FUNDAMENTOS HISTÓRICOS DE LA BIOMETRÍA APLICADA A LA DEFENSA Y SUS PLANTEAMIENTOS ÉTICOS

HISTORICAL FOUNDATIONS OF BIOMETRICS APPLIED TO DEFENSE AND ITS ETHICAL APPROACHES

Luis Illanas García https://orcid.org/0000-0002-7229-1180

Universidad Rey Juan Carlos, España.

E-mail: anibal.ad.portas@gmail.com

Miguel Madueño Álvarez https://orcid.org/0000-0001-5798-0730

Universidad Rey Juan Carlos, España.

E-mail: miguel.madueno@urjc.es

DOI: https://doi.org/10.36132/fd9w0e33

Recibido: 01 octubre 2022 / Revisado: 01 julio 2023 / Aceptado: 19 julio 2023 / Publicado: 15 febrero 2024

Resumen: Con la implementación de nuevos y más sofisticados avances en Inteligencia Artificial (IA) destinados a mejorar los sistemas de control de armamento surgen nuevas aplicaciones y la necesidad de establecer una serie de medidas de control. Los datos biométricos han evolucionado en progresión paralela a los sistemas de IA, progresando desde las huellas dactilares a los escáneres de retina y los análisis de ADN. En este trabajo nos disponemos a analizar la importancia de estos elementos de control y a su implementación en las medidas defensivas de los estados así como a cuestionar la ética de su ejecución.

Palabras clave: IA, control de armas, datos biométricos, seguridad, drones

Abstract: With the implementation of new and more sophisticated advances in Artificial Intelligence (AI) aimed at improving weapons control systems, new applications and the need for a range of control measures are emerging. Biometric data has evolved in parallel to AI systems, progressing from fingerprints to retina scans and DNA analysis. In this paper we will analyse the importance of these control elements and their implementation in the defensive measures of states, as well as question the ethics of their execution.

Keywords: AI, gun control, biometrics, security, drones

INTRODUCCIÓN

Los identificadores o datos biométricos son características biológicas únicas, por tanto distintivas y cuantificables, empleadas para describir y clasificar a los individuos y que pueden incluir múltiples elementos, desde las más conocidas huellas dactilares hasta indicadores más complejos como pueden ser la firma cardíaca o los patrones de voz[1].

A lo largo de la historia, las distintas realidades sociales, especialmente las organizadas en formas estatales con estructuras políticas y sociales sólidas, se han preocupado por obtener información que facilitase un mayor control de la población. Estados de la antigüedad como Egipto o los diferentes Estados y ciudades Estado en Mesopotamia, se estructuraron alrededor de complejos sistemas burocráticos. Esta estructura fue heredada por las sociedades posteriores con medidas tales como censos y registros de ciudadanía. Además de mantener un riguroso control de la población, permitían implementar medidas que mejorasen los sistemas fiscal y judicial, aumentando las capacidades del Estado a la hora de obligar a sus ciudadanos a cumplir las leyes o satisfacer sus obligaciones fiscales. A mayor complejidad del sistema, mayor coste a la hora de realizar estos controles de población. Durante el siglo XX, a medida que se fueron mejorando y abaratando los medios de transporte, fueron implantándose los pasaportes y las identificaciones nacionales. Ya en Babilonia, se utilizaban huellas dactilares como marca para cerrar un contrato, una medida que los Estados comenzaron a tener en cuenta a finales del siglo XIX para identificar a posibles delincuentes. A medida que la tecnología ha dispuesto de mayor capacidad para implementar nuevas medidas, estas han ido evolucionando a los análisis de retina, dentales, códigos de ADN y la más reciente biometría o sistema de identificación de los rasgos faciales por medio de cámaras de alta precisión[2].

Esta es la razón por la que, coordinados con sistemas de IA, y desde múltiples plataformas como satélites o drones, los datos biométricos se hayan convertido en una herramienta fundamental en campos relacionados con la Inteligencia, como la verificación de control de armas y acuerdos de no proliferación, vigilancia de fronteras, lucha antiterrorista o el control de armamento. Mediante el uso de datos biométricos podemos suministrar a un sistema de IA los datos necesarios para determinar el acceso y el nivel a sistemas de armamento o crear unidades autónomas controladas que basen la toma de decisiones en factores derivados, entre otros, de la captación de datos biométricos, posibilitando un nuevo escenario en la guerra moderna[3]. Uno en el que las decisiones de sistemas autónomos se basen en indicadores biométricos que definan los objetivos. A partir de 2004, EEUU desarrolló el ABIS[4], por sus siglas en inglés, Sistema Biométrico de Información Automatizada, que entró en servicio en 2009. A grandes rasgos se trata de una base de datos, construida sobre indicadores biométricos de individuos potencialmente identificados como hostiles, tanto en Iraq como en Afganistán, que se ha convertido en un sistema global de identificación de objetivos por parte del ejército de EEUU y que basa sus búsquedas en registros dactilares, oculares y faciales.

El informe de 2003 del IPTS, *Institute for Prospective Technological Studies,* dependiente de la Comisión Europea, afirmaba que EEUU había implementado sistemas de recogida de indicadores biométricos que nutriesen la base de datos del ABIS en puntos de tránsito sensibles, como aeropuertos y pasos fronterizos en zonas en conflicto, especialmente, durante esos años, en la frontera entre Afganistán y Pakistán[5].

El ABIS es un sistema en permanente actualización, capaz de recoger, procesar y almacenar diferentes indicadores biométricos, huellas dactilares, palmares, escaneos de iris, retina y parámetros faciales, de manera que puede establecer, mediante la combinación de bancos de datos y de una IA, múltiples indicadores de coincidencia con respecto a los datos almacenados a la hora de detectar a un individuo potencialmente hostil. Sin embargo, el sistema, está sujeto a supervisión dependiendo de manera decisiva del factor humano, del que pende la última respon-

[1] Sayle, Kelley, "Biometric Technologies and Global Security", *Congressional Research Service*, (2021).

[2] García Quesada, Carla y López Palafox, Juan, "Historia de la identificación personal: desde el reconocimiento facial hasta el ADN dental", *Biociencias*, 14/1 (2019).

[3] Ibid.

[4] Escobar García, Arturo, *Desarrollo e implementación de un sistema automatizado para control de datos biométricos (In&Out)*, Veracruz, Universidad Tecnológica del Centro de Veracruz, 2018.

[5] Escajeado San Epifanio, Leire, *Reconocimiento e identificación de las personas mediante biometrías estáticas y dinámicas* (Tesis doctoral), Alicante, Universidad de Alicante, 2015, p. 96.

sabilidad como elemento evaluador y supervisor, tanto de los individuos identificados positivamente, como de aquellos cuya tipificación no sea concluyente.

La proliferación de sistemas balísticos, misiles de crucero y la emergencia de las nuevas armas hipersónicas también han posibilitado el desarrollo de sistemas de IA en dos sentidos, el de la defensa frente a estas amenazas y el opuesto, para el control y optimización de los sistemas de ataque de estas armas. Estos, coordinados mediante el uso de IA han supuesto una revolución en los medios de defensa convencionales dentro de los campos de batalla modernos, dando lugar a los denominados sistemas A2/AD[6]. Sistemas de defensa multinivel, que implican la coordinación de diferentes armas en tierra, mar y aire y el empleo de sistemas específicos, posibilitando la creación de zonas de denegación en el espacio aéreo, terrestre y marítimo.

El análisis de los datos biométricos relacionados con el control de armamento no es nuevo, desde hace décadas se ha generalizado el estudio e implementación de estos sistemas.

Ya hemos hablado del uso de las huellas dactilares en Babilonia como medio para verificar un contrato, contemporáneo a Babilonia, en Egipto se emplearon descripciones físicas de comerciantes y funcionarios para distinguirlos, de la misma manera que en China, a partir del siglo XIV, se popularizaron las impresiones de pies y manos de niños. El reconocimiento mediante la descripción física se mejoró y se implementó a comienzos del XIX, y a medida que el siglo fue avanzando, se incorporaron diferentes indicadores como la impresión de las palmas de las manos y las huellas dactilares. A finales de siglo el método Bertillon, o bertillonaje, incluía la recogida de medidas corporales, huellas dactilares y fotografías[7]. Desde la década de los 60 la identificación mediante patrones biométricos fue una prioridad para las agencias de seguridad estadounidenses. Desde los primeros análisis de patrones faciales, se evolucionó hacia la automatización de los sistemas de recogida y análisis de los datos, fundamentalmente en tres campos: el reconocimiento facial; el reconocimiento de voz, cuyo principal sistema fue desarrollado a finales de la década de los setenta por la Fuerza aérea de EEUU en un programa conjunto con la industria civil; y las huellas dactilares, siendo este último el que tuvo un desarrollo más amplio hasta comienzo de la década de los noventa. Entre medias, se investigaron sistemas diferentes como el análisis corporal mediante rayos x, el análisis dérmico o el reconocimiento ocular a través del iris, una idea que ya se había propuesto en 1936, que comenzó a implementarse como uno de los sistemas más fiables durante la primera mitad de la década de los noventa[8]. La implantación definitiva de sistemas de reconocimiento mediante datos biométricos vendría con el advenimiento del nuevo siglo, con la completa automatización de los sistemas de recogida y análisis mediante múltiples patrones y el desarrollo de algoritmos diseñados para facilitar y mejorar las capacidades de los sistemas de recogida y análisis.

Actualmente el ejército de EEUU emplea -en todos sus niveles de seguridad- sistemas de identificación biométricos tales como escáneres de retina, sistemas de reconocimiento facial y los más comunes sistemas dactiloscópicos, en labores de control de pagos[9] o acceso a determinadas instalaciones, con el objeto de establecer barreras de control sobre quien accede o está autorizado al uso u observación de determinados sistemas de armamento. Como veremos más adelante, el ejército de EEUU también es pionero[10] en operar estos sistemas desde plataformas como los drones. Se trata de una cuestión que evoluciona con un crecimiento exponencial, implementan-

[6] Son recomendables algunos trabajos sobre A2/AD como: Altman, Jonathan, "Russian A2/AD in the eastern Mediterranean", *Naval War College Review*, 69/1 (2016), pp. 72-85; Takahashi, Sugio, *Counter A2/AD in Japan-US Defense Cooperation: Toward 'Allied Air-Sea Battle'*, Washington, Project 2049, 2012; y Bitzinger, Richard A., *Third offset strategy and Chinese A2/AD capabilities*, Washington, Center for a New American Security, 2016.

[7] Palacios Laval, Cristian Enrique, "Entre Bertillon y Vucetich: las tecnologías de identificación policial. Santiago de Chile, 1893-1924", *Revista Historia y Justicia*, 1 (2013).

[8] García-Vázquez, Mireya Sarai y Ramírez-Acosta, Alejandro Álvaro, "Avances en el reconocimiento del iris: perspectivas y oportunidades en la investigación de algoritmos biométricos", *Computación y sistemas,* 16/3 (2012), pp. 267-276.

[9] El sistema APPS, Afghan Personnel & Pay System, implantado en Afganistán en 2016, se basaba en indicadores biométricos de miembros de la administración, policía y del Ejército Nacional Afgano para evitar duplicidad de identidades y fraude en los pagos de las nóminas. Guo, Eileen, "Los datos biométricos de los afganos, arma para la venganza talibana", *MIT Technology Review*, (2021).

[10] Sayler Kelley "Biometric…", op. cit.

do el uso de la IA hacia sistemas de armamento autónomos, más eficaces y que garantizan la seguridad de los militares que los controlan. Dentro de estos campos de aplicación de los identificadores biométricos, el que probablemente ha recibido mayor impulso durante los últimos años es, precisamente, el de los drones y vehículos no tripulados[11]. Los sistemas de IA han convertido a estos en unidades autónomas de combate diseñadas para tomar decisiones prescindiendo del factor humano. Por ello, Naciones Unidas[12] y la UE[13] han recomendado que cualquier sistema militar basado en datos biométricos este sujeto siempre al control humano, de modo que este, sea no solo un simple operador, sino que sea protagonista del control y desactivación del sistema en caso de fallo. Evidentemente, el uso de sistemas autónomos cuya misión principal es destruir y dar caza a objetivos militares concretos sin el control humano, plantea una dicotomía importante, dado que el elemento ético se sitúa en el punto de mira de la polémica.

Por otro lado, los sistemas de identificación biométricos más avanzados incluyen -en la actualidad-, además de sistemas de procesamiento mediante una IA, satélites destinados a albergar sistemas de defensa y otros equipados con sistemas para la recogida de datos biométricos y almacenamiento de los mismos gracias a la implementación del de nominado Big Data[14]. Actualmente, la gestión de sistemas biométricos relacionados con el Departamento de Defensa de EEUU está a cargo de la Defense Forensics & Biometrics Agency[15] (DFBA), cuyas competencias detalladas por el Departamento de Defensa incluyen los siguientes campos:

– Apoyar los procesos penales proporcionando pruebas materiales que afirmen o nieguen la vinculación de una persona con un acto hostil o un delito.

– Detectar terroristas, combatientes extranjeros e insurgentes que se amparan en el anonimato para protegerse de las fuerzas estadounidenses en el país y en el extranjero.

– Proteger las fronteras de los Estados Unidos mediante el apoyo biométrico a los socios conjuntos, interinstitucionales, de inteligencia e internacionales, de los grupos e individuos que intentan entrar en el país y hacer daño a la nación y a sus ciudadanos.

– Aumentar la eficacia del control de acceso físico y lógico, permitiendo que las personas autorizadas accedan sin tarjetas o distintivos, mientras que las personas no autorizadas son señaladas cuando presentan sus datos biométricos[16].

1. MÉTODO Y MATERIALES

La llegada de la IA en toda su magnitud es un hecho que en ocasiones puede despertar un debate público sobre cuestiones éticas[17]. El control de las máquinas siempre ha sido potestad del ser humano, pero los sistemas de IA -cada vez más autónomos- están haciendo retroceder esa dependencia. Los estados mantienen una lucha competitiva por la adquisición de un poder mayor y un mejor posicionamiento en el tablero de las relaciones internacionales, más cuando asistimos a un cambio de paradigma en el que el mundo bipolar imperante en la Guerra Fría y el breve *impasse* de dominio estadounidense han dado paso a un poder multicefálico con distintos protagonistas. Esto ha provocado la constante búsqueda de nuevas herramientas más sofistica-

[11] Boyd, Aaron, "Intel Agencies Seek to Perfect Biometric Recognition from Drones", *Nextgov*, (2020).

[12] *Consejo de Seguridad de Naciones Unidas*, Resolución 2396/2017, 21 de diciembre de 2017.

[13] European Parliament, P9_TA (2021) 0009, Artificial intelligence: questions of interpretation and application of international law.

[14] Debasa, Felipe, "Algorithms, Social Rejections and Public Administration in the Current World", en Saura, José Ramón y Debasa, Felipe, *Handbook of Research on Artificial Intelligence in Goverment practices and processes*, Londres, IGI Global, 2022, pp. 66-86; y, "Big Data in Aerospace and Defence: Technology Trends", *Army Tecghnology*, 29 de septiembre de 2020.

[15] Wilson, Lauren et al, "A systems approach to biometrics in the military domain", *Journal of forensic sciences,* 63/6 (2018), pp. 1858-1863.

[16] Department of Homeland security, Biometrics, Use of Biometrics in the Department of Defense, 2021.

[17] La normativa respecto a la ética y a la protección de las personas físicas descansa en documentos como el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Algunos trabajos que profundizan en la importancia de la ética al respecto son: Saura, José Ramón, "How to use Artificial Intelligence in Education? Current insights and prospects for Goverment", en Saura, José Ramón y Debasa, Felipe, *Handbook of …*, op. cit., pp. 339-352.

das y el empleo, por tanto, de la IA para incrementar la efectividad de los sistemas de defensa en los conocidos A2/AD.

Este trabajo pretende contribuir al análisis de esa modernización y aplicación de sistemas de IA en los planes estatales de defensa, así como a los problemas y cuestionamientos que puede suscitar su uso, al tratarse de sistemas autónomos con capacidad de respuesta lógica, que no humana, frente a imprevistos. Por ello, los objetivos de este trabajo se esbozan en:

1. Analizar la implementación de sistemas de IA y biometría para su uso en las estrategias de Defensa de los estados, tanto en armamento convencional como no convencional.

2. Analizar el debate que despierta la implementación de estos sistemas frente a su uso ético, sin fallos y con una dependencia humana cada vez menor.

El fenómeno es tan coetáneo a nuestros días que no se ha producido un tiempo razonable para evaluarlo con la perspectiva histórica plena que merece, a lo que hemos de añadir la escasez de fuentes y trabajos que traten el tema en cuestión. Dado lo novedoso del tema, nos encontramos ante desconocidos planteamientos y la producción académica, por tanto, es escasa. Esto debe ser un reto para todos los investigadores que se inicien en este campo y el principio para formar eso que los historiadores del futuro denominaron prospectiva. El cambio de las nuevas tecnologías es tan vertiginoso que en tan sólo cincuenta años el mundo entero ha mutado atravesando dos revoluciones tecnológicas que han cambiado nuestros hábitos y costumbres, pero sobre todo, que han propiciado un cambio también en las relaciones entre los estados. Con esta premisa, la metodología impuesta en este trabajo debe combinar las formas básicas del método histórico con herramientas de análisis que apuestan por hipótesis previas al hecho histórico. Por ello, abordamos este estudio desde tres puntos transversales con el fin de entender mejor las características del fenómeno a analizar. En primer lugar, atendiendo a la propia geografía, elemento determinante en la forma de actuar de los estados. Seguidamente, valoramos la propia tradición histórica del país o región en cuestión, así como los aspectos generales de la historia global en torno al tema analizado, dada la trascendencia de la evolución histórica en el mismo. Y para concluir, se debe mostrar especial interés en la deriva sociopolítica del estado y en las propias necesidades que tengan sus autoridades a la hora de implementar tecnologías biométricas de control. Diferentes sistemas seguirán caminos divergentes en cuanto a la implementación de medidas, tendentes a un mayor control de la población así como a la restricción de derechos de esta, de la misma manera que un Estado delimitado por una serie de condicionantes geográficos que asegure sus fronteras, lo hará de manera diferente a como debe actuar otro a merced de múltiples líneas fronterizas más o menos permeables. Todo ello, no obstante, afectado por componentes que atentan contra la seguridad global y estatal como el terrorismo o las redes internacionales de crimen organizado.

Partiendo de esta proyección, las hipótesis de partida son dos: en primer lugar, los avances tecnológicos son responsables del cada vez menor impacto del factor humano en la recogida, el procesado de datos y en la toma de decisiones; en segundo término, los sistemas de desarrollo integrados por la IA y por la biometría son el eje principal de las estrategias de seguridad y control de armamento de los países.

Estas cuestiones están relacionadas con el debate sobre la ética de los procedimientos que oscilan entre la seguridad y la libertad[18], y en la justificación que tiene un estado para implementar medidas autónomas de un elemento capaz de detectar y eliminar a un objetivo humano. Esto puede ocasionar una pérdida irreparable, en base a unas directrices y a la decisión última y autónoma de una IA, que actuara en función de los datos que haya recibido previamente, suministrados, en cualquier caso, por un humano.

El trabajo se ha dividido en una introducción para contextualizar el objeto de estudio y dos capítulos que consideramos básicos y en los que se demuestra la implementación de estos sistemas de Defensa, basados en la combinación de aspectos biométricos y de la IA. El primero de ellos es sobre el armamento no convencional y más concretamente sobre los arsenales nucleares que siguen dominando las relaciones internacionales a nivel mundial. Durante el periodo de Guerra Fría, los arsenales fueron a la par amenaza y freno del

[18] Pérez Martínez, José Emilio, "The Dark Side of Progress: Social and Political Movements Against Artificial Intelligence in Spain", en Saura, José Ramón y Debasa, Felipe, *Handbook of* …, op. cit., pp. 226-242.

inminente estallido de una guerra global y letal[19], y en la actualidad, pese a que la economía regula el equilibrio de fuerzas, sus argumentos respaldan el poderío de los estados con el incremento de los sistemas A2/AD. El siguiente capítulo se centra en la herramienta básica de estos sistemas de defensa estratégica: los drones y LAWs, que ejemplifican la ejecución de estas teorías y abren el debate sobre la autonomía de la IA, capaz de decidir en unos segundos, sin injerencia humana en vivo.

2. CONTROL DE ARMAMENTO NO CONVENCIONAL

Durante las décadas de la política de bloques en el contexto de la Guerra Fría, cuando se enfrentaron Estados Unidos y la Unión Soviética junto a sus aliados, el control de armas se realizaba por medio de acuerdos de limitación de armamento[20], que implicaba en mayor medida el control de sistemas balísticos nucleares. Estas se basaban en el establecimiento de relaciones de confianza mutua destinados a limitar y evitar un conflicto y al establecimiento de medidas de vigilancia e información bilaterales junto con elementos neutrales o unilaterales mediante operaciones de inteligencia, donde el desarrollo tecnológico adquirió un peso determinante por medio de la implementación de sistemas de vigilancia por satélite. Medidas que eran consideradas el único medio viable de verificar el cumplimiento de lo acordado[21], aunque realmente el poder de destrucción de las armas nucleares fue, paradójicamente, lo que mantuvo la paz general en el globo y las tensiones se transmitieron únicamente a determinados ámbitos locales. Se trataba de limitar las políticas coercitivas que otorgaban las capacidades facilitadas por sistemas de armas no convencionales, fundamentalmente la capacidad nuclear, así como de los sistemas de defensa específicos, que suponían negar la capacidad del adversario. Así actuaba el Sistema de Defensa Estratégica puesto en marcha por la administración de Ronald Reagan en los últimos estertores de la Guerra Fría. Su funcionamiento efectivo sigue siendo una incógnita, pero sirvió como un elemento coercitivo frente a la URSS, que ante la duda sobre la eficacia del sistema, mantuvo una cierta cautela y negoció a la baja frente a su homólogo de Washington[22]. Mientras tanto, la Unión Soviética continuaba aumentando su arsenal balístico en paralelo a los avances tecnológicos de Estados Unidos y consiguió, también, elevar el nivel de preocupación de la administración Reagan. Esta política de acumulación de armamento no convencional para ejercer una amenaza sobre el adversario formaba parte de la paradoja estabilidad-inestabilidad. Lograr estabilidad en el propio territorio a costa de desestabilizar al adversario mediante la amenaza y la coerción que proporcionaban el armamento no convencional y la capacidad de impedir el empleo de su arsenal de armas no convencionales.

Desde entonces la defensa contra misiles ha sido una de las cuestiones estratégicas más interesantes en lo que se refiere a control de armamento, siendo en la actualidad uno de los aspectos inherentes a la defensa que más preocupan a analistas y miembros de las FFAA de todo el mundo. Desde principios de la década de los años noventa del siglo XX, el Departamento de defensa de EEUU comenzó el desarrollo e implantación de diferentes sistemas de control biométrico basados en reconocimiento facial. El pionero fue el programa FERET, *Face Recognition Technology*, desarrollado entre 1993 y 1997[23], dependiente de la Agencia de proyectos de investigación avanzados para defensa, DARPA. En esa línea, en el mismo periodo, la NNSA, Administración Nacional de Seguridad Nuclear, por sus siglas en inglés, comenzó a implantar sistemas de reconocimiento a través de escáneres de iris[24].

El documento *Missile Defense Review* de 2019, MDR, editado por el Departamento de Defensa de EEUU, recogía la necesidad de plantear una defensa multinivel frente a un ataque con misiles. Una defensa activa que combinase la detección, tanto de los sistemas de ataque enemigos con el desarrollo de sistemas de prevención, como una defensa pasiva. En este caso, contemplaba sistemas de alerta temprana controlados por otros de detección y satélites equipados con cámaras de alta resolución dotados con elementos de reconocimiento facial y sistemas de

[19] Azcona, José Manuel y Madueño, Miguel, *Guerra y Orden Internacional*, Madrid, Síntesis, 2021, p. 141.
[20] Planells Boned, Francisco, "La reducción de las armas estratégicas", *Boletín de Información*, 168 (1983), p. 1.
[21] Vaynman, Jane, "Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control" *Texas National Security Review*, 4/4 (2021).
[22] Ojeda, Jaime, "Defensa antimisiles: El sueño de Reagan", *Política Exterior*, (2004), pp. 131-142.
[23] Escajeado San Epifanio, Leire, "Reconocimiento …", op. cit., p. 90.
[24] Ibid., p. 96.

infrarrojos, todo ello coordinado mediante la implementación de la IA, facilitando así la alerta temprana y, en consecuencia, una respuesta adecuada en tiempo y forma ante un hipotético ataque[25]. Como parte de la defensa activa, son capaces de coordinar y lanzar una serie de ataques preventivos de manera prácticamente autónoma, atajando la amenaza en origen, con capacidad de reconocer sobre el terreno no solo dispositivos y elementos militares, sino también a individuos. En este caso no solamente serían capaces de detectar operadores si no que serían competentes descubriendo elementos humanos clave en la toma de decisiones y eliminarlos, en caso de disponer de los datos necesarios. En esta cuestión el sistema ABIS sería un facilitador clave.

El MDR también recoge la necesidad de implementar programas de desarrollo científico que provean de tecnología cada vez más avanzada y efectiva contra las amenazas que plantean sus enemigos. En 2021 la NNSA, que es la agencia gubernamental responsable de la seguridad de los arsenales nucleares de EEUU y del desarrollo de los programas de defensa relacionados con este tipo de elementos no convencionales, tenía implementados -como parte de su sistema de seguridad- escáneres de retina, sistemas de reconocimiento facial, dactiloscópicos y sensores de ADN. Seguimos de alguna manera ante una estrategia coercitiva por parte de todos los actores implicados, en cuya base se encuentran los sistemas de control de armamento, que son el medio del monopolio de la coerción por parte de los actores designados. La cuestión sería determinar hasta qué punto los avances tecnológicos y el cada vez menor impacto del factor humano. tanto en la recogida y procesado de datos como en la toma de decisiones, afectan en este momento al control de armamento convencional y no convencional por parte de los estados. Para ello hay que tener en cuenta, hablando en términos privativos, que la capacidad de monitorización y de procesado de datos mediante sistemas de IA facilitan la supervisión y la verificación de los límites establecidos por el derecho internacional o los acuerdos entre estados[26], y que la capacidad de recoger indicadores biométricos aumenta y mejora la cantidad y la calidad de los datos almacenados. En este sentido la mínima implicación del factor humano en favor de sistemas autónomos de IA podría determinarse, entre otros factores, por la capacidad de este de establecer la conveniencia de revelar su ventaja tecnológica o capacidades de inteligencia cuando estas detecten una alteración del statu quo establecido. El factor humano se reduciría a la mera supervisión y a la toma de decisiones en los niveles últimos del sistema, así como a controlar el flujo de información derivado de los sistemas implementados.

3. DRONES Y LAWS

Los drones, o en su acrónimo en inglés, RPAS, *Remotely Piloted Aircraft System,* o UAV, *Unmaned Aerial Vehicle*, son sistemas aéreos de transporte autónomos, que en su empleo para fines militares abarcan tareas desde diferentes formas de vigilancia y reconocimiento hasta la realización de ataques convencionales[27]. Las capacidades de vigilancia en lo que a control de armas se refiere, destacan por la versatilidad a la hora de emplearlos como herramientas de alta capacidad, incluyendo sistemas de reconocimiento facial. Podríamos considerar a los drones como una extensión de las capacidades de vigilancia y monitorización de su operador, dada su capacidad de recopilar, procesar y enviar información en tiempo real a este, y por la capacidad de los drones de operar sobre el terreno en condiciones imposibles en algunos casos para el ser humano[28], como la pérdida total de oxígeno, maniobras especiales o cambios bruscos de altitud.

Los sistemas de identificación biométricos son una de las más interesantes aplicaciones en el campo de los drones de combate y su uso se está generalizando, lográndose en caso de su empleo como plataforma de armas, un sistema de optimización de objetivos[29]. En este caso, una aplicación secundaria ha dado lugar a un nuevo paradigma sobre la aplicación de los sistemas de identificación biométricos. De esta manera, en

[25] Department of Defense - Office of the Secretary of Defense, Missile Defense Review, 2019.
[26] Vaynman, Jane, "Better Monitoring …", op. cit.
[27] *Ministerio de Defensa - Dirección General de Armamento y Material,* Plan director de RPAS, 2015.
[28] Vaynman, Jane, "Better Monitoring …", op. cit.
[29] Pulido, Guillermo, *Guerra multidominio y mosaico. El nuevo pensamiento militar estadounidense*, Madrid, Catarata, 2021.

Libia[30] fueron empleados enjambres[31] de drones turcos *Kargu 2*[32] equipados con sistemas de reconocimiento facial, diseñados para asumir la toma de decisiones en el caso de perder la conexión con su operador. Estos drones operaron de manera autónoma bajo el paraguas de la cobertura A2/AD facilitada por Turquía a las tropas del gobierno de Fayez Sarraj[33]. Como vemos, la implementación de sistemas de recogida de datos biométricos adquiere en este caso, una aplicación diferente con respecto a los sistemas de vigilancia anteriormente expuestos, ahora destinados a la identificación y selección de objetivos de manera directa sobre una zona en conflicto. Este hecho, que a comienzos de 2021 se consideraba eminentemente teórico[34], confirma la capacidad de detección de elementos y comportamientos a pequeña escala, otorgando la posibilidad de reaccionar frente a potenciales amenazas de manera inmediata en el campo de operaciones sin la necesidad de ser dirigidos por la acción humana.

Los sistemas de armas autónomas, denominados por sus siglas en inglés, LAW, *Lethal autonomous weapon*, dentro de las que se encuadran los drones, son sistemas, de acuerdo con la definición establecida por la UE, que pueden buscar, seleccionar y atacar objetivos sin intervención humana. Estas armas son una realidad desde hace algunos años, pero lo que ha cambiado realmente el paradigma es que, estas armas solamente responden a objetivos previamente programados o determinados por el factor humano, de modo que a pesar de una mayor autonomía, de facto, siguen actuando bajo las directrices insertadas por un ser humano. Lo que el ejército turco ha demostrado en Libia, ha sido que las LAWs operando por medio de una IA, una base de datos biométricos de objetivos humanos designados, pueden buscar, seleccionar y atacarlos de manera completamente autónoma, sin necesidad de un operador, es decir, prescindiendo del factor humano[35].

El uso de vehículos autónomos para control de armas, teniendo en cuenta el factor humano, facilitaría entre otras cuestiones, la velocidad y la flexibilidad de la tarea. La capacidad de recoger indicadores biométricos en labores de reconocimiento y la capacidad de procesado coordinado mediante una IA, facilitarían aún más el trabajo, incorporando nuevas variables como la detección y el reconocimiento de elementos humanos en tiempo real.

Tanto EEUU como Israel, que poseen una de las industrias de drones más potentes del mundo, están trabajando en la mejora de los sistemas de identificación biométrica operados desde drones, campo en el que la empresa de logística Amazon ha sido pionera, en la praxis del empleo de este tipo de sistemas para identificar mediante escáneres faciales a los destinatarios de sus productos y a los clientes. EEUU, mediante drones dotados de sistemas de reconocimientos facial, integrados en el sistema ABIS, programa BRIAR, *Biometric Recognition and Identification at Altitude and Range*, ha sido capaz de emplear estos indicadores biométricos para identificar y señalar objetivos a drones operando a gran altura[36], aunque como vimos, el ABIS no es un sistema completamente autónomo, ya que depende, en primera y última instancia, de las instrucciones insertadas previamente por un humano. El desarrollo de estos sistemas de reconocimiento de indicadores biométricos fueron una iniciativa de la agencia gubernamental *Intelligence Advanced Research Projects Activity,* IARPA, que desde antes de 2020 venía insistiendo en la necesidad de implementar un programa destinado al reconocimiento facial desde drones a gran altura[37].

Previamente, Israel ya había implementado sistemas de recogida y procesado de indicadores biométricos como medida de control de fronteras, sobre todo en los pasos habilitados hacia los territorios ocupados de Gaza y Cisjordania, siguiendo una línea de actuación común a otros estados como Rusia, China, Turquía o como hemos visto, los propios EEUU tanto a nivel domés-

[30] Naciones Unidas publicó un informe en el que se afirmaba el empleo de drones autónomos tipo Kargu 2 en Libia. Wendehorst, Cristiane y Duller, Yannic, *Biometric Recognition and Behavioural Detection*, Bruselas, Policy Department for Citizens' Rights and Constitutional Affairs - European Parliament, 2021, pp. 19-20.

[31] Vaynman, Jane, "Better Monitoring …", op. cit.

[32] Nash, Jim, "Like a nightmare come true: Killer robots fighting humanity's wars Face biometrics may have been used in drone combat", BiometricUpdate.com, 4 de junio de 2021.

[33] *Consejo de Seguridad de Naciones Unidas*, S/2021/229, pp. 15-16.

[34] Sayler, Kelley, "Biometric …", op. cit.

[35] *Consejo de Seguridad de Naciones Unidas*, S/2021/229, p. 17.

[36] Guo, Eileen, "Los datos biométricos …", op. cit.

[37] Boyd, Aaron, "Intel Agencies Seek to Perfect Biometric Recognition from Drones", *Nextgov*, (2020).

tico, como en teatros de operaciones considerados sensibles.

A principios de enero de 2021, Rafael Advanced Defense Systems, una de las principales empresas tecnológicas de Israel centradas en el campo de la seguridad y la defensa, anunció su primer sistema de IA diseñado para procesar información proveniente de sistemas de visión autónoma y de recogida de datos biométricos, pensados para operar tanto desde UAVs como desde sistemas autónomos susceptibles de ser empleados como LAWs. El desarrollo de sistemas de recogida de indicadores biométricos, principalmente faciales, aplicados a los drones ha sido una de las principales líneas de investigación de Rafael en los últimos años. Una de las intenciones declaradas de Rafael es, de la misma manera que Turquía, producir drones de bajo coste equipados con sistemas de reconocimiento facial, capaces de operar de manera autónoma bajo control de una IA prescindiendo del factor humano.

China es otro de los estados que ha implementado sistemas de identificación biométrica en sus vehículos no tripulados. Empresas como Hangzhou Hikvision Digital Technology, vinculada al Partido Comunista de China (PCCH) y una de las principales empresas dedicadas al suministro de sistemas de video vigilancia; y Huawei, colaboran en el desarrollo de estos sistemas, no solo circunscritos al campo de los drones y los vehículos no tripulados, sino también en sistemas de recogida e identificación convencionales o en el campo de los satélites. En este sentido, surge la duda razonable sobre si el Estado emplea o empleará la formidable maquinaria que constituye el denominado Sistema de Crédito Social, para alimentar también las bases de datos militares, como ya hace con las bases de datos de la policía, que recogen, entre otros, indicadores biométricos de ciudadanos o extranjeros que pudieran constituir potenciales objetivos y en el que Hangzhou Hikvision Digital Technology es uno de los principales suministradores de tecnología.

El programa de crédito social[38] se sustenta en tres ejes: el Big Data o los grandes bancos de datos que alimentan la propia estructura del sistema; la IA que procesa y ejecuta la información; y las cámaras dotadas de elementos de identificación biométrica, encargadas de elaborar patrones medios de identificación más rápidos y automatizados[39].

El volumen de datos generado por 730 millones de usuarios hace del mercado chino el mayor banco de información del planeta en un sistema independiente de la red global. Las grandes empresas como Tencent o Alibaba, y motores de búsqueda como Baidu, alimentan los bancos de datos gubernamentales que sustentan el sistema de crédito social. y pueden ser utilizados en la implementación de medidas de seguridad y defensa. La información se convierte así en la nueva moneda de la economía global y a cambio del acceso a determinados puntos de la red, las grandes bolsas de datos se nutren suministrando herramientas a los sistemas de defensa, que en el caso de China, es controlada por el Estado o en su defecto, por grandes multinacionales sometidas a medios de control por parte de este. Tanto China como Rusia, también se encuentran en proceso de desarrollo de LAWs, que, tras la experiencia turca en Libia, presumiblemente integrarían sistemas de identificación de objetivos mediante indicadores biométricos. Libia se ha convertido en el más reciente laboratorio de prueba de vehículos autónomos, mientras que China suministró a las fuerzas de Halifa Haftar: UAV, los modelos Sea Cavalry SD-40[40], vigilancia marítima y Wing Loong I y II[41]. Estos últimos son parte de un modelo versatil, tanto como plataforma de armas, como en labores de inteligencia equipado con dispositivos vigilancia y reconocimiento, cámaras y sensores diurnos e infrarrojos para operaciones nocturnas[42]. Dada su función como plataforma de vigilancia en el caso del Sea Cavalry y de vigilancia y ataque en el caso de los Wing Loong, ambos modelos son susceptibles de integrar sistemas de captación e identificación de datos biométricos, como reconocimiento facial. En el caso de los modelos Wing Loong optimizarían sus capacidades de ataque y harían factible su empleo como vehículo autónomo, de

[38] Madueño Álvarez, Miguel y Illanas García, Luis, "The Role of IA in a Security and Population Control System: Chinese Social Credit System", en Saura, José Ramón y Debasa, Felipe, *Handbook of…*, op. cit., pp. 190-209.

[39] Domaica Maroto, Juana María, *Datos personales biométricos dactiloscópicos y derechos fundamentales: nuevos retos para el legislador* (Tesis doctoral), UNED, 2019.

[40] "Sea Cavalry SD-40 Maritime UAV", *Naval Tecghnology*, 5 de abril de 2019.

[41] *Consejo de Seguridad de Naciones Unidas*, Informe final del Grupo de Expertos sobre Libia Establecido en virtud de la resolución 1973 (2011) del Consejo de Seguridad, 2019, p. 34.

[42] "Wing Loong Unmanned Aerial Vehicle (UAV)", *Air Force Technology*, 2 de febrero de 2021.

nuevo, prescindiendo del factor humano. El gobierno de Haftar también intentó, según manifiesta la Organización de Naciones Unidas en su informe del 8 de marzo 2021[43], solicitar a Rusia drones avanzados para labores de inteligencia y reconocimiento, que le habrían sido denegados. Sin embargo Rusia sí habría suministrado sistemas aéreos no tripulados para labores básicas de reconocimiento[44].

Turquía, como hemos visto, también implicada en Libia con drones del tipo Bayraktar TB2, es una incipiente potencia tanto en el campo de los UAV, como en el desarrollo de sistemas de recogida y procesado de datos biométricos. Desde 2016 Turquía ha empleado sistemas de recogida y procesado de datos biométricos para establecer controles sobre los flujos migratorios que atraviesan el país. La praxis turca al respecto de los Kargu 2 en Libia, indica que Turquía dispone de una tecnología propia capacitada para operar desde plataformas como drones y lo que es más importante, de forma completamente autónoma.

El análisis biométrico puede considerarse una intromisión en la construcción de la forma física humana, especialmente en el rostro. Los transhumanistas abogan desde sus primeros planteamientos que el ser humano es un híbrido entre la tecnología, la herencia biológica y las modificaciones corporales que cada individuo de manera autónoma decida. Los análisis biométricos, tal y como se conciben, estan pensados sin tener en cuenta las propuestas transhumanistas sobre la construcción de la persona, por tanto, esta investigación queda abierta hacia las nuevas formas de entendimiento del ser humano y su representación física, especialmente lo que tiene que ver con la imagen y el rostro[45].

CONCLUSIONES

Como hemos podido comprobar, los sistemas de recogida de datos biométricos en relación con el control de armamento tienen múltiples aplicaciones. Nos hemos centrado en las que hemos considerado más relevantes, tanto por la unilateralidad que la monitorización otorga a los Estados, como por la efectividad y rapidez que estos sistemas confieren a los drones para operar de manera autónoma en todos los niveles, prescindiendo del factor humano. Las consecuencias que tiene la autonomía otorgada por los sistemas biométricos y de recogida y procesado de la información implica una pérdida del factor humano, que debería ocupar el último nivel de la toma de decisiones.

En este caso el factor humano se sitúa en un primer nivel, dotando de autonomía a los medios militares para identificar, procesar y reaccionar, aunque siempre bajo la premisa de una programación previa en base a unos parámetros y unas constantes que un operador humano ha insertado en los comandos del dron. La combinación de sistemas de recogida de indicadores biométricos con sistemas de IA, mejoran las capacidades de detección y análisis de esta, aportando un corpus de datos con mayor nivel de detalle. Esto propicia una mayor rapidez de su procesado, celeridad e inmediatez a la hora de implementar medidas, tanto de manera autónoma como por la capacidad de facilitar información más detallada, sin embargo, reduce la decisión humana última.

En 2017 el Consejo de Seguridad de Naciones Unidas emitió la resolución 2396/2017 de 21 de diciembre, aprobada de acuerdo con el Capítulo VII de la Carta de Naciones Unidas, que obliga al cumplimiento de las disposiciones de la resolución a todos los Estados miembros, instando a estos a implementar sistemas de recogida de datos biométricos con el fin de implantar mejoras en las medidas de seguridad destinadas a disminuir el riesgo de ataques terroristas. Estos sistemas implican una mejora en la identificación de ciudadanos mediante escáneres faciales y huellas dactilares recogidas en pasaportes y documentos de identidad, y la implantación de sistemas de datos cruzados entre agencias y organizaciones de gobierno y de seguridad, nacionales y supranacionales.

Aunque circunscrita al ámbito civil, también la UE en abril de 2021 se manifestó a favor de una regulación estricta acerca de la captación de datos biométricos en espacios públicos por considerarlo una amenaza para la seguridad[46].

[43] *Consejo de Seguridad de Naciones Unidas*, S/2021/229, p. 17.
[44] Ibid., p. 438.
[45] Debasa, Felipe, "Transhumanismo y contracultura", en Azcona, José Manuel et al., *De la "beat generation" al movimiento punk: vástagos culturales de la sociedad de la abundancia,* Madrid, Sílex, 2021, pp. 135-158.
[46] Gil, Andrés, "Bruselas quiere prohibir 'sistemas de identificación biométrica remota en espacios públicos' en su regulación de la inteligencia artificial", *El Diario.es*, 21 de abril de 2021.

La presión sobre organizaciones terroristas y las zonas de conflicto, como puede ser el Mediterráneo oriental o el norte de África, han incrementado de manera ostensible los flujos migratorios, incluyendo un aumento del número de combatientes que regresan a sus países de origen y aumentando la percepción de amenaza. Para los Estados, estos retornados implicarían un aumento del riesgo de atentado, incluyendo la posibilidad de acceso de algunos repatriados a determinados puestos sensibles que implicarían un riesgo para la seguridad, como podrían ser agencias u organizaciones de seguridad y defensa. En este sentido se antoja imprescindible, con respecto a la cuestión de control de armamentos, implementar nuevas medidas de seguridad. Las mejoras en la capacidad de supervisión unilateral aumentarían sobre el papel la seguridad y la capacidad coercitiva de los estados a la hora de implementar controles de armamento. Elevarían los flujos de información y, en casos de control de armamento, incrementaría el control sobre esa misma información y sobre la toma de decisiones. La mayor intervención sobre estos sistemas proveería de la capacidad de activar estructuras integradas y coordinadas, facilitando -por ejemplo- el empleo de capacidades A2/AD. Los sistemas de desarrollo integrado serían así el eje principal de las estrategias de seguridad y control de armento que tendrían en los sistemas de recogida y procesado de datos biométricos un elemento capacitador.

En el caso de los sistemas autónomos, se ha priorizado la adquisición de capacidades tales como la rapidez, la flexibilidad y la seguridad, sobre todo a la hora de identificar objetivos, jugando un papel determinante el empleo de sistemas de identificación biométricos.

Como vemos, diversos organismos internacionales, Naciones Unidas y OSCE tratan de legislar al regular el uso de sistemas biométricos y su aplicación militar, fundamentalmente en aspectos derivados de sistemas de IA autónomos, basados en la recogida de indicadores biométricos, como el reconocimiento facial. Organizaciones políticas vinculantes como la UE, también están tratado de legislar sobre el uso de las LAW y de otros armamentos autónomos basados en la coordinación multinivel por medio de la IA, en el que tendría una importancia clave el uso de datos biométricos como medio de identificación de objetivos. Sin embargo, la cuestión es compleja cuando se trata de los principales actores del teatro geopolítico mundial, ya que ni EEUU, ni China, ni Rusia tienen legislación ni regulación alguna con respecto a las LAWs o drones autónomos. No parecen muy dispuestos a implementarlas, más allá de algunas iniciativas en el Congreso de EEUU destinadas a evaluar los riesgos que comporta el desarrollo de este tipo de sistemas autónomos. Si bien Rusia y China, a priori, tendrían menos condicionantes de tipo político a la hora de desarrollar e implementar este tipo de sistemas, se antoja complicado que EEUU otorgue a sus principales rivales globales el desarrollo de esta ventaja competitiva. De hecho, a comienzos de 2021, el ejército de EEUU comenzaba el proceso de implementación de un nuevo sistema basado en indicadores biométricos. El denominado NXGBCC, *Next Generation Biometric Collection Capability*, proveerá de nuevas capacidades al ejército de EEUU, incluyendo aplicaciones tácticas sobre el terreno en base a indicadores biométricos[47], centradas en la creación de bancos de datos y repositorios más eficaces y completos y en una coordinación multinivel más eficaz con el sistema ABIS, de manera que el Departamento de Defensa y las agencias y organizaciones gubernamentales que dependen de él, puedan aprovecharse de las nuevas capacidades del sistema NXGBCC[48]. Así mismo, mejora las capacidades de inteligencia, centrándose en los nuevos tipos de conflicto y en los sistemas y capacidades asociados a ellos. En este sentido, se prevé que el NXGBCC juegue un papel clave en cuestiones relacionadas con sistemas A2/AD, en la protección de estos respecto a las contramedidas desplegadas por los antagonistas del ejército de EEUU durante un conflicto, así como en la mejora de las capacidades destinadas a penetrar los sistemas enemigos[49].

Al margen de su aplicación militar, en Europa, las técnicas biométricas se evalúan por el Convenio Europeo de Derechos Humanos CEDH. Los miembros del Consejo de Europa, incluidos los 27 de la UE, Reino Unido, Rusia y Turquía, son parte del CEDH[50]. La tecnología biométrica presenta una serie de vulnerabilidades, que revelan la existencia de una duda razonable sobre, si sería viable un fallo en los sistemas que la incorporan, ya sea un fallo derivado de un mal funciona-

[47] *U.S. Army*, Army Futures Command Pamphlet "Army Futures Command Concept for Intelligence 2028" Futures and Concepts Center, 2020.
[48] Ibid.
[49] Ibid.
[50] Wendehorst, Cristiane y Duller, Yannic, *Biometric Recognition*…, op. cit.

miento o uno provocado. Así mismo muestra las preocupaciones éticas inherentes al empleo de un sistema totalmente autónomo y las implicaciones que tendría la identificación errónea de un objetivo, cuestión planteada ya por algunos autores[51]. La IA falla con regularidad a la hora de identificar determinados patrones raciales o sexuales, al tiempo que es posible engañar a los sistemas tanto de captación de indicadores biométricos como de identificación de estos[52]. Esto también implica la dificultad de las IA a la hora de discriminar entre soldados y civiles.

El cambio tecnológico, su regulación o la falta de ella, puede alterar la forma en que los Estados se relacionen entre sí en cuestiones como el control de armamento. Las características de tecnologías emergentes como son las relacionadas con la recogida de datos biométricos cada vez más precisos y fiables y su análisis y procesado mediante una IA son importantes a la hora de determinar cómo afectarán a la supervisión y a la dicotomía transparencia-seguridad. Es probable que la tecnología emergente afecte a los acuerdos de control de armemento. Las armas hipersónicas afectarían a la estabilidad de los Estados, obligando a estos a desarrollar e implementar nuevos y más complejos sistemas de identificación y detección temprana, de tal manera que denegasen a otros usuarios de este tipo de armas o de otros sistemas no convencionales. La recogida de datos biométricos experimentará, sin duda, una nueva fase.

[51] Saura, José Ramón et al., "Ethical Design in Social Media: Assessing the main performance measurements of user online behavior modification", *Journal of Business Research*, 129 (2021), pp. 271-281.
[52] Sayler, Kelley, "Biometric Technologies …", op. cit.

FUENTES

- "Big Data in Aerospace and Defence: Technology Trends", *Army Tecghnology*, 2020.
- "Sea Cavalry SD-40 Maritime UAV", *Naval Tecghnology*, 2019.
- "Wing Loong Unmanned Aerial Vehicle (UAV)", *Air Force Tecghnology*, 2020.
- *Department of Defense - Office of the Secretary of Defense*, Missile Defense Review, 2019.
- *Ministerio de Defensa - Dirección General de Armamento y Material*, Plan director de RPAS, 2015.
- *U.S. Army*, Army Futures Command Pamphlet. Army Futures Command Concept for Intelligence 2028" Futures and Concepts Center, 2020.
- *Consejo de Seguridad de Naciones Unidas*, "Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973, 2011, S/2021/229.
- *Consejo de Seguridad de Naciones Unidas*, Resolución 2396/2017, 21 de diciembre de 2017.
- *Department of Homeland Security*, Biometrics, Use of Biometrics in the Department of Defense, 2021.
- *European Parliament*, P9_TA 0009, Artificial intelligence: questions of interpretation and application of international law, 2021
- The office of the Director, Operational Test and Evaluation, "DOD Automated Biometric Identification System (ABIS)", *FY 2014 Annual Report*, pp 103-105.

BIBLIOGRAFÍA

- Altman, Jonathan, "Russian A2/AD in the eastern Mediterranean", *Naval War College Review*, 69/1, (2016), pp. 72-85.
- Azcona, Pastor y Madueño, Miguel, *Guerra y Orden Internacional*, Madrid, Síntesis, 2021, p. 141.
- Bitzinger, Richard A., *Third offset strategy and Chinese A2/AD capabilities*, Washington, Center for a New American Security, 2016.
- Boyd, Aaron, "Intel Agencies Seek to Perfect Biometric Recognition from Drones", *Nextgov*, (2020).
- Debasa, Felipe, "Transhumanismo y contracultura", en Azcona, José Manuel, Abdiu, Majlinda y Burón, Manuel, De *la beat generation" al movimiento punk: Vástagos culturales de la sociedad de la abundancia*, Madrid, Sílex, 2021.
  - "Algorithms, Social Rejections and Public Administration in the Current World", en Saura, José Ramón y Debasa, Felipe, Handbook *of Research on Artificial Intelligence in Goverment practices and processes*, Londres, IGI Global, 2022.
- Domaica Maroto, Juana María, *Datos personales biométricos dactiloscópicos y derechos fundamentales: Nuevos retos para el legislador* (Tesis doctoral), UNED, 2019.
- Escajeado San Epifanio, Leire, *Reconocimiento e identificación de las personas mediante biometrías estáticas y dinámicas* (Tesis doctoral), Alicante, Universidad de Alicante, 2015.
- Escobar García, Arturo, *Desarrollo e implementación de un sistema automatizado para control de datos biométricos (In&Out)*, Veracruz, Universidad Tecnológica del Centro de Veracruz, 2018.
- García Quesada, Carla y López Palafox, Juan, "Historia de la identificación personal: desde el

reconocimiento facial hasta el ADN dental", *Biociencias*, 14/1 (2019).

- García-Vázquez, Mireya Sarai y Ramírez-Acosta, Alejandro Álvaro, "Avances en el reconocimiento del iris: perspectivas y oportunidades en la investigación de algoritmos biométricos", *Computación y sistemas*, 16/3 (2012).
- Gil, Andrés, "Bruselas quiere prohibir "sistemas de identificación biométrica remota en espacios públicos" en su regulación de la inteligencia artificial", *El Diario.es*, 21 de abril de 2021.
- Guo, Eileen, "Los datos biométricos de los afganos, arma para la venganza talibana", *MIT Technology Review*, 2021.
- Madueño Álvarez, Miguel y Illanas García, Luis, "The Role of IA in a Security and Population Control System: Chinese Social Credit System, en Saura, José Ramón y Debasa, Felipe, *Handbook of Research on Artificial Intelligence in Goverment practices and processes*, Londres, IGI Global, 2022, pp. 190-209.
- Nash, Jim, "Like a nightmare come true: Killer robots fighting humanity's wars Face biometrics may have been used in drone combat", *BiometricUpdate.com*, 4 de junio de 2021.
- Ojeda, Jaime, "Defensa antimisiles: El sueño de Reagan", *Política Exterior*, (2004).
- Palacios Laval, Cristian Enrique, "Entre Bertillon y Vucetich: las tecnologías de identificación policial. Santiago de Chile, 1893-1924", *Revista Historia y Justicia*, 1 (2013).
- Pérez Martínez, José Emilio, "The Dark Side of Progress: Social and Political Movements Against Artificial Intelligence in Spain", en Saura, José Ramón y Debasa, Felipe, *Handbook of Research on Artificial Intelligence in Goverment practices and processes*, Londres, IGI Global, 2022, pp. 226-242.
- Planells Boned, Francisco, "La reducción de las armas estratégicas", *Boletín de Información,* 168 (1983).
- Pulido, Guillermo, *Guerra multidominio y mosaico: el nuevo pensamiento militar estadounidense*, Madrid, Catarata, 2021.
- Saura, José Ramón, "How to use Artificial Intelligence in Education? Current insights and prospects for Goverment", en Saura, José Ramón y Debasa, Felipe, *Handbook of Research on Artificial Intelligence in Goverment practices and processes*, Londres, IGI Global, 2022, pp. 339-352.
- Saura, José Ramón et all "Ethical Design in Social Media: Assessing the main performance measurements of user online behavior modification", Journal of Business Research, 129, (2021).
- Sayle, Kelley, "Biometric Technologies and Global Security", *Congressional Research Service*, 2021.
- Takahashi, Sugio, *Counter A2/AD in Japan-US Defense Cooperation: Toward 'Allied Air-Sea Battle'*, Washington, Project 2049, 2012.
- Vaynman, Jane, "Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control", *Texas National Security Review*, 4/4 (2021).
- Wendehorst, Cristiane y Duller, *Yannic, Biometric Recognition and Behavioural Detection*, Bruselas, Policy Department for Citizens' Rights and Constitutional Affairs - European Parliament, 2021.
- Wilson, Lauren et al., "A systems approach to biometrics in the military domain", *Journal of forensic sciences*, 63/6 (2018), pp. 1858-1863.