunther-jakobs-cancio-melia/>.

King, M. R. (Dir.). (n.d.). *The Good Wife* [serie]. EE. UU.: Scott Free Productions, King Size Productions.

Knight, A. (2018). Credit: The god of China's big data era. *The China dream goes digital: Technology in the age of Xi*. Disponible en: <https://ecfr.eu/publication/the_china_dream_digital_technology_in_the_age_of_xi/>.

Kostopoulos, L. (2019). The Role of Data in Algorithmic Decision-Making | UNIDIR. *unidir.org*. Disponible en: <https://www.unidir.org/publication/role-data-algorithmic-decision-making> (consulta: 26-11-2020).

La UE crea un nuevo sistema para conectar apps de rastreo de COVID-19 (2020, 26 de octubre). Gaceta Médica, 26 de octubre. Disponible en: https://n9.cl/lpbhy (consulta: 5-12-2020).

La Vanguardia (2019). El INE rastrea desde hoy los móviles de los españoles para su polémico estudio. *La Vanguardia*, 18 de noviembre. Agencias de Noticias. Disponible en: <https://acortar.link/eq1sk> (consulta: 6-12-2020).

Lejeune, B. (2020). Cómo financian el Consejo de Europa la Open Society de George Soros y Microsoft de Bill Gates. *La Gaceta de la Iberosfera*, 30 de noviembre. Disponible en: <https://n9.cl/ubt8d> (consulta: 4-12-2020).

LOI pour une République numérique (1). Pub. L. No. 2016-1321 (2016).

López Altamirano, J. (2019, 11 de abril). Origen, evolución y rol del Jurado Penal en Estados Unidos | Jazmín López. IUS360.com, 11 de abril. Disponible en: <https://n9.cl/a22o> (consulta: 29-11-2020).

Luna, A. G. (2012, 7 de noviembre). ¿Quiere contratar un ciberataque? Tan solo cuesta 10 dólares la hora. elconfidencial.com, 7 de noviembre. Disponible en: <https://n9.cl/7k0lg> (consulta: 15-11-2020).

Malenchik vs. State of Indiana. No. 79S02-0908-CR-365, 9 de junio de 2010. Indiana Supreme Court (USA).

Marant, A. (2017). *La noche temática* [Documental], 1 de octubre. Disponible en: <https://www.rtve.es/alacarta/videos/la-noche-tematica/noche-tematica-asi-empieza-terror-estudios/4240981/>.

Martínez Garay, L. (2020). Peligrosidad, algoritmos y *Due Process*: el caso State *vs*. Loomis. *Revista de Derecho Penal y Criminología* (20), 485-502. Disponible en: <https://doi.org/10.5944/rdpc.20.2018.26484>.

Martínez Martínez, R. (2020). Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. *La Ley Digital* (9604). Disponible en: <https://n9.cl/ru94>.

Martín-Retortillo Baquer, L. (2003). La calidad de la ley según la jurisprudencia del tribunal europeo de derechos humanos (especial referencia a los casos «valenzuela Contreras» y «Prado Bugallo», ambos contra España) (1). *Derecho privado y Constitución* (17), 377-406. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/835585.pdf>.

Marzal, C. (2020). PEPP-PT vs DP-3T: Privacidad en la gestión de la crisis del COVID-19. *thiber.org*, mayo (consulta: 6-12-2020).

Melvin, N. (2020, 12 de abril). La pandemia no va a cambiar el mundo, va a acelerar lo que ya estaba pasando (C. Maza, *interviewer*). *elconfidencial*, 12 de abril. Disponible en: <https://n9.cl/i8tz4>.

Méndez, M. A. (2020). El plan del Gobierno para rastrear a 30M de españoles con una "app" tras el confinamiento. elconfidencial.com, 19 de abril. Disponible en: <https://n9.cl/flzg4> (consulta: 6-12-2020).

Mendiola Zuriarrain, J. (2017). China está ensayando con un sistema que anticipa los delitos antes de que se cometan. *El País*, 13 de agosto. Disponible en: <https://elpais.com/tecnologia/2017/08/07/actualidad/1502125524_290007.html?autoplay=1>.

Miguel Martínez Martínez, J., Tudela, A., Alegre Benítez, C. (2018). *El control y la vigilancia en (y de) la red: Gobernanza y subjetivación 1*. Disponible en: <https://acortar.link/YQEwC>.

Miret, J. M. (2013). Alan Turing: El descifrado de la máquina Enigma [Blog]. *El País*, 6 de junio. Disponible en: <https://blogs.elpais.com/

turing/2013/06/alan-turing-el-descifrado-de-la-maquina-enigma.html> (consulta: 14-11-2020).

Mozur, P. (2018). El autoritarismo chino del futuro se basa en la alta tecnología. *The New York Times*, 13 de julio. Disponible en: <https://www.nytimes.com/es/2018/07/13/espanol/china-reconocimiento-facial.html>.

Munárriz, Á. (2020, 22 de marzo). La pandemia agita el orden global y lanza al mundo a una era de incertidumbre. *infolibre.es*, 22 de marzo. Disponible en: <https://acortar.link/kAxfV> (consulta: 6-12-2020).

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org. Disponible en: <https://bitcoin.org/bitcoin.pdf>.

Novo Foncuberta, M. (2016, 22 de marzo). Lecciones británicas: Un modelo de contraterrorismo *El País*, 22 de marzo. Disponible en: <http://agendapublica.elpais.com/lecciones-britanicas-un-modelo-de-contraterrorismo/> (consulta: 14-11-2020).

Oficina de las Naciones Unidas contra la Droga y el Delito (2010). Sistemas policiales de información e inteligencia. *Oficina de las Naciones Unidas contra la Droga y el Delito*. Disponible en: <https://acortar.link/U5s3q>.

Omega Research Foundation (2000). Crowd Control Technologies (An appraisal of technologies for political control). Final Study Working document for the STOA Panel. *omegaresearchfoundation.org*. Disponible en: <https://acortar.link/5Gwuu>.

Omega Research Foundation, European Parliament (1999). Development of Surveillance Technology and Risk of Abuse of Economic Information 1/4. *cryptome.org*. Scientific and Technological Options Assessment. Disponible en: <http://cryptome.org/dst-1.htm>.

Organización para la Cooperación y el Desarrollo Económico (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Disponible en: <https://www.oecd.org/sti/ieconomy/15590267.pdf>.

Organización para la Seguridad y la Cooperación en Europa (2017). Guía de la OSCE sobre actividad policial basada en la inteligencia TNTD/SPMU serie de publicación vol. 13. *osce.org*. Disponible en: <https://www.osce.org/files/f/documents/6/4/455536.pdf>.

Pandemia de COVID-19 - Wikipedia, la enciclopedia libre (2020). *wikipedia.org*. Disponible en: <https://es.wikipedia.org/wiki/Pandemia_de_COVID-19#Internet (consulta: 6-12-2020).

Parlamento Europeo y Consejo Europeo (2001). *Directiva 2001/29/CE, Relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información*, 2001/29/CE.

Parlamento Europeo y Consejo Europeo (2002). *Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)*. Pub. L. No. 2002/58/CE.

Parlamento Europeo y Consejo Europeo (2006). *Directiva 2006/24/CE, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones*. Pub. L. No. 2006/24/CE. Texto consolidado.

Pastorino, C. (2020). WannaCry: tres años después sigue siendo una amenaza activa de la cual debemos aprender | WeLiveSecurity. *welivesecurity*, 12 de mayo. Disponible en: <https://acortar.link/owobb> (consulta: 6-12-2020).

Peirano, M. (2018). Palantir, el mayor invento de espionaje del mundo del megamillonario Peter Thiel. elconfidencial.com, 22 de abril. Disponible en: <https://acortar.link/qQWyi> (consulta: 3-12-2020).

Pérez Colomé, J. (2020). La guerra de la app de rastreo del virus: investigadores y gobiernos europeos compiten por su opción. *El País*, 20 de abril. Disponible en: <https://acortar.link/lJ2N5> (consulta: 6-12-2020).

Puerto, M. I., Sferrazza-Taibi, P. (2018). La sentencia schrems del tribunal de justicia de la unión europea: Un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional ***. *Revista Derecho del Estado* (40), 209-236. Disponible en: <https://doi.org/10.18601/01229893.n40.09>.

Ríos, R. (2018). El escándalo de Facebook y Cambridge Analytica. *ReasonWhy*. Disponible en: <https://acortar.link/OAUuP>.

Rodríguez, D. (2017). Ángel Ochoa: "WannaCry ha sido una prueba de concepto, lo peor puede estar por venir". *globbsecurity.com*, 4 de junio. Disponible en: <https://globbsecurity.com/angel-ochoa-wannacry-prueba-concepto (consulta: 6-12-2020).

Rodriguez, R. (2018, 7 de febrero). Las gafas de Robocop llegan a China: así se descubre a un delincuente en tres segundos. *elconfidencial.com*, 7 de febrero. Disponible en: <https://acortar.link/UsCbH> (consulta: 29-11-2020).

Rosenberg, M., Confessore, N., Cadwalladr, C. (2018). La empresa que explotó millones de datos de usuarios de Facebook. *The New York Times*, 20 de marzo. Disponible en: <https://www.nytimes.com/es/2018/03/20/espanol/cambridge-analytica-facebook.html>.

Rubio Hancok, J. (2016). 11 ocasiones en las que "The Good Wife" se inspiró en noticias reales. *El País*, 8 de mayo. Disponible en: <https://verne.elpais.com/verne/2016/05/06/articulo/1462524269_396260.html> (consulta: 15-11-2020).

S. and Marper vs. United Kingdom. European Court of Human Rights (Grand Chamber), 4 de diciembre de 2008. Applications nos. 30562/04 and 30566/04.

Sánchez, J. M. (2018). Más de 130.000 posibles afectados en España por la filtración de datos de Facebook. *abc.es*, 5 de abril. Disponible en: <https://n9.cl/59vwk> (consulta: 4-12-2020).

Sánchez, J. M. (2020a). Aplicaciones contra el coronavirus: ¿qué hacen otros países para defender la privacidad? *abc.es*, 6 de abril. Disponible en: <https://n9.cl/1492b> (consulta: 6-12-2020).

Sánchez, J. M. (2020b). Radar Covid: luces y sombras de la aplicación de rastreo de coronavirus. *abc.es*, 24 de agosto. Disponible en: <https://n9.cl/ewqt4> (consulta: 6-12-2020).

Schmid, G. (2001). Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON) (2001/2098(INI)). Comisión Temporal sobre el sistema de interceptación. *europarl.europa.eu*. ECHELON. Disponible en: <https://n9.cl/xvtmn>.

Schwabe, J. (2009). Jurisprudencia del Tribunal Constitucional Federal Alemán. (Ed.), *kas.de*. Fundación Konrad Adenauer A.C. Disponible en: <http://www.kas.de/>.

Scorsese, M. (Dir.) (1995). *Casino* [film]. EE. UU.: Universal Pictures, Légende Entreprises, Syalis DA, De Fina-Cappa.

Scott, T. (Dir.). (1998). *Enemigo público (Enemy Of The State)* [film]. EE. UU:. Touchstone Pictures.

Seifert, J. (2008). Data Mining and Homeland Security: An Overview. fas.org. Disponible en: <https://fas.org/sgp/crs/homesec/RL31798.pdf>.

Servicio Andaluz de Salud (2021). COVID-19. Información para la ciudadanía. Disponible en: <https://acortar.link/1p0xr> (consulta: 22-6-2021).

Snowden, E. (2019). *Vigilancia permanente* (E. Cruz Santaella, trans.). Barcelona: Editorial Planeta.

Spielberg, S. (Dir.) (2002). *Minority Report* [film]. EE. UU. 20th Century Fox, DreamWorks SKG, Cruise-Wagner Productions, Blue Tulip Productions, Ronald Shusett/Gary Goldman, Amblin Entertainment, Digital Image Associates, Parkes+MacDonald Image Nation.

State of Wisconsin vs. Eric L. Loomis. 2015AP157-CR (Supreme Court of Wisconsin (USA) July 13, 2016).

Suárez-Gonzalo, S. (2018). Tus likes ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EEUU 2016. *Quaderns Del CAC* (48), 27-36. Disponible en: <https://www.cac.cat/sites/default/files/2018-08/Q44_ES.pdf>.

Talegón, B. (2020, 12 de marzo). El simulacro «evento 201» y las recomendaciones que daban los expertos en octubre de 2019 ante una pandemia global. *diario16*, 12 de marzo. Disponible en: <https://acortar.link/t5srt> (consulta: 6-12-2020).

The Conversation (2020, 21 de abril). El coronavirus ni se creó, ni se escapó de un laboratorio. *nationalgeographic.com*, 21 de abril. Disponible en: <https://acortar.link/WZzF1> (consulta: 6-12-2020).

Trauth-Goik, A. (2019). "Constructing a Culture of Honesty and Integrity": The Evolution of China's Han-centric Surveillance System. *IEEE Technology and Society Magazine* 38(4), 75-81. Disponible en: <https://ieeexplore.ieee.org/abstract/document/8924737>.

Turek, H. (2020). Algoritmos abiertos: experiencias de Francia, los Países Bajos y Nueva Zelanda. *opengovpartnership*, 20 de junio. Disponible en: <https://acortar.link/uyh2d> (consulta: 29-11-2020).

Valencia, G. (2018, 3 de abril). La democracia de la manipulación y el capitalismo de la vigilancia. *semana.com*, 3 de abril. Disponible en: <https://acortar.link/3IMtQ> (consulta: 3-12-2020).

Varsavsky, M. (2020). Coronavirus: del Gran Hermano a la Gran Hermandad. *El País*, 31 de marzo. Disponible en: <https://acortar.link/mIOYw> (consulta: 6-12-2020).

Véliz, C. (2020, 28 de noviembre). La privacidad es colectiva, como el medioambiente. Si no cuidas tus datos, otros sufren las consecuencias (M. G. Pascual, *interviewer*). *El País*, 28 de noviembre. Disponible en: <https://retina.elpais.com/retina/2020/11/27/talento/1606484799_921538.html>.

Verhoeven, P. (Dir.) (1987). *Robocop* [film]. EE. UU.: Orion Pictures.

VV. AA. (Dir.) (1999). *Los Soprano* [serie]. EE. UU.: HBO, Brillstein Entertainment Partners.

Werbach, K. (2020). Panopticon Reborn: Social Credit as Regulation for the Algorithmic Age. *papers.ssrn.com*, 6 de agosto. Disponible en: <https://acortar.link/sfTgc> (consulta: 2-12-2020).

Wright, J., Brooker, C. (Dirs). (2016). *Nosedive* [serie]. United Kingdom: Channel-4/Netflix.

Zhou, C. (2019). China to expand controversial social credit system to 33 million companies ahead of 2020. *abc.net.au*, 19 de septiembre. Disponible en: <https://acortar.link/bID6T> (consulta: 2-12-2020).

Zuboff, S. (1AD, 2019). Qué es el "oscuro" capitalismo de la vigilancia de Facebook y Google y por qué lo comparan con la conquista española (L. Blanco, *interviewer*). *bbc.com*, marzo. Disponible en: <https://www.bbc.com/mundo/noticias-47372336>.

Zuboff, S. (2020a). *La era del capitalismo de la vigilancia* (1.ª ed). Barcelona (España): Paidós.

Zuboff, S. (2020b, 1 de marzo). Capitalismo de la vigilancia. *políticaexterior.com*, 1 de marzo. Disponible en: <https://www.politicaexterior.com/articulo/capitalismo-de-la-vigilancia/> (consulta: 29-11-2020).