Publicado en la página web del CEEEP

Fecha: 11 de enero de 2022

THINK TANK DEL EJÉRCITO DEL PERÚ

Inteligencia artificial en la Seguridad Nacional: Límites legales

Jean Carlo Cuba Yaranga, Psicólogo por la Universidad San Agustín de Arequipa, Abogado por la Universidad Católica de Santa María, Magister en Derechos Humanos por la Pontificia Universidad Católica del Perú, Especialización en Políticas Públicas para la igualdad en América Latina - Consejo Latinoamericano de Ciencias Sociales (CLACSO), Diploma en Gobernabilidad, Gerencia Política y Gestión Pública por la Pontificia Universidad Católica del Perú. Ha concluido la Maestría en Desarrollo y Defensa Nacional por el Centro de Altos Estudios Nacionales - Escuela de Postgrado.

Resumen

Términos como *big data*, mecatrónica y sensorización, toma de decisiones, computación neuromórfica y percepción por ordenador son algunos de los conceptos y tecnologías integrados a la Seguridad Nacional que se encuentran en constante evolución. Estos avances científicos cuentan con la legislación nacional e internacional existente como único límite para evitar su uso indiscriminado. En ese sentido, en este artículo se analizan los actuales y posibles usos de la Inteligencia Artificial como medios que se van sumando a distintas estrategias de ataque y defensa en el marco de la Seguridad Nacional, así como si la legislación existente para limitar su uso cumple con su finalidad.

Palabras claves: Inteligencia artificial, seguridad nacional, legislación nacional e internacional, inteligencia artificial en la seguridad nacional.

Introducción

En ciertos espacios de análisis es común buscar un meta-mensaje en cada evento o imagen, como suele suceder con las portadas de la revista inglesa de relaciones internacionales y economía, *The Economist*, la cual, en julio de 2020 publicó "*Hacia una nueva normalidad 2021–2030*". En este escrito, 50 expertos mundiales dedujeron cómo cambiaría la vida en la sociedad, basados en la tendencia actual y futura, y entre los 20 puntos tratados, consideraron la implantación de la Inteligencia Artificial (IA) en todo acto humano, desde temas domésticos hasta la toma de decisiones trascendentales por parte de los gobiernos. Esta información no puede pasar desapercibida, ya que los avances tecnológicos de los últimos años han acelerado lo que -para muchos especialistas- se consideraría una "Cuarta Revolución Industrial".

Estos cambios vienen afectando a todas las estructuras de la vida en comunidades humanas, que van desde el beneficio absoluto y controlado de los avances científicos hasta visiones apocalípticas en un futuro que sobrepasen la autonomía, dada su rapidez y eficiencia. Ante estas posibilidades, los países industrializados han iniciado discusiones sobre la influencia de la IA, incluyendo los primeros esbozos por normar o incluir pautas específicas para su uso por parte de los Estados en defensa de sus intereses.

En las actuales circunstancias, donde la seguridad se ha convertido en uno de los aspectos neurálgicos para el desarrollo, el Perú debe estar a la vanguardia y hacer uso de todo instrumento que permita garantizar la salvaguarda de la integridad de sus ciudadanos y cumplir con el objetivo de convivencia pacífica, siendo necesario replantear la existencia de límites legales en la utilización de la IA. De no existir requerimientos mínimos, el uso indiscriminado de IA podría atentar, directa o indirectamente, contra la dignidad del ciudadano (en temas como vida privada e intimidad) e incluso contra su integridad (armas con altos grados de autonomía), por lo cual es necesario prever las circunstancias cercanas.

En este sentido, en este artículo se expone el panorama general del uso de la IA en la Seguridad Nacional, incluyendo sus áreas de mayor desarrollo, y se analizan los criterios legales vigentes que limitan su uso, evaluando si estos tienden a ser eficaces frente a próximos eventos.

Inicio de la Cuarta Revolución Industrial

Académicos y especialistas señalan que, desde inicios del milenio actual, el mundo ha entrado a la primera fase de lo que denominan la "Cuarta Revolución Industrial". Al respecto, Klaus Schwab, fundador del Foro Económico Mundial, señala que esta nueva reestructuración del planeta se relaciona con el mundo digital y está caracterizada por "…*un internet más ubicuo y móvil, por sensores más pequeños y potentes que son cada vez más baratos, y por la inteligencia artificial y el aprendizaje de la máquina*" [1]. Frente a esta afirmación, António Manuel de Oliveira Guterres, Secretario General de la Organización de las Naciones Unidas, advirtió el año 2018 que el mundo aún no está preparado para la última revolución porque se acrecientan las posibilidades de caos social y el uso indiscriminado de IA en toda situación humana, lo que conllevaría a masas humanas sustituidas por máquinas más eficientes y al uso de armas autónomas sin restricción.

Siendo "el desarrollo de la IA" el eje de este proceso de transformación social, aparece un primer problema: conceptualizarla, por lo que existe un debate permanente para definirla ya que la sola mención de la palabra "inteligencia" la complica. Por ello, al hablar de IA existen elementos constantes que, si bien no dan como resultado una definición absoluta, si ayudan a enmarcar la idea.

Para Nicolas Miailhe y Cyrus Hodes, la IA es un conjunto de "agentes" (programas que se ejecutan en sistemas informáticos) capaces de aprender, adaptarse y desarrollarse en entornos dinámicos e inciertos[2]. En este sentido, la noción de inteligencia se suma a las de autonomía y adaptabilidad a través de la capacidad para aprender de un entorno dinámico. Oportunamente, la Red Iberoamericana de Protección de Datos, señala que, si bien no existe una única definición sobre IA, podría afirmarse que, en su concepción, se trata de un término "sombrilla", pues en él se incluyen distintas ideas y técnicas informáticas que van evolucionando, desde algoritmos hasta sistemas computacionales de *Deep* Learnig[3].

Por otra parte, la IA se puede categorizar en cuatro enfoques**:** (1) los sistemas que piensan como humanos (sistemas computacionales con información precedente que procesan con el objetivo de predecir eventos o conductas), (2) los sistemas que piensan racionalmente (con la semejanza de la lógica humana que es usada como alternativa para resolver problemas por medio de inferencias), (3) los sistemas que actúan como humanos (sistemas que pueden ejecutar funciones propias de los humanos y que requieren de inteligencia) y (4) los sistemas que actúan racionalmente (la llamada "singularidad tecnológica", máquinas con la capacidad de automatizar una conducta inteligente) [4].

La posibilidad de amplificación en las repercusiones del uso de la IA cada día se va convirtiendo en parte de la realidad, a tal grado que tanto países como organismos internacionales buscan hallar puntos conexos para regular el uso de la IA, entre los que resaltan la Organización de Naciones Unidas, la Unión Europea o la Organización para la Cooperación y el Desarrollo Económicos (OCDE) [5]. Por lo que existe un panorama en el que la IA se va haciendo omnipresente en varias áreas privadas y/o estatales como el de la Seguridad Nacional.

Inteligencia artificial en la Seguridad Nacional

En este contexto, existen varios escenarios públicos y privados en los cuales se vienen desarrollando las diversas técnicas de IA. Por ejemplo, en la temática estatal de las Políticas de Estado se considera de forma primordial a la Seguridad Nacional, la cual es definida por el Centro de Altos Estudios Nacionales como "…*la situación en la que el Estado tiene garantizada su existencia, presencia y vigencia, así como su soberanía, independencia e integridad territorial y de su patrimonio, sus intereses nacionales, su paz y estabilidad interna, para actuar con plena autoridad y libre de toda subordinación, frente a todo tipo de amenazas*" [6].

Considerando que es una obligación del Estado salvaguardar su soberanía, este debe contar con la mayor cantidad de recursos y tecnologías que permitan enfrentar todo tipo de amenazas. Es aquí en donde la IA constituye un factor gravitante por la rapidez y efectividad del resultado en el binomio de ataque – defensa, elemento básico de toda estrategia de protección de la Seguridad

Nacional. Por ello, en el caso del ataque se buscan resultados con nula o baja cantidad de efectos colaterales y en el caso de la defensa se prioriza el resguardo total del bien protegido; sin embargo, todo esto ya no se limita únicamente al plano físico, sino que abarca el campo virtual, por lo que aparece la figura de la ciberseguridad[7].

A nivel mundial, naciones y organizaciones supranacionales buscan desarrollar proyectos que generen nuevo conocimiento y contribuyan a mejorar la seguridad de los países, tanto en el plano particular de una dimensión como en el multidimensional o, como bien menciona el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), sobre el trinomio perfecto para balancear las acciones de la IA aplicada al campo militar: el factor lógico (referido al proceso de datos), el factor físico (armamento) y el factor humano (conocimiento continuo de la situación) [8].

Riesgos del uso de IA en aspectos referidos a la Seguridad Nacional

De los posibles riesgos del uso de la IA -en el contexto de la Seguridad Nacional- no se puede pasar por alto que el Perú es un país que adquiere tecnología externa y que, actualmente, en cuestiones tecnológicas existe una "carrera" entre dos potencias: la República Popular China y los Estados Unidos. Por un lado, las inversiones chinas pasan por clústeres que forman parte de una triangulación entre el apoyo del Estado, del partido y de las empresas privadas a fin de afianzar su presencia para el año 2035 y -diez años después- vencer a su principal rival. Por otro lado, Estados Unidos continúa liderando las investigaciones en este campo. No obstante, el resultado de tal "competencia" es incierto, aunque se podría afirmar que existirán monopolios regionales e información "flotante" en aspectos de Seguridad Nacional que se convertirán en vulnerabilidad al depender de otro Estado[9].

La posición del Perú como un país importador de tecnología lleva a la reflexión de que ningún acto o creación humana es infalible y, si se trata de nuevas tecnologías, el nivel de incertidumbre es alto. Esto no significa que -con el tiempo- dichos errores serán superados relativamente por la misma IA, que se caracteriza por su rápida evolución. Al respecto, en casos sobre protección de datos, la Red Iberoamericana de Protección de Datos encuentra dos riesgos esenciales: la preconfiguración del algoritmo y la calidad de la información. En el primer riesgo podría introducirse, consciente o inconscientemente, los prejuicios del creador, mientras que en el segundo riesgo, la forma como está programada la IA podría provocar generalidades en su procesamiento de datos que perjudicarían a terceros, sin dejar de lado que la IA podría también obtener datos falsos que sesgarían su desempeño[10].

En ese sentido, estos riesgos podrían ocurrir tanto en el acceso a información de baja calidad como por maniobras estratégicas de un adversario para sesgar su conducta. Situación que no se enmarca en mera especulación ya que los sistemas pueden fallar y, tanto los sesgos como los errores humanos (intencionales o no), pueden magnificar estas fallas con consecuencias catastróficas debido a que la IA lleva las amenazas al plano digital y de la información. De este modo, el uso de algoritmos modifica los escenarios de riesgo de seguridad para ciudadanos, organizaciones y Estados[11].

Otro riesgo a tener en cuenta es el nivel de vulnerabilidad de la IA a los ciberataques, lo que permitiría manipular el sistema remotamente y hacer que actúe de forma contraria a sus objetivos al encontrase "*hackeado*"; de esa manera, se obtendría ilegalmente información privada. Este riesgo se elevaría si se confía en un único algoritmo ya que también presenta riesgos asociados a la seguridad del código y, en caso de corromperse o verse alterado, podría dejar a organizaciones y Estados indefensos[12]. Desde otra perspectiva, se presenta la posibilidad en la cual los mismos responsables del manejo de la IA podrían hacer uso y abuso de sistemas a través de la ciber vigilancia como método de control social, o realizando campañas de desinformación debido a que dicho *software* tiene la capacidad de analizar ingentes cantidades de datos de ciudadanos o empresas, pudiéndose "perfilar" al elemento vigilado para fines ajenos al de la protección del Estado.

Legislación internacional y nacional

No se debe pensar en la IA como arma *per se* pues solo es un medio creado por el hombre para resolver determinadas tareas. Muy distinto es el uso que se haga de la misma al convertirla en un instrumento o intermediario sofisticado para el resguardo de la Seguridad Nacional, lo que lleva a la IA al campo del debate ético y, subsiguientemente, al legal.

En el aspecto legal se puede mencionar que posterior a la Segunda Guerra Mundial toda discusión que tratase de temas específicos sobre tecnología llamada "inteligencia" era muy lejana. Autores como José Luis Calvo Pérez tienen como debate primigenio del asunto a la "Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados", del 15 de septiembre de 1980[13]. Adicionalmente, se puede mencionar la "Clausula Martens", una declaración de principios en pro de la humanidad, siendo sus conclusiones aplicables de forma extensiva a situaciones similares[14].

Con el paso del tiempo y frente a las posibilidades de error, vulnerabilidad o mal uso de la IA, la preocupación por el rápido avance científico contra un ralentizado debate legal conduce a los Estados a buscar la ampliación o hacer más específica la regulación. Esta situación viene ocurriendo en la Unión Europea, donde se

percibe que el tema va rebasando los protocolos por la "carrera" entre los avances chinos y estadounidenses, evitando convertirse en una colonia tecnológica de cualquiera de las dos potencias[15]. Al respecto, la conclusión a la que llegó el análisis de la Escuela Politécnica Federal de Zurich es que un acuerdo global sobre el uso de la IA debe girar en base a cinco principios éticos: transparencia, justicia y equidad, no maleficencia, responsabilidad y privacidad. Sin embargo, este análisis subraya que existen desacuerdos sustanciales en la forma en que se interpretan estos principios, por qué se consideran importantes y cómo deben implementarse[16].

Adicionalmente, se debe recalcar que la regulación de la IA debe relacionarse con cuatro importantes ejes de base en el debate: (1) la caja negra (la regulación no debe generalizarse porque los algoritmos usados *"son cualitativamente distintos… gran parte del procesamiento, almacenamiento y uso de la información es realizado por el algoritmo mismo y de forma poco transparente dentro de una caja negra de procesamiento prácticamente inescrutable"*[17]), (2) los sesgos de los algoritmos (se encuentra relacionada al programador del sistema y los sesgos que podría programar o un algoritmo básicamente desarrollado que puede causar situaciones de discriminación), (3) la ética de selección (entendido como los casos en los cuales la máquina toma decisiones en un panorama conflictivo, que para un ser humano lo llevaría a un dilema moral, en el caso del sistema se debe definir quién, ante una situación así, sería el responsable) y (4) el manejo de la información (como los sistemas de *Big Data* que manejan y analizan grandes cantidades de datos en tiempo reducido, la regulación se debe centrar en *"cómo y a quiénes - personas u organizaciones- se les otorga el acceso a dichos datos. La información es poder y, en la actualidad, se deposita una carga excesiva sobre el individuo para administrar sus derechos de privacidad"*[18]).

Al respecto, los países con capacidad tecnológica que investigan y desarrollan la IA como arma o implemento de seguridad buscan limitar cualquier legislación que los afecte con el Derecho Internacional Humanitario porque, de darse mayor especificidad en la legislación, consideran sería un obstáculo a futuras investigaciones[19]. Sin embargo, António Guterres, Secretario General de la ONU, durante la Conferencia sobre tecnología en Lisboa, fue enfático al señalar que toda arma autónoma basada en IA debe ser proscrita por el Derecho Internacional, ya que si la IA tiene una función en pro de la humanidad existe la faceta en la cual el uso involucraría el remplazo de los hombres por las máquinas, consecuentemente (en el caso de la IA como arma autónoma) *"las armas […] tendrán la posibilidad de matar por sí mismas"* [20].

Respecto al caso peruano, es incipiente en lo referente a formular propuestas legislativas en temas relacionados a la IA en la Defensa y Seguridad Nacional. No obstante, sus avances se centran más en el tema de la Ciberseguridad; es decir, la IA no convertida en arma de guerra, sino como parte de los mecanismos de

defensa en el ciberespacio. Esto se corrobora en el "Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe", en donde se menciona que el Perú no cuenta con una Estrategia Nacional de Seguridad Cibernética, pero sí presenta avances en temas de Ciberseguridad[21].

En el año 2000, el Congreso de la República del Perú promulgó la "Ley que Incorpora los Delitos Informáticos al Código Penal - Ley N° 27309", la cual penaba a aquellos que transgredían, de algún modo, una base de datos; cinco años después, la Policía Nacional creó la División de Investigación de Delitos de Alta Tecnología (DIVINDAT). Posteriormente, en el año 2001, se promulgó la "Ley de Protección de Datos Personales - Ley N° 29733" con el objeto de garantizar el derecho fundamental a la protección de los datos personales; mientras que en el 2013 se actualizó la "Ley de Delitos Informáticos - Ley N° 30096" debido a que los sistemas y base de datos caían en un estado de vulneración frente a los nuevos ciberataques y que posiblemente vaya evolucionando con el avance de la ciencia y tecnología[22]. Finalmente, en el año 2019, se aprobó el dictamen del proyecto de Ley de Ciberseguridad que busca establecer el marco normativo en materia de seguridad digital en el Perú, y se promulgó una de las normas con mayor especificidad del tema, la "Ley de Ciberdefensa - Ley N° 30999" que regula "*las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley*". Con la citada norma, el Estado peruano puede realizar operaciones haciendo uso de sus fuerzas en el ciberespacio, amparándose siempre en la Carta de las Naciones Unidas (artículo 51°) y las disposiciones del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario[23].

Conclusiones

Por lo analizado, resulta claro señalar que se ha iniciado el proceso de adecuación a la denominada "Cuarta Revolución", aunque los especialistas señalan que el crecimiento exponencial de los avances tecnológicos versus al casi inexistente debate sobre la temática no permiten que el mundo esté preparado para dicho cambio social. La característica por antonomasia de la "Cuarta Revolución" es la presencia de la IA, la cual no tiene un concepto definitivo, pero hay aspectos que son base para definirla, tales y como la autonomía y la capacidad de adaptarse por medio del aprendizaje. En ese sentido, al ser las potencias industrializadas las que tienen el monopolio de la IA de última generación, países como el Perú se convierten en un "adquiriente cautivo" de la tecnología, lo que significa mayores costos en programación y actualización.

El debate internacional sobre la legalidad del uso de la IA cuando es empleada en armas autónomas suele estar a cargo de las potencias que la investigan y desarrollan y pretenden limitarlo a los principios del Derecho Internacional Humanitario; en cambio, en el área que implica IA sobre Ciberseguridad las normas

se van actualizando constantemente. En el caso peruano, desde el año 2000 se pretende estar a la vanguardia legislativa de los avances científicos, pero dirigidos especialmente al cuidado y penalidades contra la transgresión de base de datos.

Notas finales

[1] Klaus Schwab, "La Cuarta Revolución Industrial". (Madid: Penguin Random House, 2016), 13.

[2] Nicolas Miailhe y Cyrus Hodes. «La troisième ère de l'intelligence artificielle.» Comprendre l'essor de l'intelligence artificielle, Instituto Veolia Nicolas Miailhe Cyrus Hodes https://www.institut.veolia.org/sites/g/files/dvc2551/files/document/2018/03/Facts-AI-03_La_troisieme_ere_de_lintelligence_artificielle_-_Nicolas_Miailhe_Cyrus_Hodes.pdf (Consultado el 17 de mayo de 2021).

[3] Red Iberoamericana de Protección de Datos, «Recomendaciones generales para el tratamiento de Datos en la Inteligencia Artificial.», (Ministerio de Justicia y Derechos Humanos. 21 de junio de 2019). https://www.minjus.gob.pe/wp-content/uploads/2019/12/RECOMENDACIONES-GENERALES-PARA-EL-TRATAMIENTO-DE-DATOS-EN-LA-IA.pdf (consultado el 20 de mayo de 2021).

[4] Jairo Andrés Villalba Gómez, «Problemas bioéticos emergentes de la inteligencia artificial.» Diversitas: Perspectivas en Psicología (Universidad Santo Tomás) XII, nº 1 (Febrero 2016): 137 - 147.

[5] Por ejemplo, países como Canadá, China, Dinamarca, Estados Unidos, Francia, Finlandia, India, Italia, Japón, México, Singapur, Corea del Sur, Suecia, Taiwán, Emiratos Árabes, y el Reino Unido tienen planes nacionales sobre IA, véase María Belén Abdala, Santiago Lacroix Eussler, y Santiago Soubie. «La política de la Inteligencia Artificial: sus usos en el sector público y sus implicancias regulatorias.» (Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento. Octubre de 2019). https://www.cippec.org/wp-content/uploads/2019/10/185-DT-Abdala-Lacroix-y-Soubie-La-pol%C3%ADtica-de-la-Inteligencia-Artifici....pdf (consultado el 23 de junio de 2021).

[6] Centro de Altos Estudios Nacionales, "Líneas de investigación", (Centro de Altos Estudios Nacionales. 2019). https://www.caen.edu.pe/wordpress/direccion-de-investigacion/lineas-de-investigacion/ (consultado el 14 de junio de 2021).

[7] Abdala, Lacroix y Soubie. La política de la Inteligencia Artificial.

[8] En el mismo texto se analiza el caso de la European Defence Agency (EDA), que es la conjunción de profesionales de la especialidad en grupos llamados "CapTechs" (Capability Technology Group) que actualmente son doce, véase Centro Superior de Estudios de la Defensa Nacional (CESEDEN) «La inteligencia artificial aplicada a la defensa.» Centro Superior de Estudios de la Defensa Nacional. (Junio de 2018). http://www.ieee.es/Galerias/fichero/docs_trabajo/2019/DIEEET0-2018La_inteligencia_artificial.pdf (consultado el 14 de Junio de 2021).

[9] Joaquín Fournier Guimbao, «Inteligencia Artificial: una carrera hacia un futuro tecnológico.» (Instituto Español Estudios Estratégicos. 13 de julio de 2021). http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO89_2021_JOAFOU_Inteligencia.pdf (consultado el 4 de Agosto de 2021).

[10] Red Iberoamericana de Protección de Datos, Recomendaciones generales para el tratamiento de Datos en la Inteligencia Artificial.

[11] Abdala, Lacroix y Soubie. La política de la Inteligencia Artificial.

[12] Ibíd., 13.

[13] Esta Convención tiene sus orígenes en el año de 1968, año en que tanto el Secretario General de las Naciones Unidas como con organismos internacionales y el Comité Internacional de la Cruz Roja, tratarán sobre "la necesidad de prohibición y limitación del empleo de ciertos métodos y medios de guerra, y le pedía que tomara cualesquiera medidas que fueran necesarias para dar cumplimiento a las disposiciones de la resolución", véase Organización de Naciones Unidas, «Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados.» (United Nations Audiovisual Library of International Law. 15 de Septiembre de 1980). https://legal.un.org/avl/pdf/ha/cprccc/cprccc_ph_s.pdf (consultado el 28 de Julio de 2021).

[14] Basada en la declaración del delegado de Rusia en la Conferencia de la Paz de La Haya de 1899, von Martens, que en su versión original redactada en la Convención con respecto a las leyes de la guerra terrestre (la Haya II) del 29 de julio de 1899, se traduciría de la siguiente manera: "Mientras que se forma un Código más completo de las leyes de la guerra, las Altas Partes Contratantes juzgan oportuno declarar que, en los casos no comprendidos en las disposiciones reglamentarias adoptadas por ellas, las poblaciones y los beligerantes permanecen bajo la garantía y el régimen de los principios del Derecho de Gentes preconizados por los usos establecidos entre las naciones civilizadas, por las leyes de la humanidad y por las exigencias de la conciencia pública" véase Rupert Ticehurst, «La Cláusula de Martens y el derecho de los conflictos armados.» (Revista International de la Cruz Roja, 1996) 324 - 339.

[15] Fournier, «Inteligencia Artificial: una carrera hacia un futuro tecnológico.»

[16] Rafael De Asis, «Inteligencia Artificial y Derechos Humanos.», (E- Archivo de la Universidad Carlos III de Madrid. Abril de 2020). https://e-archivo.uc3m.es/bitstream/handle/10016/30453/WF-20-04.pdf?sequence=1&isAllowed=y (consultado el 16 de Junio de 2021).

[17] Abdala, Lacroix y Soubie. La política de la Inteligencia Artificial, 17.

[18] Ibíd.[19] José Luis Calvo Pérez, «Debate internacional en torno a los sistemas de armas autónomos letales. Consideraciones tecnológicas, jurídicas y éticas.» (Ministerio de Defensa - Armada Española. Revista general de marina 278, nº 3, 2020) 457 - 469.

[20] Su declaración fue la siguiente: "Como Secretario General de las Naciones Unidas mi preocupación es asegurarme que la ONU es capaz de apoyar las tecnologías de vanguardia para aprovechar al máximo su impacto positivo, tanto en las personas como en el planeta, y, a su vez, limitar su uso incorrecto", además de señalar que la "militarización de la inteligencia artificial representa un grave peligro…[porque] hará muy difícil evitar la escalada de conflictos y garantizar el respeto del derecho internacional humanitario en los campos de batalla". Finalizó señalando: "Las máquinas que tienen el poder y la discreción de quitar vidas humanas son políticamente inaceptables, son moralmente repugnantes y deben ser prohibidas por el derecho

internacional", véase Noticias ONU, "Las armas autónomas deben ser prohibidas en el derecho internacional" (Organización de Naciones Unidas, 5 de Noviembre de 2018). https://news.un.org/es/story/2018/11/1444982 (consultado el 16 de Junio de 2021).

[21] Banco Interamericano de Desarrollo; Organización de los Estados Americanos, «Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.», (Banco Interamericano de Desarrollo. Julio de 2020). https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf (consultado el 16 de Julio de 2021).

[22] El objeto de la Ley es "… garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen". Véase Ley de protección de datos personales - Ley N°29733 Congreso de la República, (El Peruano - Normas Legales. 21 de junio de 2011). https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf (consultado el16 de Julio de 2021).

[23] Artículo 51.- Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales, véase Organización de Naciones Unidas, «Carta de las Naciones Unidas.», (Naciones Unidas. 26 de junio de 1945). https://www.un.org/es/about-us/un-charter/chapter-7 (consultado el 23 de mayo de 2021).