Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

JONATÁN CRUZ ÁNGELES*

TECNOLOGIAS EMERGENTES PARA MEJORAR LA GESTION DE LAS FRONTERAS EUROPEAS: *¿QUO VADIS, FRONTEX?*

1. *Introducción*

El sistema de gestión actual de las fronteras externas de la Unión Europea es un ejemplo perfecto de un poder disciplinario[1], es decir, el poder que se ejerce a través de mecanismos de vigilancia y control para regular la conducta de las personas. Para Foucault, el control fronterizo representaría claramente una forma de ejercer este tipo de poder, ya que busca regular la entrada y salida de personas de un territorio determinado. Esta tesis sostiene que el control fronterizo se convierte en un mecanismo para la normalización de las conductas y la construcción de una ciudadanía controlada. Entonces, la frontera se convierte en un lugar donde se establecen las normas de conducta y se delimitan los límites entre lo permisible y lo prohibido. De este modo, el control fronterizo se convierte en un mecanismo para la construcción de la identidad nacional y la delimitación de lo que se considera "nosotros" y "ellos". Además, Foucault argumenta que el control fronterizo también es una forma de ejercer el poder a través de la vigilancia. La vigilancia fronteriza busca detectar y prevenir cualquier conducta considerada anormal o peligrosa. Esto se logra a través de la

* Profesor Ayudante Doctor en el Área de Derecho Internacional Público y Relaciones Internacionales, Departamento de Derecho Público y Común Europeo, Facultad de Ciencias Sociales y Jurídicas, Universidad de Jaén (España). ORCID: 0000-0002-8648-5525.

[1] M. FOUCAULT, *Surveiller et punir*, Paris, 1975.

implementación de mecanismos de control como la documentación, la registración y la detección de personas sospechosas.

Una frontera genera discriminación[2] de aquellas personas que pertenecen a un colectivo imaginario al que identificamos como inmigración irregular. Una forma de desigualdad y exclusión social. Según la tesis de Rancière, el control fronterizo sería una especie de mecanismo para la reproducción de las desigualdades sociales, ya que se utiliza para delimitar quién tiene derecho a entrar y vivir en un territorio determinado. Rancière sostiene que la inmigración irregular se presenta como un problema a ser controlado y eliminado, en lugar de como una oportunidad para ampliar la diversidad y el progreso social. La inmigración irregular se ve como una amenaza a la seguridad y a la estabilidad del territorio, en lugar de como una oportunidad para ampliar la diversidad cultural y la riqueza humana. Además, Rancière argumenta que el control fronterizo también es una forma de ejercer el poder a través de la exclusión. La exclusión fronteriza busca excluir a aquellas personas consideradas como "otras" o "extranjeras", negando su derecho a entrar y vivir en un territorio determinado. Esto se logra a través de la implementación de mecanismos de control como la deportación, el refugio y la detención de personas inmigrantes.

Partiendo de esta premisa, debemos tener en cuenta, además, cómo la pandemia ha tenido un gran impacto en el control de nuestras fronteras[3]. Según la tesis defendida por Agamben, la emergencia sanitaria podría concebirse como un aumento del control estatal y la restricción de la libertad individual, con el objetivo de proteger la salud pública. Agamben argumenta que estas medidas pueden tener consecuencias duraderas en la vida política y social. En esta línea de pensamiento, podríamos afirmar que la pandemia habría llevado a la declaración de un estado de excepción, en el cual se suspenden ciertas garantías y derechos civiles para hacer frente a la crisis. En este contexto, el control fronterizo se convierte en un mecanismo para la limitación de la movilidad y la restricción de la libertad individual, con el objetivo de proteger la salud pública. Además, también podría afirmarse que el control fronterizo se convierte en un mecanismo para la construcción de la identidad nacional. La pandemia habría llevado a un aumento del nacionalismo y el proteccionismo, con el objetivo de proteger a los ciudadanos de un territorio determinado. En este contexto, el control fronterizo se convertiría en un mecanismo para la delimitación de lo que se considera "nosotros" y "ellos".

En esta nueva realidad post-pandémica, la Guardia Europea de Fronteras y Costas (también conocida como Frontex), en colaboración con el Centro de Competencia de Análisis y Minería de Texto (TMA-CC) ha desarrollado una herramienta de minería de datos que le ha permitido identificar tecnologías emergentes o nuevas aplicaciones emergentes de tecnologías ya conocidas en el campo específico de la gestión de fronteras[4]. Esta estrategia

---

[2] J. RANCIERE, *Le maître ignorant. Cinq leçons sur l´émancipation intellectuelle*, Paris, 1987.

[3] G. AGAMBIEN, *Etat d´exception*, Paris, 2003.

[4] Comisión Europea, JRC Technical Report, *Weak Signals in Border Management and Surveillance Technologies,* 2022. Frontex ha realizado la siguiente clasificación: (1) tecnologías de primera prioridad: satélites de gran altitud (posible aplicabilidad: vigilancia fronteriza), Blockchain (posible aplicación: controles fronterizos), internet de las cosas (posible aplicabilidad: vigilancia fronteriza), videovigilancia inteligente (posible aplicabilidad: vigilancia fronteriza), radar GNSS para vigilancia marítima (posible aplicabilidad: vigilancia fronteriza), rastreo por escaneo (posible aplicabilidad: vigilancia fronteriza), red de sensores submarinos (posible aplicabilidad: vigilancia fronteriza); (2) tecnologías de segunda prioridad: video sinopsis (posible aplicabilidad: vigilancia fronteriza), vehículos no tripulados (posible aplicabilidad: vigilancia fronteriza), vigilancia algorítmica (sólo para datos no personales), (posible aplicabilidad: controles fronterizos, vigilancia fronteriza), microdrones (posible aplicabilidad: vigilancia fronteriza).

basada en la automatización y la digitalización de los procesos de control fronterizo plantean desafíos éticos y políticos importantes, ya que pueden aumentar la eficacia del control, pero también pueden aumentar la discriminación y la exclusión[5]. Según Balibar, la implementación de tecnologías avanzadas en el control fronterizo puede llevar a un aumento de la precisión y la eficacia en la detección de personas inmigrantes, pero también puede llevar a un aumento de la discriminación y la exclusión. La automatización y la digitalización pueden conducir a la creación de perfiles y estereotipos basados en la raza, la nacionalidad y otros factores, lo que puede llevar a un aumento de la discriminación y la exclusión de personas inmigrantes. Además, Balibar argumenta que la implementación de tecnologías avanzadas en el control fronterizo también plantea desafíos éticos y políticos en términos de privacidad y seguridad. La recolección y el almacenamiento de datos personales pueden violar los derechos y las libertades individuales y pueden poner en peligro la privacidad y la seguridad de las personas inmigrantes. Para poder entender mejor estos desafíos, planteamos un ejercicio de (de)construcción de categorías e integración de todas estas tecnologías emergentes al sistema actual de gestión y supervisión de las fronteras exteriores de la Unión Europea. Con este objetivo, las hemos clasificado en cuatro generaciones. La primera generación parte del estudio de las nuevas aplicaciones de aquellas tecnologías de vigilancia consideradas como tradicionales. La segunda generación abarca específicamente las tecnologías de vigilancia aérea y marítima. La tercera generación se centra en la cuestión de la seguridad cibernética. Y, en último lugar, la cuarta generación comprendería las denominadas tecnologías de vigilancia inteligentes.

2. *La primera generación: tecnologías de vigilancia tradicionales*

La primera categoría de tecnologías de vigilancia de fronteras exteriores de la Unión Europea se refiere a las tecnologías tradicionales utilizadas para detectar y rastrear la actividad en las fronteras. Estas tecnologías incluyen satélites de gran altitud, radares, una red de sensores submarinos y sistemas de videovigilancia. Desde hace décadas, estas tecnologías han sido utilizadas para monitorear las fronteras y detectar posibles amenazas, como el tráfico de drogas, el contrabando y el tráfico de personas. Estos sistemas también son útiles para detectar actividades ilegales, como la pesca ilegal o la deforestación. A pesar de que estas tecnologías son consideradas "tradicionales", aún tienen un papel importante en la vigilancia de las fronteras exteriores de la Unión Europea. A menudo, son utilizadas en combinación con tecnologías más avanzadas, como drones y tecnologías cibernéticas, para proporcionar una visión más completa y precisa de la actividad en las fronteras. La primera generación de tecnologías de vigilancia de fronteras se caracteriza por su capacidad para cubrir grandes áreas y su fiabilidad, especialmente en condiciones climáticas adversas, lo que la hace esencial para la seguridad de la Unión Europea.

2.1 *Satélites de gran altitud para vigilar fronteras*

Los pseudosatélites de gran altitud son aeronaves no tripuladas que operan en la estratosfera a altitudes de aproximadamente veinte kilómetros o más. Estos satélites pueden volar muy por encima de la altitud que alcanzan otros aparatos convencionales y adoptan la

[5] E. BALIBAR, *Frontières de la Démocratie*, Paris, 2013.

forma de aeronaves, aviones o globos y ofrecen una cobertura continua de día y de noche del territorio perimetrado. La formación de equipos de vehículos no tripulados se ha convertido en una pieza esencial en misiones científicas, en misiones de rescate en desastres naturales y se utilizan también como una herramienta o arma de guerra (*warfare*)[6]. En el campo de la investigación científica, estos satélites se utilizan para estudiar la Tierra y el espacio exterior, proporcionando información valiosa sobre el clima, el medio ambiente y otros fenómenos naturales. En situaciones de desastres naturales, los satélites de gran altitud son esenciales para el rescate y la recuperación. Proporcionan imágenes de satélite de alta resolución de las áreas afectadas, lo que permite a los equipos de rescate identificar las zonas más críticas y planificar su respuesta. También se utilizan para la comunicación en áreas remotas donde los sistemas de telecomunicaciones tradicionales han sido dañados. En la guerra moderna, los satélites de gran altitud juegan un papel clave en la inteligencia militar y la planificación de operaciones. Proporcionan imágenes de satélite de alta resolución de las áreas objetivo, lo que permite a los ejércitos planificar ataques precisos y estratégicos. Además, estos satélites también se utilizan para la detección de misiles, lo que ayuda a los ejércitos a detectar e interceptar amenazas aéreas. En términos de comunicaciones, los satélites de gran altitud son esenciales para mantener la comunicación entre unidades militares en campo de batalla, permitiendo la coordinación y el intercambio de información en tiempo real. También son utilizados para la navegación, facilitando a los ejércitos a navegar por terrenos difíciles y a planificar rutas de ataque[7].

En lo referente a la vigilancia y control de fronteras, los satélites de gran altitud presentan toda una serie de aplicaciones específicas: (1) observación del territorio (pueden generar imágenes en tiempo real de alta resolución de las fronteras, lo que permite a las autoridades detectar y monitorear actividades sospechosas. Estas imágenes pueden ser utilizadas para detectar la presencia de personas, vehículos y embarcaciones que se mueven a través de la frontera); (2) detección de radares (facilita la labor de las autoridades de detectar y monitorear la actividad de los radares, lo que puede proporcionar información valiosa sobre el tráfico aéreo y el tráfico marítimo cerca de la frontera); (3) comunicaciones (es especialmente importante en áreas remotas donde las comunicaciones terrestres pueden ser interrumpidas); (4) monitoreo de las condiciones climáticas (es de gran utilidad a la hora de tomar decisiones informadas sobre el despliegue de personal y los recursos en áreas donde se espera que se produzcan condiciones climáticas desfavorables por parte de las autoridades). Además, estos satélites suponen una alternativa resistente y flexible que puede complementar la actividad de satélites tradicionales y drones. Son particularmente útiles para facilitar comunicaciones en áreas remotas que carecen de infraestructuras o en Alta Mar.

---

[6] K. K. NAIR, *Small satellites and sustainable Development: solutions in international space law*, Montreal, 2019. Este libro analiza el derecho internacional del espacio y el derecho espacial en relación con el uso de satélites. Aborda temas como la propiedad y el control de los satélites, la responsabilidad por daños causados por satélites y el derecho a la exploración y el uso pacífico del espacio.

[7] Un ejemplo de cómo los satélites de gran altitud han sido utilizados en la guerra moderna es en el conflicto en Irak (2003). Los satélites de gran altitud fueron utilizados para proporcionar imágenes de satélite de alta resolución de las áreas objetivo, lo que permitió a los ejércitos estadounidenses y británicos planificar ataques precisos y estratégicos. También fueron utilizados para la detección de misiles, lo que ayudó a los ejércitos a interceptar amenazas aéreas. Además, los satélites de gran altitud también fueron esenciales para mantener la comunicación entre unidades militares en campo de batalla. Desde entonces, los satélites de gran altitud han sido utilizados en una variedad de guerras y operaciones militares en todo el mundo, como la guerra en Afganistán, la intervención en Libia en 2011, el conflicto en Siria, la operación "Chamma" en Irak y Siria, entre otros.

2.2 *Radares (Sistema Global de Navegación por Satélites)*

Los radares (Sistema Global de Navegación por Satélites, o GNSS en inglés) son sistemas de posicionamiento que utilizan señales de satélites para determinar la posición, velocidad y tiempo de un dispositivo receptor en la Tierra. El sistema más conocido es el GPS (Sistema de Posicionamiento Global) de la NASA, pero también existen otros sistemas GNSS como el GLONASS de Rusia, Galileo de la Unión Europea y BeiDou de China[8]. Estos sistemas permiten a los usuarios obtener información precisa sobre su posición en tiempo real. Una de las aplicaciones más comunes es la navegación, ya que los dispositivos GPS se utilizan ampliamente en automóviles, teléfonos móviles y otros dispositivos móviles para brindar información precisa sobre la posición y la ruta. Otra aplicación importante es en el campo de la agricultura, donde los sistemas GNSS son usados para guiar tractores y otros equipos agrícolas con precisión, aportando una mayor eficiencia en el uso de los recursos y una mejor gestión de la tierra. En la construcción, los sistemas GNSS tienen la función de guiar la excavación y la construcción de estructuras, obteniendo una mayor precisión en las mediciones y una mejor planificación del proyecto. En la logística, éstos se utilizan para rastrear la ubicación de camiones y barcos, lo que permite a las empresas una mejor planificación de la logística y una mayor eficiencia en la entrega de bienes. En la navegación marítima, los citados sistemas GNSS sirven para guiar los barcos y los buques con precisión, mejorando la seguridad en el mar y también la planificación de las rutas. En la aviación también encuentran aplicación guiando los aviones con precisión, obteniendo, como se ha señalado para la navegación marítima, una mejor seguridad en el aire y una mejor planificación de las rutas.

Los sistemas de navegación por satélite, como el GPS, juegan un rol importante en el ámbito de la supervisión y control de fronteras. Estos sistemas pueden ser utilizados para monitorear la posición de los vehículos y los barcos en tiempo real, lo que permite a las autoridades detectar y prevenir la entrada ilegal de personas y bienes a través de las fronteras. Asimismo, los sistemas de navegación por satélite también pueden ser utilizados para rastrear y monitorear la posición de los aviones no tripulados (drones) que tienen la potencialidad de violar la frontera. Otra aplicación importante es el monitoreo de la posición de los buques en tiempo real en la costa y en el mar, ya que esto permite a las autoridades detectar y prevenir actividades ilegales, como el tráfico de drogas o personas. Además, los sistemas de navegación por satélite también pueden ser útiles en la mejora de la seguridad en la frontera

[8] La Convención de las Naciones Unidas sobre el Derecho del Mar de 1982 (UNCLOS o CONVEMAR) establece en su artículo 87 que los Estados tienen derecho a establecer sistemas de navegación por satélite y a utilizarlos libremente. La Organización de Aviación Civil Internacional (OACI) ha adoptado normas y procedimientos para garantizar la seguridad y la eficiencia en el uso de los sistemas de navegación por satélite en la aviación. La Unión Internacional de Telecomunicaciones (UIT) es responsable de coordinar la asignación de frecuencias para los sistemas de navegación por satélite a nivel internacional, asegurando así que no haya interferencia entre los diferentes sistemas. La Organización Europea para la Exploración y el Uso del Espacio (ESA) y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) también han adoptado normas y acuerdos para regular el uso de los sistemas de navegación por satélite. En conjunto, estas normas y acuerdos internacionales buscan garantizar el uso libre y seguro de los sistemas de navegación por satélite a nivel mundial, y promover la cooperación entre los estados y las organizaciones internacionales en este ámbito.

mediante la creación de una red de sensores que detecten y alerten sobre la presencia de personas y vehículos en áreas no autorizadas.

En relación con la detección de objetivos, el uso de estos sistemas ofrece dos ventajas importantes. Primero, su capacidad para adaptarse a cualquier clima. Los sistemas GNSS-R utilizan las señales reflejadas por los satélites de navegación para detectar objetivos en la Tierra, lo que les permite operar en cualquier condición climática, incluyendo nubes densas, lluvia o nieve, haciéndolos ideales para las áreas remotas o de difícil acceso. Segundo, los sistemas GNSS-R ofrecen una cobertura mundial. Los satélites de navegación se encuentran en órbita alrededor del globo terráqueo, facilitando a los sistemas GNSS-R detectar objetivos en cualquier lugar del mundo. Esto es especialmente valioso en funciones como la vigilancia de fronteras, la seguridad marítima y la detección de desastres naturales, dando a las autoridades una visión global de la situación en tiempo real.

El seguimiento durante la exploración (TWS, por sus siglas en inglés) es un modo de funcionamiento del radar en el que este asigna parte de su potencia al seguimiento de objetivos mientras que, al mismo tiempo, tiene capacidad suficiente para escanear y procesar otros objetivos. En este tipo de operación, el radar puede monitorear varios objetivos simultáneamente y asignar recursos dinámicamente para seguir de manera eficiente a los objetivos más importantes. A diferencia del modo de seguimiento directo, en el que el radar dirige toda su potencia únicamente a rastrear los objetivos fijados, el TWS permite al radar mantener una mayor flexibilidad y adaptabilidad en su operación, ya que puede cambiar de objetivo rápidamente en caso de ser necesario. Esto es especialmente valioso en aplicaciones como la vigilancia aérea, la defensa antiaérea y la defensa naval, posibilitando que el radar detecte y siga varios objetivos simultáneamente, mejorando su eficiencia y eficacia en su tarea.

2.3 *Red de sensores submarinos*

Una red de sensores submarinos es un conjunto de dispositivos tecnológicos instalados en el fondo del mar o en la columna de agua para recopilar información sobre el medio marino. Estos sensores pueden ser de diversos tipos, dependiendo de la información que se desea recopilar[9]. Por ejemplo, se pueden utilizar sensores de temperatura para medir la temperatura del agua en diferentes profundidades, sensores de salinidad para medir la concentración de sales en el agua, sensores de corriente para medir la velocidad y dirección de las corrientes marinas, sensores de oxígeno para medir la concentración de oxígeno disuelto en el agua, y sensores de nutrientes para medir la presencia de nutrientes en el agua, como nitrógeno y fósforo. Estos sensores se comunican entre sí y con un sistema de recolección de datos en la superficie a través de una red de comunicaciones submarinas. El sistema de recolección de datos en la superficie se encarga de recibir y procesar los datos

[9] La Convención de las Naciones Unidas sobre el Derecho del Mar establece los principios y las reglas para la delimitación de las fronteras marítimas y establece las reglas para la explotación de los recursos naturales en las aguas internacionales. Esta convención también establece las reglas para la investigación científica en las aguas internacionales y establece que los Estados tienen la responsabilidad de garantizar que cualquier actividad en las aguas internacionales no dañe los intereses de otros Estados. Además, existen varios tratados y convenios internacionales específicos que regulan la instalación y uso de redes de sensores submarinos. Por ejemplo, el Protocolo de 1996 sobre las minas marítimas de la Convención de las Naciones Unidas sobre el Derecho del Mar prohíbe la colocación de minas marítimas en las aguas internacionales, y establece las reglas para la identificación y eliminación de minas marítimas existentes. Otro ejemplo es la Convención de la UNESCO sobre la Protección del Patrimonio Submarino que establece las reglas para la investigación y explotación de los sitios submarinos con valor cultural o arqueológico.

recolectados por los sensores, y puede incluir una estación base en tierra o un buque de investigación. Los datos recopilados pueden ser transmitidos en tiempo real a un centro de control en la tierra para su procesamiento y análisis.

Las redes de sensores submarinos se utilizan en una variedad de aplicaciones, como la investigación científica -para estudiar los ecosistemas marinos y los cambios en el clima marino-, la exploración de recursos naturales -para localizar y evaluar los recursos minerales, petroleros y de gas natural en el fondo del mar-, la vigilancia marítima -para monitorear la actividad humana en el mar, como la pesca ilegal y la contaminación- y la gestión del medio ambiente -para monitorear el estado de conservación de los ecosistemas marinos y para detectar y medir la contaminación del agua-. La gestión y control de fronteras es una aplicación específica de las redes de sensores submarinos. Un uso de estas redes puede ser el monitoreo la actividad humana en las aguas fronterizas, como el tráfico marítimo, la pesca ilegal y el contrabando[10]. Los sensores submarinos pueden detectar y seguir barcos y submarinos, por lo que servirán en las tareas de identificación y rastreo de las embarcaciones sospechosas. Además, las redes de sensores submarinos serían útiles para detectar y monitorear la presencia de minas marítimas y otros artefactos peligrosos en las aguas fronterizas. Esto puede ayudar a garantizar la seguridad de la navegación y a prevenir accidentes marítimos.

2.4 *Sistemas de videovigilancia*

La video sinopsis es una técnica de procesamiento automático de videos que tiene como objetivo generar un resumen de las principales escenas y eventos de un video. Esto se logra mediante el uso de algoritmos de procesamiento de lenguaje natural y aprendizaje automático, que analizan el contenido del video y extraen información relevante para generar una descripción breve del mismo[11]. La video sinopsis puede ser útil en una variedad de aplicaciones, como la indexación de videos para la búsqueda, la clasificación de contenido y la recomendación de videos. En el caso de la indexación de videos, serviría a los usuarios a encontrar rápidamente videos relacionados con un tema específico. En la clasificación de contenido, podría ser de ayuda en la determinación de si un video es apropiado para una audiencia específica. En el supuesto de la recomendación de videos, una video sinopsis puede ayudar a los usuarios a descubrir nuevos videos que sean interesantes para ellos. Para generar una video sinopsis, los algoritmos primero analizan el contenido del video para extraer información relevante, como personajes, escenas, diálogos y eventos clave. Luego, utilizan esta información para generar un resumen del video que incluya las escenas y eventos más importantes. Esto se logra mediante el uso de técnicas de procesamiento de lenguaje natural, como el análisis semántico y la detección de eventos. La video sinopsis también puede incluir elementos visuales, como imágenes de las escenas clave o capturas de pantalla, para proporcionar una representación visual del contenido del video. Además, los algoritmos pueden usar información adicional, como subtítulos y metadatos, para mejorar la precisión de la sinopsis generada.

[10] L. OTTO, *Global Challenges in Maritime Security: An Introduction. Advanced Sciences and Technologies for Security Applications*, Cham, 2020.
[11] M. D. FAM, *Camera Power: Proof, Policing, Privacy, and Audiovisual Big Data*, Cambridge, 2019.

Esta técnica puede tener varias aplicaciones específicas en la vigilancia y control de fronteras[12]. Entre éstas, podemos destacar: (1) detección de intrusos (los algoritmos de video sinopsis se podría usar en el análisis continuo de los videos capturados por cámaras de vigilancia en fronteras para detectar la presencia de personas no autorizadas); (2) seguimiento de vehículos (en particular, el movimiento de vehículos a lo largo de las fronteras, facilitando que se detecten actividades sospechosas); (3) identificación de objetos (los algoritmos de video se pueden entrenar para detectar y reconocer automáticamente objetos específicos, como armas o paquetes sospechosos, identificando, en consecuencia, posibles amenazas); (4) análisis de patrones (en concreto, patrones en el comportamiento de las personas y los vehículos a lo largo de las fronteras, lo que puede ayudar a identificar tendencias y patrones sospechosos(; (5) identificación de rutas utilizadas por traficantes (con ello, se detectarían patrones en su comportamiento, y, además, las rutas de tráfico de drogas o personas).

3. *La segunda generación: tecnologías de vigilancia aérea y submarina*

La segunda categoría de tecnologías de vigilancia de fronteras exteriores de la Unión Europea se refiere a las tecnologías de vigilancia aérea y submarina. Estas tecnologías incluyen vehículos aéreos no tripulados (UAV, por sus siglas en inglés), microdrones y rastreo por escaneo. Han sido desarrolladas para proporcionar una vigilancia más detallada y precisa en el aire y en el mar. Piénsese que los UAVs y los microdrones son capaces de volar a baja altitud y tienen cámaras de alta resolución, permitiendo una vigilancia más cercana y detallada de las actividades en las fronteras. El rastreo por escaneo, por otro lado, ofrece una detección precisa de objetos en el mar y su posición. Estas tecnologías son especialmente útiles para detectar actividades sospechosas en zonas remotas o difíciles de acceder. Por ejemplo, los UAVs y los microdrones podrían vigilar las costas y las zonas marítimas, mientras que el rastreo por escaneo es especialmente útil para detectar la pesca ilegal o el tráfico de drogas en el mar. La segunda generación de tecnologías de vigilancia de fronteras se caracteriza por su capacidad para cubrir áreas específicas y su precisión en la detección de objetos, lo que la hace esencial para la seguridad de la Unión Europea, especialmente en zonas costeras y marítimas.

3.1 *Vehículos no tripulados*

[12] En el marco del Derecho de la Unión Europea, esta actividad estaría sujeta a la regulación establecida en: (1) el Reglamento General de Protección de Datos (RGPD) que establece las normas para la protección de datos personales en la UE y podría limitar la capacidad de los Estados miembros de la UE para recopilar y utilizar información a través de la video sinopsis, especialmente si la información recopilada es considerada información personal; (2) la Directiva de protección de datos para las fuerzas de seguridad y el orden público que establece una normativa específica para la protección de datos personales en el ámbito de las fuerzas de seguridad y el orden público, incluyendo la recopilación de datos de video y (3) la Carta de los Derechos Fundamentales de la Unión Europea que identifica los derechos fundamentales de los ciudadanos de la UE, incluyendo el derecho a la privacidad y el derecho a la protección de datos personales, y podría limitar la capacidad de los Estados miembros de la UE para recopilar y utilizar información a través de la video sinopsis.

Los vehículos no tripulados (UAVs)[13], también conocidos como drones, son aeronaves que no tienen un piloto a bordo y se controlan a distancia o siguen una ruta predeterminada. Estos vehículos encuentran aplicción en una variedad de aplicaciones, desde la vigilancia y el monitoreo ambiental hasta la agricultura, la fotografía aérea y la entrega de paquetes. Los vehículos no tripulados pueden ser divididos en dos categorías principales: los vehículos no tripulados de uso civil y los vehículos no tripulados militares. Los primeros -de uso civil- se utilizan principalmente para fines comerciales, científicos y de entretenimiento. Por ejemplo, en la agricultura tienen como función monitorear los cultivos y detectar plagas; en la construcción, inspeccionar edificios e infraestructuras; y en la fotografía y el cine, tomar imágenes aéreas. Los vehículos no tripulados militares -los segundos-, por otro lado, son usados principalmente para fines de inteligencia, vigilancia y ataque. Hay una variedad de tipos de vehículos no tripulados, desde pequeños y ligeros dispositivos de mano hasta grandes y complejos sistemas que pueden llevar cargas pesadas. Los vehículos no tripulados más pequeños son generalmente propulsados por baterías y se controlan con un mando a distancia. Los vehículos no tripulados más grandes, por otro lado, suelen tener motores de combustión y pueden volar durante períodos prolongados. Algunos vehículos no tripulados también están equipados con cámaras de alta resolución, sensores y otros equipos para recopilar datos.

A medida que la tecnología de los UAVs ha avanzado, se han desarrollado nuevos usos para estos vehículos[14]. En relación con la vigilancia y el control de fronteras, algunas de las funciones más comunes incluyen: (1) monitoreo de la frontera de un país, detectando y rastreando actividad sospechosa, como el tráfico de drogas o personas; (2) búsqueda y rescate de personas que se han perdido en áreas remotas o de difícil acceso; (3) patrullaje de frontera, detectando y reportando actividad sospechosa; (4) inteligencia (recopilación información sobre el terreno, el clima y la vegetación, ayudando a los oficiales fronterizos a planificar mejor sus operaciones); (5) identificación -pueden ser equipados con cámaras de alta resolución y tecnología de reconocimiento de rostros y placas de matrícula, permitiendo a los oficiales fronterizos a identificar y detener a personas sospechosas; (6) control de incendios (esto es, monitoreo y control de incendios forestales, de forma que los bomberos puedan ejecutar una mejor planificación de sus operaciones y proteger mejor a las comunidades cercanas); (7) seguridad (detectando y neutralizando dispositivos explosivos, escoltando convoyes y protegiendo instalaciones críticas).

[13] El derecho internacional regula los vehículos no tripulados (UAVs) a través de varias convenciones y acuerdos internacionales. La Convención de las Naciones Unidas sobre el Derecho del Aire, que fue adoptada en 1944, establece las normas básicas para la regulación de los UAVs y su uso en el espacio aéreo. También establece las obligaciones de los Estados en relación con la seguridad de la navegación aérea y la protección de los derechos de los pasajeros. La Convención de Vuelo Seguro de 1944 establece las normas para la seguridad en el vuelo, incluyendo las normas para la construcción, mantenimiento y operación de los UAVs. Esta convención también establece las obligaciones de los Estados en relación con la investigación de accidentes de avión y la prevención de colisiones. Además de estas convenciones básicas, también existen varios acuerdos internacionales específicos que regulan el uso de los UAVs. Por ejemplo, el Protocolo de 1944 sobre las Señales Internacionales de Aeronaves establece las normas para la señalización de los UAVs y su identificación. El derecho internacional también regula el uso de los UAVs en operaciones militares y de seguridad. La Convención de las Naciones Unidas sobre el Derecho del Aire y la Convención de Vuelo Seguro de 1944 se aplican a los UAVs utilizados en operaciones militares y de seguridad, y establecen las obligaciones de los Estados en relación con la seguridad del vuelo y la protección de los derechos de los pasajeros.

[14] A. ZAVRSNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Cham, 2016.

Asimismo, el uso de esta tipología de vehículos para la supervisión y control de las fronteras de la Unión Europea puede plantear varios problemas relacionados con el reconocimiento y protección de los derechos de las personas migrantes: (1) protección de la privacidad (si se equipan con cámaras de alta resolución y tecnología de reconocimiento de rostros, las autoridades recopilarían información sobre las personas que se encuentran en la frontera, trayendo consigo preocupaciones sobre la privacidad y el derecho al debido proceso); (2) protección de determinados derechos humanos (podría conducir a supuestos de tortura o trato inhumano o degradante); y (3) protección de los derechos de los refugiados (puede aumentar las dificultades para que los refugiados y las personas que buscan asilo, obstaculizando su acceso a procedimientos de asilo justos y eficaces).

3.2 *Microdrones*

Los microdrones son pequeños dispositivos voladores controlados a distancia que se están utilizando cada vez más en una variedad de aplicaciones. A diferencia de los drones tradicionales, los microdrones son característicos por su tamaño compacto, lo que les permite maniobrar en espacios confinados y lugares de difícil acceso. También son conocidos por su bajo ruido y su capacidad para volar a bajas altitudes, haciéndolos ideales para funcionalidades discretas. Estos drones encuentran aplicación en una variedad de industrias, como la agricultura, la construcción, la minería y la vigilancia de la fauna. Comenzando por la agricultura, servirían para monitorear los campos, detectar plagas y enfermedades en las cosechas, así como planificar el riego. En la construcción, para inspeccionar estructuras y para planificar el trabajo en altura. Pasando a la minería, para explorar las minas y para monitorear las operaciones. Con respecto a la vigilancia de la fauna, para monitorear los animales en su hábitat natural y para estudiar sus patrones de comportamiento. En cuanto a su tecnología, los microdrones actuales están equipados con una variedad de sensores, como cámaras, termómetros, sensores de humedad, GPS y sistemas de navegación. Estos sensores les permiten recolectar una gran cantidad de datos, que luego pueden ser analizados para obtener información valiosa. Además, muchos microdrones están equipados con sistemas de inteligencia artificial, permitiéndoles volar de forma autónoma y tomar decisiones sin intervención humana.

La vigilancia y control de fronteras es un desafío importante para muchos países, apareciendo los microdrones como una herramienta valiosa para abordar este problema. Estos dispositivos voladores son idóneos para este tipo de aplicaciones debido a su capacidad para maniobrar en lugares de difícil acceso, su bajo ruido y su capacidad para volar a bajas altitudes. Uno de sus usos más comunes en la vigilancia y control de fronteras es la detección y rastreo de inmigrantes ilegales. Estos drones pueden ser equipados con cámaras de alta resolución y sensores infrarrojos para detectar a las personas que intentan cruzar la frontera de forma ilegal, y también pueden ser equipados con GPS para rastrear su movimiento. Además, los microdrones pueden ser utilizados para monitorear el tráfico de drogas y armas, ya que los citados dispositivos pueden detectar los vehículos y embarcaciones que transportan estos productos ilegales. Otra aplicación importante de los microdrones en la vigilancia y control de fronteras es la realización de inspecciones de fronteras; en particular, zonas de frontera terrestres y marítimas, para detectar y rastrear a los contrabandistas, y para apoyar a las fuerzas de seguridad en la lucha contra el terrorismo. Además, otro uso sería el monitoreo de la actividad en las zonas de frontera, para detectar cualquier actividad sospechosa, y para tomar medidas preventivas antes de que se produzcan incidentes.

3.3 *Rastreo por escaneo*

La tecnología de rastreo por escaneo sirve para rastrear y monitorear a personas, vehículos y cargamentos a medida que cruzan fronteras, puertos y aeropuertos[15]. Esta tecnología incluye el uso de escáneres de rayos X, detectores de metales, termografía y reconocimiento facial para identificar objetos y personas sospechosos. Uno de los principales beneficios del rastreo por escaneo es que permite a las autoridades detectar cualquier aspecto que pueda ser considerado una amenaza para la seguridad nacional, como armas, drogas o explosivos. Lo anterior ayuda a prevenir atentados terroristas y aumenta la seguridad en los puntos de entrada y salida del país. Además, esta tecnología de rastreo por escaneo también es útil para detectar el tráfico de personas y el contrabando de bienes. Efectivamente, los escáneres de rayos X y los detectores de metales pueden detectar objetos ocultos en las ropas o en los vehículos, mientras que el reconocimiento facial puede ayudar a identificar a individuos sospechosos. Sin embargo, también existen algunas desventajas en el uso de la tecnología de rastreo por escaneo. Por ejemplo, el uso de escáneres de rayos X puede exponer a las personas a niveles peligrosamente altos de radiación, mientras que el uso excesivo de tecnología de reconocimiento facial puede llevar a problemas de privacidad y discriminación. Además, la tecnología de rastreo por escaneo puede ser costosa y requiere una gran cantidad de personal capacitado para operar y mantener los equipos.

Los avances recientes en el procesamiento de señales han permitido el desarrollo de sistemas de videovigilancia inteligentes, especialmente aquellos que pueden adaptarse de manera flexible a la tasa de recopilación de datos de video. Estos sistemas utilizan tecnologías avanzadas de procesamiento de señales para analizar las imágenes capturadas y detectar indicadores de incidentes, como actividades sospechosas o personas inusuales en una zona determinada. Cuando se detecta un indicador de incidente, la tasa de recopilación de datos aumenta automáticamente para proporcionar información más detallada para elaborar un análisis más preciso y creíble. Esto permite a las autoridades responder rápidamente a cualquier amenaza potencial y tomar medidas para evitar un incidente. Además, el desarrollo de análisis de video impulsado por la Inteligencia Artificial contribuye a ir más allá de la seguridad y la vigilancia básicas hacia operaciones fortalecidas. Estas tecnologías utilizan redes neuronales de aprendizaje profundo para analizar videos y "aprender" a identificar objetos, personas, actividades, emociones, en tiempo real o a posteriori. Así, se estaría ante una monitorización más precisa y una detección temprana de amenazas, fundamental en la prevención de incidentes y la garantía de la seguridad de las fronteras.

[15] Uno de los principales tratados internacionales que podría aplicarse en este ámbito es la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que establece las obligaciones de los Estados para prevenir, investigar y sancionar la delincuencia organizada transnacional, incluyendo la trata de personas y el tráfico de drogas. Además, la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas también establece obligaciones para los Estados para prevenir y combatir el tráfico de drogas a través de sus fronteras. En cuanto a la privacidad, la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos establecen la protección de la privacidad y el derecho a la protección de datos personales. En este sentido, el uso de la tecnología de reconocimiento facial y el monitoreo de personas debe ser regulado para asegurar que no se violen estos derechos.

4. *La tercera generación: tecnología de seguridad cibernética*

La tercera categoría de tecnologías de vigilancia de fronteras exteriores de la Unión Europea se refiere a la tecnología de seguridad cibernética. Este grupo se focaliza en el uso del blockchain para el control de fronteras, que es una tecnología descentralizada que permite registrar transacciones en un libro de contabilidad digital, conocido como cadena de bloques, de forma segura y transparente. Al utilizar blockchain para el control de fronteras, se puede garantizar que la información relacionada con la vigilancia de las fronteras sea precisa, auténtica y segura. Además, permite una mayor transparencia en la gestión de la información, ya que todas las transacciones están registradas en el libro de contabilidad digital y son visibles a todos los participantes en la red. Esto también ayuda a reducir los errores humanos y a mejorar la eficiencia en la gestión de la información. La tercera generación de tecnologías de vigilancia de fronteras se caracteriza por su capacidad para proporcionar una mayor seguridad y transparencia en la gestión de la información relacionada con la vigilancia de las fronteras, convirtiéndose en esencial para garantizar la seguridad y estabilidad de la Unión Europea.

4.1 *Blockchain para el control de las fronteras*

La tecnología blockchain se basa en la creación de una cadena de bloques, un registro digital descentralizado que almacena información de forma segura e inmutable[16]. Cada bloque contiene una serie de transacciones y una referencia al bloque anterior, creando una cadena que es difícil de alterar. Esto permite a las personas confiar en los registros sin tener que depender de una autoridad central. Una de sus características más importantes es su seguridad. Los bloques son cifrados y protegidos mediante técnicas de criptografía, lo que significa que sólo las personas autorizadas pueden acceder a la información. Además, la descentralización significa que no hay un punto único de fallo, reduciendo el riesgo de ataques cibernéticos. Otra ventaja de la tecnología blockchain es la transparencia. Cualquier persona puede ver las transacciones registradas en la cadena de bloques, aumentando la transparencia en las operaciones financieras y comerciales. Además, las smart contracts, o contratos inteligentes, permiten automatizar procesos y acuerdos comerciales mediante la programación de reglas y condiciones en el código del contrato[17].

La tecnología blockchain tiene un gran potencial para mejorar la gestión y control de fronteras, puesto que posibilita el registro y la verificación de la información de los viajeros de manera segura y transparente. Algunos ejemplos concretos de cómo se podría utilizar en este ámbito incluyen: (1) registrar y verificar la información de pasaportes y visados de los viajeros, reduciendo el riesgo de fraudes y mejorando la eficiencia en los procesos de fronteras. Por ejemplo, se podría utilizar un sistema basado en blockchain que almacena la

[16] Actualmente, el derecho internacional no tiene un marco regulador específico para la tecnología blockchain, por lo que se aplican las regulaciones existentes en áreas como el cumplimiento de la ley, la privacidad, la prevención del blanqueo de capitales y la protección de los derechos de propiedad intelectual. Sin embargo, las regulaciones varían entre países. Por ejemplo, en algunos países como Japón y Malta, se han adoptado regulaciones específicas para fomentar el uso de la tecnología blockchain en la industria financiera y de seguros. Mientras tanto, en otros países como China y Rusia, las regulaciones son más restrictivas y limitan el uso de criptomonedas y las inversiones en proyectos de blockchain. Es importante mencionar que la regulación de esta materia está en constante evolución, y se espera que en el futuro se establezcan marcos regulatorios específicos a nivel internacional para regular el uso de la tecnología blockchain.

[17] S. GRUNDMANN, *European contract law in the digital age*, Cambridge, 2018.

información de los pasaportes y visados de los viajeros, y que permite a las autoridades fronterizas verificar la autenticidad de esta información en tiempo real; (2) uso de contratos inteligentes para automatizar la verificación de cumplimiento de los requisitos de inmigración y para la gestión de los permisos de trabajo. Por ejemplo, piénsese en un contrato inteligente que verifique automáticamente si un viajero cumple con los requisitos de inmigración antes de permitirle cruzar la frontera; (3) combinar enfoques biométricos novedosos, identidad digital descentralizada y entorno de control de fronteras. Por ejemplo, se podría utilizar un sistema basado en blockchain que almacena la información biométrica de los viajeros, como huellas dactilares o reconocimiento facial, y que permite a las autoridades fronterizas verificar la identidad de los viajeros de manera segura y transparente. Además, la combinación de tecnologías blockchain con otras tecnologías emergentes, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y la criptografía, permite aprovechar las ventajas de estas tecnologías para mejorar aún más la gestión y control de fronteras. Por ejemplo, se podría utilizar dispositivos IoT conectados a la red blockchain para registrar y verificar la información de los viajeros en tiempo real, o utilizar sistemas de reconocimiento facial basados en IA para verificar la identidad de los viajeros de manera automatizada. También se podría utilizar la criptografía para garantizar la confidencialidad y la seguridad de la información transmitida entre los dispositivos IoT y la red blockchain, ayudando a proteger la privacidad de los viajeros.

5. *La cuarta generación: tecnologías de vigilancia inteligentes*

La cuarta categoría de tecnologías de vigilancia de fronteras exteriores de la Unión Europea se refiere a las tecnologías de vigilancia inteligentes. Estas tecnologías incluyen el internet de las cosas (IoT) y el control de fronteras con algoritmos de aprendizaje automático. El IoT se refiere a la conexión de dispositivos y objetos a Internet, que conllevaría la recopilación y transmisión de datos en tiempo real. Al utilizar el IoT en la vigilancia de fronteras, se pueden recopilar y analizar datos en tiempo real sobre la actividad en las fronteras, detectando posibles amenazas con mayor rapidez y precisión. Por otro lado, el uso de algoritmos de aprendizaje automático en el control de fronteras posibilita una mayor eficiencia en la detección y respuesta a posibles amenazas. Estos algoritmos son capaces de aprender y mejorar continuamente a partir de los datos recopilados, y, en consecuencia, detectan cada vez más precisa patrones de actividad sospechosa. La cuarta generación de tecnologías de vigilancia de fronteras se caracteriza por su capacidad para proporcionar una mayor eficiencia en la detección y respuesta a posibles amenazas, y contribuyen a la mejora continua de la seguridad en las fronteras. De esta forma, se podría afirmar que es esencial para garantizar la seguridad y estabilidad de la Unión Europea.

5.1 *El internet de las cosas y el control de fronteras*

El Internet de las cosas (IoT) es una tecnología que permite conectar dispositivos y objetos cotidianos a internet mediante sensores y dispositivos de comunicación inalámbricos[18]. De esta forma, los dispositivos recolectan y comparten datos con otros

[18] El derecho internacional aún no ha desarrollado un marco normativo específico para regulación del Internet de las cosas (IoT). Sin embargo, existen algunos tratados internacionales y normas sectoriales que abordan aspectos relacionados con IoT, como la privacidad y la seguridad de la información. Por ejemplo, el Convenio

dispositivos y sistemas automatizando, así, procesos y tomando decisiones basadas en datos. La aplicación de IoT se ha extendido en una variedad de industrias, incluyendo la fabricación, el transporte, la energía y la salud. En la fabricación, los sensores IoT se utilizan para monitorear el rendimiento de maquinaria y detectar problemas antes de que ocurran. Con respecto al transporte, los vehículos conectados pueden comunicarse entre sí y con los semáforos para mejorar el flujo de tráfico. En en ámbito de la energía, los sensores IoT miden y monitorean el consumo de energía en edificios y hogares. En la salud, estos dispositivos monitorean la salud de las personas, tales como la presión arterial y la actividad física.

En cuanto a la supervisión y control de fronteras, la tecnología IoT puede ser utilizada para analizar y controlar el tráfico de personas y vehículos en las fronteras. Los sensores y cámaras IoT pueden ser instalados en puntos críticos para detectar y alertar a las autoridades de posibles violaciones de la frontera. Los vehículos y barcos también pueden ser equipados con dispositivos IoT para rastrear su posición y detectar cualquier actividad sospechosa. Además, los drones equipados con cámaras y sensores IoT podrían tener como utilidad la vigilancia de áreas remotas de la frontera. No obstante, esta tecnología también presenta algunos desafíos en relación con la supervisión y control de fronteras. Por ejemplo, en lo relativo a la privacidad y la seguridad de los datos recolectados. También se plantea si la información recogida puede ser usada de manera abusiva por parte de las autoridades para vigilar a las personas de manera invasiva. Además, el costo de implementar y mantener la tecnología IoT en las fronteras puede ser significativo. Al margen de estos desafíos, es innegable que la tecnología IoT tiene el potencial de mejorar la seguridad de las fronteras y ayudar a las autoridades a tomar decisiones informadas.

5.2 *Vigilancia algorítmica*

La tecnología de vigilancia algorítmica se refiere a la utilización de algoritmos de aprendizaje automático para analizar y procesar grandes cantidades de datos y detectar patrones o comportamientos sospechosos[19]. Una de las aplicaciones de estos algoritmos

de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad (ONU-CRPD) establece las obligaciones de las partes para garantizar el acceso a las tecnologías de la información y la comunicación, incluyendo IoT, para las personas con discapacidad. Además, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea establece regulaciones para la protección de los datos personales en relación con el procesamiento de datos por parte de las empresas y organizaciones, incluyendo las relacionadas con IoT. Otra normativa internacional aplicable sería la ISO/IEC 30141:2018 "Internet of Things (IoT) -- Security for consumer IoT services" que establece las normas de seguridad para los servicios de IoT destinados al consumidor. A medida que IoT continúe desarrollándose y expandiéndose, es probable que se desarrollen más regulaciones internacionales específicas para abordar los desafíos legales y de seguridad que surgen de la aplicación de esta tecnología.

[19] La Carta de Derechos Fundamentales de la Unión Europea y el Reglamento General de Protección de Datos (RGPD) establecen un marco para garantizar que la tecnología de vigilancia algorítmica se utilice de manera ética y respete los derechos humanos y las leyes en materia de privacidad. La Carta de Derechos Fundamentales de la Unión Europea establece varios derechos fundamentales que son relevantes para la vigilancia algorítmica, como el derecho a la privacidad (Artículo 7), el derecho a la protección de datos personales (Artículo 8), y el derecho a un juicio justo (Artículo 47). Estos derechos fundamentales deben ser considerados al desarrollar y utilizar tecnologías de vigilancia algorítmica. El RGPD, por su parte, establece requisitos para la protección de datos personales y regula cómo las empresas y las organizaciones pueden recolectar, almacenar y utilizar estos datos. En particular, el RGPD establece principios como la transparencia, la rendición de cuentas, y la privacidad por diseño, los cuales son importantes para garantizar que la tecnología de vigilancia algorítmica se utilice de manera ética y respete los derechos de privacidad de los ciudadanos. Por ejemplo, el RGPD requiere que las empresas y organizaciones informen a los individuos sobre cómo sus datos personales son recolectados

puede ser vigilar una amplia variedad de entornos, como ciudades, edificios públicos, redes de transporte, y fronteras. Esta tecnología se basa en la recolección de datos a través de diferentes dispositivos, como cámaras de vigilancia, sensores, teléfonos móviles, y redes sociales. Estos datos son analizados mediante algoritmos de aprendizaje automático que buscan patrones y comportamientos sospechosos. Por ejemplo, un algoritmo de vigilancia algorítmica puede ser utilizado para detectar personas que se encuentran en un área prohibida o para identificar comportamientos sospechosos en una multitud. La tecnología de vigilancia algorítmica también puede mejorar la eficacia de la seguridad y la respuesta en caso de emergencia. Por ejemplo, los algoritmos de vigilancia algorítmica pueden servir en tareas como detectar y analizar el tráfico vehicular, de forma que las autoridades de tránsito puedan reaccionar rápidamente en caso de accidentes o congestión del tráfico. También se puede pensar en otras tareas como detectar incendios y alertar a los bomberos, o para detectar y alertar sobre posibles actividades terroristas. Sin embargo, la tecnología de vigilancia algorítmica también ha generado preocupaciones en relación a la privacidad y el acceso no autorizado a la información personal. La recolección masiva de datos y la capacidad de analizar y rastrear a las personas pueden ser utilizadas para vigilar a individuos y grupos. Lo anterior podría conducir a la violación de toda una serie de derechos civiles, así como del derecho a la privacidad de los ciudadanos[20].

En cuanto a su aplicación específica a la supervisión y vigilancia de fronteras, la tecnología de vigilancia algorítmica encontraría un uso en la detección y en el análisis del tráfico fronterizo. En consecuencia, se facilita la labor de las autoridades de detectar y prevenir el tráfico de drogas, armas, y personas ilegalmente. También pueden ser utilizadas para detectar y analizar patrones de tráfico sospechosos, pudiendo las autoridades identificar y monitorear a individuos o grupos que podrían representar una amenaza para la seguridad nacional. Además, los algoritmos de vigilancia algorítmica pueden servir en el análisis y procesamiento de información recopilada a través de diferentes medios, como imágenes de satélite, drones, cámaras de vigilancia, y sensores, y, consecuentemente, se produciría una mejor detección y monitoreo de las actividades en las fronteras. Otro uso sería la mejora de la eficacia de los sistemas de identificación y autenticación, como los sistemas de reconocimiento facial y huella dactilar, mejorando el control de acceso a las fronteras. Esto puede ayudar a reducir el riesgo de entrada de personas no autorizadas y mejorar la seguridad nacional. Sin embargo, es importante tener en cuenta que la tecnología de vigilancia algorítmica también plantea desafíos éticos y legales, como se ha indicado con respecto a otras tecnologías, especialmente en lo que respecta a la privacidad y los derechos civiles. Es importante asegurar que los sistemas de vigilancia algorítmica sean transparentes y respeten los marcos normativos en materia de privacidad y derechos civiles. También es fundamental, a nuestro juicio, monitorear continuamente el rendimiento y la eficacia de estos sistemas con el objetivo de asegurar que no se estén violando los derechos de los ciudadanos y que se estén alcanzando los objetivos de seguridad deseados.

y utilizados, y obtengan el consentimiento explícito de los individuos para el tratamiento de sus datos personales. Además, las empresas y organizaciones deben garantizar la seguridad de los datos personales y notificar a las autoridades de protección de datos y a los individuos en caso de una violación de seguridad.

[20] J. GRANT-ALLEN, P. HUNN (eds.), *Smart legal contracts: computable law in theory and practice*, Oxford, 2013.

6. *Conclusiones*

La implementación de las cuatro generaciones de tecnologías de vigilancia de fronteras exteriores de la Unión Europea ha permitido una mayor precisión y eficiencia en la detección y respuesta a posibles amenazas, en la línea de pensamiento de James Hathaway[21]. No obstante, también ha generado críticas en relación a la privacidad y la protección de los derechos civiles de los ciudadanos, tal y como señala Milanovic[22]. Partiendo de la dicotomía clásica entre seguridad y disfrute de derechos de los ciudadanos, podemos señalar una serie de avances y peligros en relación con la implementación y desarrollo de todas y cada una de las cuatro generaciones de tecnologías de frontera:

La primera generación de tecnologías -donde se podrían encuadrar satélites de gran altitud, radares, una red de sensores submarinos y sistemas de videovigilancia- ha permitido detectar y rastrear la actividad en las fronteras desde hace décadas. Sin embargo, esta actividad de vigilancia de las fronteras puede poner en peligro el derecho a la privacidad de las personas, como trata en su obra Andrew Clapham[23]. Por ejemplo, el uso de dispositivos de videovigilancia en las fronteras puede plantear una serie de problemas en torno al registro de la actividad de las personas grabadas y su posible uso para fines no autorizados.

La segunda generación de tecnologías -donde se subsumirían vehículos aéreos no tripulados, microdrones y rastreo por escaneo- ha traído consigo una vigilancia más detallada y precisa en el aire y en el mar. Estas tecnologías son especialmente útiles para detectar actividades sospechosas en zonas remotas o difíciles de acceder. Sin embargo, el uso de drones y microdrones en zonas urbanas también puede generar ciertos riesgos para la privacidad de las personas, como afirman Anna Masutti y Filippo Tomasello[24].

Con la tercera generación de tecnologías -en la que tiene un protagonismo fundamental el uso de blockchain para el control de fronteras- ha aumentado la transparencia y la seguridad en la gestión de la información relacionada con la vigilancia de las fronteras, tal y como plantea Malcolm Campbell-Verduyn[25]. Sin embargo, la descentralización de la información en la blockchain puede generar brechas de seguridad en el tratamiento de la información. Aunque, lo cierto es que, a día de hoy (enero 2023), en el marco de la Unión Europea, los distintos agentes encargados del tratamiento de este tipo de datos trabajan utilizando un sistema centralizado con protocolos de seguridad muy estrictos[26].

La cuarta generación de tecnologías -en la que se engloban el internet de las cosas y el control de fronteras con algoritmos de aprendizaje automático- ha aumentado la eficiencia en la detección y respuesta a posibles amenazas. Sin embargo, el uso de algoritmos de aprendizaje automático en el control de fronteras puede plantear situaciones de discriminación, como plantea Frank Pasquale[27]. Por ejemplo, sería razonable que el uso de algoritmos de aprendizaje automático en el control de fronteras pueda crear preocupaciones sobre la posible discriminación basada en el origen étnico o la nacionalidad de las personas.

---

[21] J. C. HATHAWAY, *Human rights and refugee law*, Cheltenham, 2013.
[22] M. MILANOVIC, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*, Oxford, 2014.
[23] A. CLAPHAM, *Human rights and non-state actors*, Cheltenham, 2013.
[24] A. MASUTTI, F. TOMASELLO, *International regulation of non-military drones*, Cheltenham, 2018.
[25] M. CAMPBELL-VERDUYN, *Bitcoin and beyond: cryptocurrencies, blockchains, and global governance*, New York, 2018.
[26] J. CRUZ-ANGELES, *Procesamiento informático de datos y protección de derechos fundametnales en las fronteras exteriores de la Unión Europea*, in *Freedom, Security and Justice: European Legal Studies*, 2020, pp. 94 ss.
[27] F. PASQUALE, *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*, Oxford, 2020.

En definitiva, aunque las tecnologías de vigilancia de fronteras exteriores de la Unión Europea han permitido desarrollar una mayor precisión y eficiencia en la detección y respuesta a posibles amenazas, también han generado críticas en relación con la protección del derecho a la privacidad de los ciudadanos, así como de sus derechos civiles, según afirman varios autores iusinternacionalistas de reconocido prestigio. A tal efecto, es importante tener en cuenta la necesidad de aprobación de normativas adecuadas a medida que se desarrollan e implementan nuevas tecnologías para la supervisión y gestión de las fronteras, tratando de asegurar que se respeten los derechos de todas las personas y se adopten medidas adecuadas para proteger la privacidad y la seguridad de la información.