

LA HUMANIZACIÓN DE LOS USOS Y DESARROLLOS TECNOLÓGICOS A TRAVÉS DE INTERACCIONES CON EL DERECHO INTERNACIONAL

THE HUMANIZATION OF TECHNOLOGICAL USES AND DEVELOPMENTS THROUGH INTERACTIONS WITH INTERNATIONAL LAW

Nicolás CARRILLO SANTARELLI

Resumen: la tecnología avanza con frecuencia a pasos tan agigantados que, para muchos, hacen al derecho internacional quedar rezagado. Esto sería especialmente preocupante en aquellos eventos en los que los usos de la tecnología pueden afectar o poner en riesgo el goce y ejercicio de derechos basados directamente en la dignidad humana, como podría acontecer con las armas autónomas, entre otras. Sin embargo, en el texto se argumenta que el derecho internacional dispone en sus distintas ramas de principios y criterios de interpretación que permiten, por una parte, considerar ilícitos los abusos con independencia del medio por el cual se cometan, incluso si es a través de la tecnología; y, además, dan cabida a la consideración de que las libertades y derechos fundamentales pueden ejercerse también en contextos tecnológicos, como por ejemplo acontece con internet y la libertad de expresión. Por otra parte, se argumenta que la tecnología también ofrece oportunidades y exigencias de protección, como ocurre en lo concerniente al suministro de alimentos y asistencia humanitaria por medio de *drones* o el rescate de personas en situación de riesgo con medios tecnológicos.

Palabras clave: derecho y tecnología; derechos humanos; dignidad humana; armas autónomas; libertad de expresión; asistencia humanitaria.

Abstract: technological developments often take place in such a fast pace that lead many to think that the law will inevitably lag behind. This would be especially worrisome when it comes to situations in which the uses of technology can affect or threaten the enjoyment of rights directly based on human dignity, as may happen in relation to the deployment of autonomous weapons, among others. Nonetheless, in this text it is argued that international law possesses principles and interpretation criteria in different branches that permit to consider abuses as wrongful regardless of how or through which means they are perpetrated; or that permit to protect the exercise of freedoms in technological contexts, as happens with freedom of expression on the internet. It is also explained how technology provides both opportunities and demands of protection, as in relation to the supply of food and humanitarian assistance through drones or the rescue of persons at risk with the help of technological advances.

Keywords: law and technology; human rights; human dignity; autonomous weapons; freedom of expression; humanitarian assistance.

Introducción

Los desarrollos tecnológicos avanzan en un ritmo vertiginoso, permitiendo operaciones que antes eran imposibles o mucho más costosas, lentas o ineficientes. Este incremento en la posibilidad de actuar puede ser aprovechado tanto por actores no estatales como por los Estados y sus agentes.¹ Las posibilidades adicionales o intensificadas facilitan en ocasiones el cumplimiento de compromisos jurídicos, aunque también pueden ofrecer tentaciones de realizar comportamientos ilícitos de forma sencilla o con altas posibilidades de eludir escrutinios, o de “relajar” las exigencias de los estándares internacionales. Por otra parte, la tecnología puede contribuir a acelerar cambios en la costumbre internacional sobre determinadas materias, como por ejemplo en lo relativo a la regulación del uso de la fuerza. Frente a todas estas posibilidades, debe asegurarse que el derecho ofrezca una regulación humanizada, que por una parte prohíba abusos que se prevalgan de la tecnología y, por la otra, oriente su desarrollo de forma coherente con el debido respeto a la dignidad humana.

Adicionalmente debe reconocerse que, en ocasiones, puede haber dudas sobre la licitud del uso, o incluso el desarrollo, de aplicaciones y herramientas tecnológicas. Esto hace que sea posible que se produzcan hechos ilícitos sin la presencia de mala fe al ignorarse que hay prohibiciones o, incluso, que algunos intenten aprovecharse de las ambigüedades de forma premeditada. También puede acontecer que las incertidumbres sobre las prescripciones jurídicas frenen desarrollos interesantes o que alienten implementaciones riesgosas.

En otras palabras, la tecnología ofrece oportunidades y genera riesgos y desafíos para la protección de bienes jurídicos e intereses internacionales, incluyendo los relativos a la protección del valor intrínseco de los seres humanos. En consecuencia, se ha de procurar que los desarrollos tecnológicos no tengan ineludiblemente, o con una altísima probabilidad, usos que sean inherentemente contrarios a protecciones humanitarias. Esta idea ha motivado la prohibición internacional de, por ejemplo, las armas químicas, minas antipersonal y municiones en racimo. Además de aquella dimensión prohibitiva,

¹ Es necesario examinar en concreto los factores que influyen y motivan el comportamiento de estos agentes, en tanto el Estado, por más que se conciba formalmente como una unidad, actúa *de facto* de forma desagregada. Ver: Eric A. Posner, *The Perils of Global Legalism*, The University of Chicago Press, 2009, págs. 40-41, 71.

también conviene regular el uso de tecnologías con un impacto potencial positivo o negativo. Después de todo, por lo *general*, salvo en aquellos casos de desarrollos que inherente o ineludiblemente contraríen a la protección de la dignidad humana, será el *uso* concreto de desarrollos tecnológicos el que en últimas adolezca de ilicitud o se considere permitido o tolerado por el derecho.²

Estas consideraciones se basan en la idea de que es importante evitar que el derecho “se arrodille” o tan sólo tome nota de *fait accompli*.³ El derecho puede tener un papel crucial como factor de promoción de usos, implementaciones y desarrollos tecnológicos que faciliten y hagan más eficiente la asistencia humanitaria y la protección del goce y ejercicio de los derechos humanos. Con base en esta idea, el presente capítulo tiene el propósito de examinar qué procesos jurídicos pueden y deben emplearse para proteger la dignidad humana frente a (y aprovechándose de) la tecnología, entendiendo como proceso jurídico a toda dinámica de interacción con el derecho internacional, en lugar de optar por un significado referente a procedimientos formales. Conviene tener en cuenta que hay múltiples procesos jurídicos, que no se limitan a la adopción de normas o a su aplicación judicial, y que los procesos jurídicos se usan y pueden usarse en la práctica para perseguir determinados propósitos y políticas (que no son necesariamente legítimas), siendo crucial procurar que persigan la defensa de los derechos humanos.⁴

² Vid. Kenneth Anderson et al., “Adapting the Law of Armed Conflict to Autonomous Weapon Systems”, *International Law Studies*, Vol. 90, 2014, págs. 393, 395, 406-407, 411.

³ Ver el video del panel de discusión sobre *Drones* en el Consejo de Derechos Humanos del 22 de septiembre de 2014, donde se dijo que “the law should not follow drones, drones should follow the law”: “Panel discussion on Drones - 28th Meeting 28th Regular Session of Human Rights Council”, disponible en: <http://webtv.un.org/search/panel-discussion-on-drones-28th-meeting-28th-regular-session-of-human-rights-council/3798750531001?term=drones> (última visita: 13 de noviembre de 2014).

⁴ Sobre la noción de procesos jurídicos y una aproximación política a los mismos, ver: Myres S. McDougal y Harold D. Lasswell, “The Identification and Appraisal of Diverse Systems of Public Order”, *The American Journal of International Law*, Vol. 53, 1959; Myres S. McDougal, “Some basic theoretical concepts about international law: a policy-oriented framework of inquiry”, *The Journal of Conflict Resolution*, Vol. IV, 1960 (aunque creo que es adecuado intentar buscar objetivos de protección por medio del derecho y sus procesos, reconociendo límites y barreras cuando las haya para advertir la necesidad sobre su cambio y tener discusiones honestas sobre la conveniencia de éste, no comparto la concepción que percibo un tanto politizada en el contexto de la guerra fría de los derechos que parece entrecerarse en algún apartado de los textos citados, aunque sí es acertada su observación sobre contradicciones entre principios y valores del sistema internacional).

Para analizar lo referente a la posibilidad de emplear procesos jurídicos con el fin de humanizar la respuesta del derecho al uso y desarrollo de tecnologías, se analizará que procesos pueden emplearse frente a casos y cuestiones discutidos en la práctica, como en lo concerniente al uso de *drones* en operaciones tanto militares como civiles; las preguntas sobre la licitud de responder en legítima defensa a acciones cibernéticas; el ejercicio de derechos humanos en internet; la protección frente a agresiones que se aprovechen de la tecnología, incluyendo al *cyberbullying*; y la lucha contra iniciativas como el reclutamiento de personas dispuestas a cometer actos de terrorismo y otras conductas ilícitas en internet. Sobra decir que este texto ofrece ejemplos sobre procesos que pueden lidiar con determinados asuntos, sin que pueda considerarse que lo hace de forma o exhaustiva reduccionista en el sentido de sugerir que sólo existen esos casos o que la única respuesta posible es la relacionada con el proceso jurídico que se mencionará, pues en la práctica habrá muchas sutilezas y se requiere la complementariedad de procesos e iniciativas, incluyendo las no jurídicas, para alcanzar una protección efectiva de los seres humanos.

La primera sección de este texto se dedica al análisis de procesos jurídicos relacionados con aspectos normativos o de regulación, a saber: si es necesario o conveniente regular de forma expresa o concreta determinados usos y desarrollos tecnológicos que puedan generar desafíos u ofrecer oportunidades para la protección efectiva e integral de los derechos humanos o si, por el contrario, es posible o suficiente acudir a principios y reglas existentes y al *soft law* (entendido como *soft instrumentum*)⁵ de forma definitiva o transitoria (mientras se desarrollan de forma progresiva normas consideradas indispensables o aconsejables). Posteriormente, la segunda sección se ocupa de procesos jurídicos distintos a los relativos a la *creación o identificación* del derecho aplicable, analizándose en ella procesos y dinámicas de *aplicación y garantía* del derecho internacional, como por ejemplo las relacionadas con recursos de reclamación y reparación, para buscar la protección de víctimas actuales y potenciales;⁶ la promoción

⁵ Vid. Jean d'Aspremont, "Softness in International Law: A Self-Serving Quest for New Legal Materials", *European Journal of International Law*, Vol. 19, 2008, págs. 1081-1084.

⁶ Sobre la protección de víctimas potenciales, ver: Carlos M. Ayala Corao, "La ejecución de las sentencias de la Corte Interamericana de Derechos Humanos", Año 5, Nº 1, 2007, pág. 129; Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-21/14, *Derechos y garantías de niñas y*

de consideraciones humanitarias y el que se evite apoyar abusos que se sirvan de la tecnología y de ambigüedades jurídicas.

1. Identificación y regulación de principios y reglas internacionales para exigir un uso de la tecnología respetuoso de la dignidad humana

En líneas generales, esta sección estudia los procesos jurídicos a los que se puede (y debe) acudir para buscar la compatibilidad del posicionamiento de la regulación interna e internacional frente al uso de las nuevas tecnologías con valores y principios sobre derechos humanos, entendiendo por aquellos todos los reconocidos directamente a favor de los individuos que estén fundados en la dignidad humana. En ocasiones, esto será posible mediante la *identificación* de principios y reglas ya existentes que, incluso sin regular el uso de las tecnologías de forma concreta (quizás por no haber podido anticiparlas), permiten obtener aquel propósito gracias a una interpretación evolutiva o contextualizada, que por ejemplo permita entender como prohibidos determinados usos o desarrollos por estimarlos como contrarios a derechos humanos, incluyendo las libertades de expresión, pensamiento y la privacidad en sus manifestaciones en internet.

Seguidamente, se destaca cómo en ocasiones puede ser necesario o conveniente desarrollar una *regulación* que se dedique a las tecnologías de forma directa y teniendo en cuenta sus particularidades (hasta que ello se logre, será necesario aplicar la *lex lata* con interpretaciones teleológicas que busquen asegurar el respeto de la dignidad humana), bien porque hay ambigüedad en el derecho positivo existente en relación con las tecnologías en sí, o porque nos enfrentamos a situaciones complejas en las que puede usarse la tecnología y no hay claridad o se han presentado debates sobre la existencia o el contenido de la regulación internacional, no necesariamente estando aquellas discusiones por la tecnología (como, por ejemplo, en lo referente a la legítima defensa con *drones* contra actores no estatales ubicados en el territorio de un tercer Estado o al uso y desarrollo de armas autónomas); o porque se estima que es preferible disponer de reglas concretas y especiales para evitar contradicciones u ofrecer

niños en el contexto de la migración y/o en necesidad de protección internacional, 19 de agosto de 2014, párrs. 92, 106 y pie de página 72 en esa opinión.

estándares técnicamente idóneos o claros (por ejemplo, para regular el uso de vehículos aéreos no tripulados con tareas civiles). Esta sección se ocupa, entonces, de la diáda interpretación y regulación (desarrollo progresivo).

a. La identificación de normas y principios vinculantes o de *soft law* aplicables o pertinentes para exigir un uso de la tecnología respetuoso de los derechos humanos

De forma preliminar, es necesario advertir que, en ocasiones, puede resultar extremadamente conveniente o indispensable regular cuestiones relativas a la tecnología, por ejemplo para prohibir determinados desarrollos o usos tecnológicos considerados (por la sociedad civil que presiona, los sujetos negociadores, por participantes en formación de costumbre o por promotores de normas) intrínsecamente, o de forma potencial, como contrarios a postulados de la protección de la dignidad humana, en tanto faciliten, intensifiquen, se usen en o habiliten⁷ la contravención de los intereses y bienes jurídicos protegidos. No obstante, las dificultades relativas al tiempo o a las gestiones necesarias para conseguir acuerdos en determinada materia pueden hacer que los procesos para crear o declarar normas pertinentes sean, en ocasiones, inviables o demasiado tortuosos. Aquellas dificultades pueden obedecer, quizás, a actitudes reacias que desdeñen la protección de “los otros” (los extranjeros, los pobres y marginados) o al secretismo de quienes se benefician de la tecnología a pesar de que se use en detrimento de otros, lo que puede llevarles a preferir (de forma cuestionable) ambigüedades normativas o regulaciones laxas.

En consecuencia, si hay dificultades para crear normas, mientras (si) se superan obstáculos de negociación y oposición de quienes se aprovechan de la tecnología de

⁷ Los criterios de habilitación, intensificación o facilitación o uso son tenidos en cuenta en otros contextos, como el relativo a la complicidad en violaciones de derechos humanos, al considerarse que quien actúa según ellos en conexión con una violación puede ser responsable por complicidad. Vid. Comisión Internacional de Juristas, *Complicidad empresarial y responsabilidad legal: Volumen 1, Afrontar los hechos y establecer un camino legal*, Informe del Panel de Expertos Juristas sobre Complicidad Empresarial en Crímenes Internacionales, Ginebra, 2010, págs. 11-17; Jennifer Zerk, “Corporate liability for gross human rights abuses: Towards a fairer and more effective system of domestic law remedies”, *Report prepared for the Office of the UN High Commissioner for Human Rights*, págs. 8 y 16.

forma cuestionable con usos cuya licitud es dudosa, y para evitar situaciones de *non liquet e* impunidad,⁸ es posible, necesario y conveniente acudir al derecho existente de forma ingeniosa y permitida (incluyendo a los principios generales del derecho que, como señaló el juez Cançado en su opinión frente al caso *Pulp Mills* de la Corte Internacional de Justicia, pueden tener aplicabilidad directa en ocasiones), teniendo en cuenta criterios como los que se expondrán más adelante. En primer lugar, teniendo en cuenta que la interpretación teleológica es un componente de la regla general de interpretación de normas internacionales (como se desprende del artículo 31 de la Convención de Viena sobre el Derecho de los Tratados), ha de efectuarse una interpretación que procure la protección efectiva de la dignidad humana en ámbitos o frente a usos tecnológicos. Por otra parte, deben ser tenidos en cuenta postulados y principios básicos del derecho internacional de los derechos humanos, como por ejemplo la prohibición de la discriminación, el principio *pro personae* o *pro homine* y la prevalencia de las normas y dimensiones sobre derechos humanos que sean imperativas sobre toda manifestación fáctica o normativa contraria a ellas, a la que se priva de efectividad (y, cuando la contradicción es insalvable, de validez o vigencia).⁹ Como mínimo, aquellos (y otros) criterios han de guiar la interpretación de toda norma que sea pertinente examinar a la hora de indagar si un comportamiento, situación o uso relacionado con el desarrollo o empleo de herramientas o aplicaciones tecnológicas puede suponer una amenaza para el goce y ejercicio de los derechos humanos, caso en el cual adolecerá de ilicitud de forma implícita.

Un corolario de los anteriores criterios, ampliamente reconocido en el derecho internacional de los derechos humanos, es el considerar que las normas deben ser interpretadas de forma evolutiva para responder a desafíos actuales (tarea que se facilita

⁸ El derecho internacional de los derechos humanos exige combatir la impunidad. Ver: Declaración y Programa de Acción de Viena, Aprobados por la Conferencia Mundial de Derechos Humanos el 25 de junio de 1993, párrs. II.60 y II.91.

⁹ Vid. Tribunal Internacional para juzgar a los presuntos responsables de graves violaciones del derecho internacional humanitario cometidas en el territorio de la ex-Yugoslavia a partir de 1991, *Prosecutor v. Anto Furundzija*, Sentencia, 10 de diciembre de 1998, párrs. 153-156; artículos 53 y 64 de la Convención de Viena sobre el Derecho de los Tratados.

por la amplitud de muchas de sus normas),¹⁰ teniendo en cuenta desarrollos al interior de determinado régimen del derecho internacional y en otros ámbitos del derecho internacional¹¹.

Como ejemplos de los anteriores lineamientos, puede señalarse en un primer lugar que el Comité de Derechos Humanos manifestó de forma enfática en su Observación general número 34, sobre las libertades de opinión y expresión, que ella protege las expresiones en cualquier forma y por cualquier medio, incluyendo los medios electrónicos e internet, a través de los cuales cualquier persona puede manifestarse. Por esta razón, el Comité consideró que no se deben limitar aquellas expresiones, a no ser que se pueda realizar una restricción admisible según las normas internacionales sobre derechos humanos; y que los derechos internos deben ser compatibles con aquellas exigencias. Por su parte, la Comisión Interamericana de Derechos Humanos, como se manifiesta en un informe temático sobre el tema, ha considerado que derechos y libertades como la libertad de expresión pueden ejercerse en internet, y ha valorado como positivo el que las manifestaciones de aquel ejercicio puedan tener dinámicas democratizadoras y efectos positivos en la efectividad del goce de los derechos humanos. Más aún, la protección de aquellos derechos y libertades ejercidos *online* es apremiante: tal ejercicio posibilita iniciativas de activismo o control al Estado, y tristemente en la práctica tanto entes estatales como no estatales han agredido seriamente a quienes las ejercen, como reflejan, por ejemplo, crueles asesinatos de *bloggers* en Bangladesh.¹² Hacer hincapié en los procesos de identificación y *garantía* de la libertad de expresión en uno de los ámbitos en los que se puede verter, a saber, en internet, no es baladí: hay que tener en cuenta que distintos gobiernos y Estados han adoptado y empleado medidas para coartar su ejercicio en internet y que se considera

¹⁰ Corte Interamericana de Derechos Humanos, *Caso de los "Niños de la calle" (Villagrán Morales y otros) Vs. Guatemala*, Sentencia, 19 de noviembre de 1999, párr. 193; Eric A. Posner, *The Twilight of Human Rights Law*, Oxford University Press, 2014, págs. 95-97.

¹¹ Vid. Tribunal Europeo de Derechos Humanos, *Caso Al-Adsani Vs. el Reino Unido*, Sentencia, 21 de noviembre de 2001, párr. 55.

¹² Comité de Derechos Humanos, Observación general N° 34, *Artículo 19: Libertad de opinión y libertad de expresión*, CCPR/C/GC/34, 12 de septiembre de 2011, párrs. 12, 15, 39, 43 y 44; Comisión Interamericana de Derechos Humanos, *Libertad de expresión e internet*, OEA/SER.L/V/II.CIDH/RELE/INF.11/13, 31 de diciembre de 2013, párrs. 1-2, 10-13; Ishaan Tharoor, "Islamists hack another blogger to death in Bangladesh", *The Washington Post*, 30 de marzo de 2015.

que su goce ha empeorado en muchos lugares. Por estos motivos, es útil que se recuerde que las normas internas que pretendan limitar contenidos en redes sociales y realizar restricciones deben ser compatibles con criterios y estándares internacionales, como los relativos a la libertad de expresión o a la privacidad, al ser suficiente el derecho interno para asegurar estas exigencias.¹³

Por otra parte, en relación con los posibles usos positivos de la tecnología desde una perspectiva de derechos humanos (incluso en relación con la libertad de expresión y con controles sociales del Estado), puede mencionarse como ejemplo el hecho de que el uso de internet y sus herramientas y aplicaciones facilita la denuncia de abusos estatales y no estatales,¹⁴ la adquisición de información, la organización de campañas e iniciativas de promoción de derechos humanos¹⁵ o el intercambio de ideas. Estas posibilidades ofrecen un gran potencial democratizador y de participación política y no se relacionan únicamente con la libertad de expresión en sus dimensiones tanto individual como social sino, además, con el derecho a la educación (que puede ser promovido por diversos medios, como demuestran cursos *online* o conferencias y audiencias exhibidas en *streaming* o almacenadas en páginas web) o con el derecho a participar en la vida cultural por medio de la expresión y comunicaciones en internet u otros medios, entre otros derechos. Incluso los videojuegos pueden servir para sensibilizar o *educar* sobre el derecho internacional humanitario (en adelante, DIH) y otros regímenes del derecho internacional, incrementando la probabilidad de su implementación y recepción o

¹³ Vid. Comisión de Derecho Internacional, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001, artículos 3 y 32; Vauhini Vara, "The World Cracks Down on the Internet", *The New Yorker*, 4 de diciembre de 2014, disponible en: http://www.newyorker.com/tech/elements/world-cracks-internet?mbid=social_facebook (última visita: 12 de diciembre de 2014); Caitlin Dewey, "Two weeks after Zuckerberg said 'je suis Charlie,' Facebook begins censoring images of prophet Muhammad", *The Washington Post*, 27 de enero de 2015; Simon Denyer, "Is this North Korea? Chinese netizens squirm as party tightens grip on Internet", *The Washington Post*, 29 de enero de 2015.

¹⁴ Vid. Vanessa H. Larson, "This Mysterious Twitter User Predicts Turkish Government Crackdowns", *Foreign Policy*, 16 de diciembre de 2014, disponible en: http://foreignpolicy.com/2014/12/16/this_mysterious_twitter_user_predicts_turkish_government_crackdowns/?utm_source=Sailthru&utm_medium=email&utm_term=%2AEditors%20Picks&utm_campaign=2014_EditorsPicks_Promo%20NYURS16%2F12 (última visita: 18 de diciembre de 2014).

¹⁵ Vid. Hahrie Han, "Put the debate about slacktivism to rest", *OUPblog*, 19 de noviembre de 2014, disponible en: http://blog.oup.com/2014/11/slacktivism-digital-activism-high-engagement-organizations/?utm_source=facebook&utm_medium=oupacademic&utm_campaign=oupblog (última visita: 22 de diciembre de 2014).

internalización merced a la difusión sobre estándares internacionales.¹⁶ Estas razones pueden explicar por qué regímenes abusivos implementan controles o restricciones a actividades de la índole descrita, quizá temerosos de la exposición mediática de hechos ilícitos o de cuestionamientos a su “sabiduría”.

Otro ejemplo interesante se encuentra en el informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre “El derecho a la privacidad en la era digital”. En él se señala precisamente que internet y los desarrollos tecnológicos permiten potenciar la democratización, el intercambio de ideas y la promoción de derechos humanos. Debe destacarse que en el informe también se indica que en internet hay riesgos de que entes estatales y no estatales cometan abusos e interceptaciones que constituyan “injerencias arbitrarias o ilegales en el derecho a la privacidad”.

En aquel informe también se observa, de forma acertada, que las empresas privadas pueden ser cómplices o participantes en violaciones de derechos humanos que se prevalgan de la tecnología, que pueden estar relacionadas, entre otras posibilidades, con aspectos sobre inteligencia artificial (por ejemplo, sobre espionaje, identificación de datos y personas, vigilancia, etc.), automatización (de armas u otros elementos), *gig economy* o libertad digital, incluyendo este último ámbito el derecho a la privacidad en el contexto de internet (siguiendo órdenes estatal o sin ellas), según se puso de manifiesto con el escándalo de Facebook y Cambridge Analytica. Por esta razón, y para evitar que sus actividades tengan un impacto negativo sobre el goce y ejercicio de los derechos humanos, para respetar el contenido y los principios del derecho internacional de los derechos humanos las empresas deberán, por ejemplo, anunciar al público y a las

¹⁶ Vid. Corte Interamericana de Derechos Humanos, *Caso “La Última Tentación de Cristo” (Olmedo Bustos y otros) vs. Chile*, Sentencia, 5 de febrero de 2001, párrs. 64-68; artículos 13.2.b y 13.2.c del Pacto Internacional de Derechos Económicos, Sociales y Culturales y 13.3.b y 13.3.c del Protocolo adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales (“Protocolo de San Salvador”); Comité de Derechos Humanos Económicos, Sociales y Culturales, Observación General N° 21, *Derechos de toda persona a participar en la vida cultural (artículo 15, párrafo 1 a), del Pacto Internacional de Derechos Económicos, Sociales y Culturales*, E/C.12/GC/21/Rev.1, 17 de mayo de 2010, párr. 32; Nicolás Carrillo Santarelli, “La influencia “artística” de las emociones y la empatía en el contenido, la interpretación y la efectividad del derecho internacional”, *Anuario Mexicano de Derecho Internacional*, Vol. XVII, 2017, pp. 97-98.

autoridades pertinentes (por ejemplo, judiciales) sobre posibles incompatibilidades y riesgos e interpretar de la forma más restringida posible peticiones del Estado que puedan ser problemáticas, con el fin de evitar que se vulnere el derecho a la privacidad (u otros, puede añadirse).¹⁷ Estos llamados se hacen invocando, entre otras consideraciones, los Principios Rectores sobre las empresas y los derechos humanos, cuyo componente del deber empresarial de respeto de los derechos humanos tiene, curiosamente, y *según ellos*, una naturaleza preponderantemente voluntaria o de responsabilidad social corporativa. No obstante, algunos consideramos que las empresas y otros entes no estatales sí tienen algunas obligaciones internacionales, como la de respetar normas de *ius cogens* y el deber de no participar en crímenes internacionales (por ejemplo, como cómplices). Por otra parte, admitiendo que esta es una interpretación probablemente controvertida, considero que la alusión a *empresas* y derechos humanos en desarrollos contemporáneos hace posible considerar que quienes se dedican a actividades y negocios ilícitos, sin perjuicio de su responsabilidad independiente por tal motivo, pueden ver generada a su cargo una responsabilidad adicional cuando vulnere derechos humanos con sus actividades, incluyendo aquellas relacionadas con desarrollos y usos tecnológicos, por lo cual *hackers* y otros pueden estar obligados por los estándares mínimos aquí identificados y por otros que surjan con un desarrollo progresivo.¹⁸

¹⁷ Consejo de Derechos Humanos de las Naciones Unidas, *El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, A/HRC/27/37, 30 de junio de 2014, párrs. 1-5, 42-45, 47, 49-51; “Technology and human rights”, *Business & Human Rights Resource Centre*, disponible en: <https://www.business-humanrights.org/en/technology-and-human-rights> (última visita: 15 de julio de 2014), en donde se mencionan los cuatro ámbitos de relación entre empresas, tecnología y derechos humanos mencionados en el texto principal; “Facebook to face lawsuits alleging failure to protect users’ personal information over Cambridge Analytica data breach”, *Business & Human Rights Resource Centre*, disponible en: <https://www.business-humanrights.org/en/facebook-to-face-lawsuits-alleging-failure-to-protect-users-personal-information-over-cambridge-analytica-data-breach> (última visita: 15 de julio de 2018).

¹⁸ Vid. John H. Knox, “The Human Rights Council Endorses “Guiding Principles” for Corporations”, *ASIL Insights*, Vol. 15, 2011; Roland Portmann, *Legal Personality in International Law*, Cambridge University Press, 2010, pág. 166; Edmund F. Byrne, “Business Ethics Should Study Illicit Businesses: To Advance Respect for Human Rights”, *Journal of Business Ethics*, Vol. 103, 2011; Mark Klamberg, “The Legality of Rebel Courts during Non-International Armed Conflicts”, *Journal of International Criminal Justice*, Vol. 16, 2018, pág. 7 (con una discusión análoga sobre cómo incluso si no hay permisibilidad de detenciones no estatales durante conflictos armados, ellas no necesariamente tienen determina gravedad, que sí puede generarse si incurrir en otras conductas, lo cual pone de manifiesto que puede haber distintas conductas relacionadas con ilicitud independiente, siendo unas más graves que otras *ocasiones*).

Los dos ejemplos citados ilustran cómo en múltiples oportunidades una interpretación humanizada y actualizada a escenarios contemporáneos del derecho existente permite identificar comportamientos recomendados (como sucede frente a las empresas), de riesgo y prohibidos (como violaciones cometidas por orden estatal), además de estándares que deben seguir todos los actores que potencialmente puedan actuar en contra de los derechos humanos en un entorno cibernético o con medios tecnológicos.

Por este motivo, es importante identificar conductas potencialmente lesivas para desprender sus consecuencias regulatorias, que pueden incluso estar ya presentes en el derecho positivo (cuando ello no sea el caso, debe efectuarse una regulación *de lege ferenda*). Por ejemplo, una serie de conductas que por su relevancia negativa merecen ser enfrentadas se relacionan con la capacidad de los Estados o grupos armados no estatales para adquirir, alterar, manipular o “hackear”¹⁹ determinados medios o aparatos, como vehículos aéreos no tripulados o *drones*. En estos casos, debe insistirse en que aquellos entes tienen un deber de respeto, bien sea reconocido expresamente (ej. de los Estados o grupos que participan en conflictos armados) o presente de forma implícita,²⁰ que les exige abstenerse de violar mediante el uso, obtención o fabricación de aquellos instrumentos, según el caso, normas y bienes jurídicos internacionales que protejan de forma directa o indirecta a los derechos humanos, entre las que se incluyen aquellas que regulan y prohíben el uso de la fuerza armada.²¹ Un ejemplo de lo anterior se ilustra con la amenaza de que Corea del Norte ataque a Corea del Sur u otros Estados y poblaciones con armas nucleares o con *drones* que, a pesar de no ser sofisticados en comparación con aquellos que poseen otros actores, puedan en todo caso generar daños significativos (siendo siempre es relevante la afectación de derechos humanos).²²

¹⁹ Ver, por ejemplo, “German Heron Drone Hacked and Crashed by Taliban in Afghanistan”, *The Aviationist* (Blog), 13 de noviembre de 2013, disponible en: <http://theaviationist.com/2013/11/13/heron-hacked-afghanistan/> (última visita: 7 de noviembre de 2014).

²⁰ Vid. Jordan J. Paust, “The Reality of Private Rights, Duties, and Participation in the International Legal Process”, *Michigan Journal of International Law*, Vol. 25, 2004, págs. 1242-1243.

²¹ Vid. Stephan Hobe, “Individuals and Groups as Global Actors: The Denationalization of International Transactions”, in Rainer Hofmann (ed.), *Non-State Actors as New Subjects of International Law*, Duncker & Humblot (ed.), 1999, págs. 121-122.

²² Ver Van Jackson, “Kim Jong Un’s Tin Can Air Force”, *Foreign Policy*, 11 de noviembre de 2014, disponible en: http://www.foreignpolicy.com/articles/2014/11/11/north_korea_drones_kim_jong_un_seoul_tin_can_bo

A la luz de las anteriores consideraciones, se debe enfatizar que los abusos potenciales o actuales que se faciliten o realicen por medio de la tecnología no son necesariamente estatales. Al respecto, los debates sobre si hay obligaciones no estatales en materia de derechos humanos, y la existencia fáctica de abusos atribuibles a entes no estatales, ponen de relieve que la protección de la dignidad humana frente a determinados desarrollos y usos tecnológicos no será completa a no ser que se ofrezca y exija respeto frente a cualquier violador potencial, estatal o no, poderoso (en términos bélicos, económicos, etc.) o no. Además, es importante para las empresas que prestan servicios tecnológicos contar con personal que se encargue de la debida diligencia para evitar impactos negativos sobre el goce y ejercicio de derechos humanos. Todo esto es así tanto por la posibilidad fáctica de que cualquiera de los actores no estatales, incluso de forma aislada, participe en una violación, lo que hace importante ofrecer a las víctimas medios y recursos para defenderse si no es suficiente o efectiva la protección interna; como por el hecho de que la protección de la dignidad es incondicional²³ y, en consecuencia, no depende de la identidad del agresor. Es pertinente mencionar que, aunque son insuficientes de forma aislada para asegurar la protección de los individuos, no debe desdeñarse el impacto positivo que pueden tener posibles iniciativas voluntarias (como la adopción de códigos de conducta o el empleo de personas que eviten la comisión de hechos ilícitos), no vinculantes y de *soft law*, como los Principios Rectores sobre las empresas y los derechos humanos, dirigidos a los Estados o actores no estatales, en relación con la tecnología. Esto se explica en tanto aquellos estándares, así como las normas vinculantes, pueden tener efectos y funciones educativas y expresivas o simbólicas (con un posible respaldo del derecho positivo y sus mecanismos en el caso del *hard law*) e incluso cierto impacto sobre presiones frente a las actitudes y cultura de sus destinatarios, que se facilita si han sido aceptadas por los destinatarios respectivos

[mb_deadly?utm_content=buffer9ac10&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer](#) (última visita: 13 de noviembre de 2014).

²³ Sobre la incondicionalidad de la dignidad humana, vid. Andrew Clapham, *Human Rights Obligations of Non-State Actors*, Oxford University Press, 2006, pág. 56; Oliver Sensen, “Human Dignity in Historical Perspective: The Contemporary and Traditional Paradigms”, *European Journal of Political Theory*, Vol. 10, 2011. Acerca del empleo de personas que garanticen que las actividades de empresas sobre tecnología respeten estándares de derechos humanos, ver Henry Farrell, “The New Economy’s Old Business Model is Dead”, *Foreign Policy*, 13 de julio de 2018.

y/o por los *stakeholders* que se beneficiarían de su observancia, lo que los dotaría de legitimidad procesal. La insuficiencia de las estrategias voluntarias se explica por la consideración de que su incumplimiento no genera directamente responsabilidad u otras consecuencias jurídicas, por el hecho de que en ocasiones pueden adoptarse e únicamente para perseguir fines estratégicos, y por la frecuente ausencia de acceso a recursos efectivos de protección cuando son violadas. No obstante, se puede recomendar su adopción como complemento a estrategias de protección basadas en normas vinculantes.

Como se examinará en la segunda sección de este texto, la posibilidad de acudir a principios y normas de *lex lata* de forma evolutiva, para hacer frente a desafíos y desarrollos tecnológicos actuales, no sirve únicamente para identificar normas aplicables que protejan derechos humanos, sino que además permite guiar la acción de las autoridades y la interpretación de normas de forma que se procure aquella protección, por ejemplo para proteger a las víctimas de agresiones en espacios cibernéticos.

b. Procesos de avergonzamiento, codificación y desarrollo progresivo del derecho internacional para proteger derechos humanos frente a actores que usan desarrollos y aplicaciones tecnológicas de forma lesiva

Es necesario indagar si es posible recurrir a la *lex lata* para proteger la dignidad humana frente a desafíos tecnológicos, pero el derecho positivo puede ser, en ocasiones, insuficiente. Ello puede deberse, entre otras posibilidades, a las siguientes razones: (1) a una eventual necesidad de ofrecer reglas *precisas* que respondan de forma concreta a exigencias de que se regule el uso de determinadas tecnologías teniendo en cuenta sus características concretas, por ejemplo para ofrecer normas sobre su uso eficiente con determinados parámetros de seguridad; o (2) a la presencia en el derecho internacional de vacíos o dudas considerables, no resueltas con *auctoritas*, que pueden ser explotados o puestos de manifiesto por la práctica de quienes usan la tecnología de determinada manera, contexto en el que se incrementa o facilita la posibilidad de que se incurra en conductas que se sirvan de la tecnología cuya legalidad o impacto en los derechos

humanos sea incierto o controvertido, lo que exige una respuesta clarificadora de cara al futuro y a favor de las eventuales víctimas.

En los anteriores supuestos, es aconsejable adoptar regulaciones que regulen adecuadamente la situación para impedir que determinada práctica que pueda ser contraria al proceso de humanización del derecho internacional cristalice como costumbre o se considere tolerada o aceptada (según el criterio Lotus), o incluso que clarifiquen dentro de qué límites se puede usar determinada tecnología y qué usos se han de considerar prohibidos. En tercer lugar, puede decirse que incluso cuando no haya dudas o posturas encontradas frente a ciertos usos de la tecnología, en ocasiones la regulación o adopción de estándares, incluso de *soft law*, puede usarse para (3) reiterar, aclarar o expresar de forma meridiana el rechazo a determinadas prácticas consideradas como ilícitas, bien porque son de esa forma por gran parte de la sociedad internacional o porque contravienen normas y principios que protegen intereses comunes o comunitario.²⁴ Estos estándares permiten aprovecharse de los posibles efectos simbólicos o expresivos del derecho para intentar ejercer mayor presión y cambiar actitudes. La adopción de estándares también puede tener la finalidad de (4) crear mecanismos u órganos de supervisión.

Una primera dificultad que hace insuficiente apoyarse de forma exclusiva en la *lex lata* y exige desarrollar una regulación concreta frente a usos y desarrollos tecnológicos se presenta cuando haya situaciones y conductas con peculiaridades que deban ser objeto de una regulación que las tenga en cuenta para que la respuesta jurídica frente a ellas sea adecuada, incluso técnicamente, en lugar de ser obsoleta. Argumentos de esta índole se han discutido en el ámbito de la responsabilidad de actores como los grupos armados o las organizaciones internacionales, toda vez que sus peculiaridades exigen que

²⁴ Acerca del principio *Lotus* y su crítica en el sentido de que no hay exclusivamente una consideración binario de permitido o prohibido a los Estados (los soberanos, otro tanto sucede con otros actores en el derecho internacional), ver: Jan Klabbbers, *International Law*, Cambridge University Press, 2013, locations 1136-1154, 1678 (versión Kindle); Corte Internacional de Justicia, *Accordance with International Law of the Unilateral Declaration of Independence in respect of Kosovo*, Opinión Consultiva, 22 de julio de 2010, Declaración del juez Simma, párrs. 9-10. Sobre la noción de protección jurídica internacional de intereses con dimensión comunitaria, vid. Santiago Villalpando, "The Legal Dimension of the International Community: How Community Interests Are Protected in International Law", *European Journal of International Law*, Vol. 21, 2010.

determinadas normas sobre su responsabilidad sean distintas a las previstas para la responsabilidad estatal (siempre y cuando se garanticen mínimos comunes denominadores, por ejemplo en cuanto a reparaciones).²⁵ Esta lógica subyacente también es pertinente al analizar la legalidad de usos y desarrollos tecnológicos.

La consideración de especificidades y problemas de determinados implementos y aplicaciones tecnológicas puede ser importante en diversas dimensiones. Por ejemplo, es importante determinar cómo equilibrar o hacer proporcionado el ejercicio de derechos de distintos actores, como usuarios de internet que invocan su privacidad y otros actores que estiman importante poder compartir o publicar determinada información u opinión, cuestión que de alguna manera se ha discutido en el derecho de la Unión Europea en relación con el llamado “derecho al olvido” o a solicitar que buscadores, como Google, no ofrezcan determinados resultados; siendo también relevantes las consideraciones sobre la existencia de un deber de realizar rectificaciones por “trinos” en Twitter u otras publicaciones en redes sociales, según decidió la Corte Constitucional colombiana; o la decisión de que el presidente estadounidense Trump no podía bloquear a alguien en Twitter por cuanto esta acción sería inconstitucional y contraria a la primera enmienda, según decidió una juez federal en los Estados Unidos de América.²⁶

Los esfuerzos regulatorios (y de interpretación) también permiten hacer frente a los problemas generados por el uso simultáneo de tecnologías nuevas y antiguas, por ejemplo en materia de seguridad aérea. Esto ocurre con preguntas sobre la posibilidad de que el espacio aéreo sea usado no sólo por aviones con pasajeros sino, además, por vehículos aéreos no tripulados, lo que exigiría regular diversas cuestiones como la altura

²⁵ Vid. Robert Dufresne, Review of: Liesbeth Zegveld, *The Accountability of Armed Opposition Groups in International Law*, *European Journal of International Law*, Vol. 15, 2004, pp. 227, 229; José E. Alvarez, “Are Corporations “Subjects” of International Law?”, *Santa Clara Journal of International Law*, Vol. 9, 2011, págs. 30-34; Nicolás Carrillo Santarelli, “The Links between the Responsibility of International Organizations and the Quest towards a More Reasonable and Humane International Legal system”, *International Organizations Law Review*, Vol. 7, 2010, págs. 444-446, 451.

²⁶ Tribunal de Justicia de la Unión Europea (Gran Sala), *Procedimiento entre Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos, Mario Costeja González*, Sentencia sobre petición de decisión prejudicial, 13 de mayo de 2014; Corte Constitucional de Colombia, Sentencia T-121/18, 9 de abril de 2018; John Herrman y Charlie Savage, “Trump’s Blocking of Twitter Users is Unconstitutional, Judge Says”, *The New York Times*, 23 de mayo de 2018.

a la que éstos pueden sobrevolar o los espacios en los que se ha de prohibir su vuelo, entre otras cuestiones que buscan evitar accidentes. La posibilidad de dichos accidentes no es mera especulación, y por ello hay aspectos sobre responsabilidad y prevención que deben ser tratados no sólo de forma operativa y en la práctica sino, además, en un plano normativo.

Sobre las anteriores cuestiones, puede citarse el caso de un avión con pasajeros y un vehículo aéreo no tripulado alemán con tareas de inspección que casi colisionan en Afganistán, lo que motivó el desarrollo e implementación de tecnología para detectar y evitar otros vehículos y colisiones; el hecho de que en los Estados Unidos de América, a pesar de la presencia de estándares sobre altitud y lugares en los que no pueden usarse drones, ha habido múltiples incidentes en los que vehículos aéreos no tripulados casi chocan con aviones tripulados, siendo difícil realizar controles por la proliferación de vehículos aéreos no tripulados en el mercado, lo que, sumado a riesgos e incidentes, ha llevado en ocasiones a la adopción de regulaciones internas restrictivas, cuya flexibilización, motivada por razones económicas y por la evolución de la práctica, se plantea a condición de que haya garantías frente a los riesgos; y además el hecho que hay *drones* que han sido usados de formas o en zonas prohibidas, además de temerse su adquisición y uso con fines ilícitos.

Por otra parte, debe resaltarse que los esfuerzos en la industria realizados por científicos e ingenieros, como por ejemplo en el diseño de automóviles automáticos o en la fabricación de modelos *Phantom* por parte de una empresa china que hizo una programación para que no puedan volar a cierta altura o despegar en las proximidades de los aeropuertos, revelan una toma de consciencia sobre la necesidad de tener medidas de precaución. Pero además de la auto-regulación, los entes de control también pueden normativamente precauciones a través de estándares vinculantes. Entre los aspectos a tener en cuenta se encuentran consideraciones sobre riesgos y ventajas en términos de seguridad y preguntas sobre responsabilidad extracontractual. Estas y otras consideraciones explican el cuidado que se debe tener al proponer regulaciones sobre el uso de tecnologías, como las de *drones* u otras, incluso con fines recreativos cuyo uso tenga relevancia jurídica internacional o en materia de derechos humanos, para

garantizar la seguridad (por ejemplo, prohibiéndose sobrevolar a cierta altura o sobre personas ajenas a la empresa involucrada) y privacidad (por ejemplo, proponiéndose reglas sobre su respeto por parte de agentes estatales que usen *drones*), entre otros aspectos. Tanto la regulación como su implementación pueden dificultarse ante la popularización y proliferación de ciertos desarrollos tecnológicos, lo que ha llevado a algunos a sugerir que se sancionen determinados usos para estimular ciertas conductas y desestimular infracciones;²⁷ y exige que los operadores jurídicos no sean simplemente reactivos o pasivos.

Siendo importante regular, garantizar e implementar medidas y estándares de respeto, seguridad y precaución, es recomendable que quienes se encargan del diseño, programación y venta de tecnología adopten medidas que en ocasiones vayan más allá de lo que exige el derecho positivo actual, que puede estar desactualizado o ceder a presiones de intereses económicos, para procurar evitar la causación de daños. Su conocimiento técnico hace que sus iniciativas sean cruciales, y pone de manifiesto la frecuente necesidad de que los estándares (sobre calidad, etc.) e iniciativas de las autoridades y otros actores se complementen y retroalimenten. Claro está, una vez han sido identificados los riesgos por las autoridades, su deber de ser diligentes en la protección de derechos humanos, que a mi juicio exige una diligencia para cerciorarse de la seguridad del uso de la tecnología, ellas están obligadas a adoptar estándares y medidas de precaución necesarias frente a los riesgos que han identificado.

²⁷ Sobre todas las cuestiones discutidas en los tres anteriores párrafos, ver: Craig Whitlock, “FAA rules might allow thousands of business drones”, *The Washington Post*, 16 de febrero de 2015; The World Post, “German Drone, Afghan Passenger Plane Near-Collision Shown in Terrifying Footage”, 6 de abril de 2013, disponible en: http://www.huffingtonpost.com/2013/06/04/drone-plane-collision-video_n_3381207.html (última visita: 13 de noviembre de 2014); Craig Whitlock, “Drone close calls with aircraft surge”, *The Washington Post*, 27 de noviembre de 2014, disponible en: <http://thewashingtonpost.newspaperdirect.com/epaper/viewer.aspx> (última visita: 27 de noviembre de 2014); “La CNN utilizará ‘drones’ en sus investigaciones periodísticas con el permiso del Gobierno”, *El Mundo*, 13 de enero de 2015; Emily Badger, “5 confounding questions that hold the key to the future of driverless cars”, *The Washington Post*, 15 de enero de 2015; Dan Lamothe, “A drone crashes in the middle of a Capitol Hill hearing about drones”, *The Washington Post*, 21 de enero de 2015; Carol D. Leonnig *et al.*, “Device found on White House grounds identified as drone; no threat posed”, *The Washington Post*, 26 de enero de 2015; “Video Feature: Inside the F 015, Mercedes’s Self-Driving Car”, *The New York Times*, 19 de marzo de 2015.

Frente a la pregunta sobre si determinadas cuestiones sobre el uso de la tecnología y las responsabilidades que pueden surgir por determinados usos de ella deben ser resueltas, coordinadas o incluso tratadas por el derecho u órganos internacionales o si, por el contrario, han de ser de competencia exclusiva de los ordenamientos jurídicos internos de los Estados y ciertas organizaciones con competencias en la materia, puede responderse que ambos niveles de gobernanza tienen un papel relevante por cumplir con base en diversos argumentos. En primer lugar, existen organizaciones internacionales en cuyo seno se han adoptado estándares de coordinación o sobre parámetros mínimos ante desafíos comunes o que ignoren fronteras. Por ejemplo, en la Asamblea de la Organización de Aviación Civil Internacional se ha promovido la adopción y ratificación de tratados sobre aviación que incluyen normas sobre la protección de las personas.²⁸ En segundo lugar, y por las mismas razones, algunos instrumentos internacionales ya se han ocupado de la regulación de la tecnología, por ejemplo en lo relativo a aspectos sobre la aviación comercial que son relevantes a efectos de la seguridad aérea, lo que supone la protección de derechos humanos como la vida e integridad personal; o en lo concerniente a la reparación de daños por actividades en el espacio ultraterrestre. Conviene recordar que las normas del derecho internacional pueden optar por exigir a sus destinatarios adoptar en su derecho interno determinado contenido normativo e incluso pueden, de forma más intensa, regular estándares que vinculen directamente incluso a sujetos privados sin necesidad de la mediación del derecho interno.²⁹

Debe añadirse que es conveniente procurar una uniformidad básica o un mínimo común denominador que facilite el uso de ciertos desarrollos tecnológicos en cualquier lugar del mundo y que establezca responsabilidades mediante un derecho común, para evitar dificultades generadas por vacíos, contradicciones y diferencias considerables que de

²⁸ Ver las Resoluciones A37-22 y A37-23 de la Asamblea, sobre la Declaración consolidada de los criterios permanentes de la OACI en la esfera jurídica, Apéndice C y la Promoción del Convenio de Beijing y del Protocolo de Beijing de 201, respectivamente.

²⁹ Ver, entre otros, el Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional, hecho en Beijing el 10 de septiembre de 2010; el Convenio sobre Aviación Civil Internacional; la Declaración de los principios jurídicos que deben regir las actividades de los Estados en la exploración y utilización del espacio ultraterrestre, punto 8; o el Convenio sobre la responsabilidad internacional por daños causados por objetos espaciales; John H. Knox, "Horizontal Human Rights Law", *American Journal of International Law*, Vol. 102, 2008, págs. 18-31.

otra forma pudiese haber en distintos derechos internos, los que podrían incluso bloquear el uso de implementaciones que pudiesen buscar ayudar a las víctimas o llevar a dinámicas de *fórum shopping* o *race to the bottom*. Es importante promover regulaciones que procuren evitar accidentes que puedan lesionar la integridad personal y otros derechos de los individuos, y el que los expertos discutan sobre estos temas y ofrezcan estándares comunes que sean tenidos en cuenta de forma obligatoria o recomendatoria por los derechos internos y distintos actores. La relevancia de estos objetivos se hace notar de forma especial si se tiene en cuenta que las normas internas y su implementación efectiva deben ser consistentes con la protección y el respeto debidos a los derechos humanos, y que las normativas internas que sean contrarias a los estándares internacionales, por ejemplo en lo relativo al goce de derechos humanos, son deficientes y entrañan una contravención de las obligaciones de adecuar e implementar el derecho interno de conformidad con las exigencias del derecho internacional.³⁰

Los estándares generales universales (o incluso regionales, que pueden inspirar futuros desarrollos en un mayor ámbito subjetivo y territorial o atajar problemas de la región) relativos al uso de desarrollos tecnológicos no sirven únicamente para procurar la compatibilidad de prácticas y normas internas con los derechos humanos sino, además, para armonizar distintas aplicaciones tecnológicas y permitir que se usen en beneficio (o para comodidad) de los individuos de forma segura.

Ciertamente hay usos de la tecnología que benefician a los individuos o/e incrementan la promoción de derechos humanos. Al respecto, se ha discutido que algunas nuevas aplicaciones y desarrollos tecnológicos, como los relacionadas con el uso de vehículos terrestres, acuáticos o aéreos no tripulados o remotamente pilotados, pueden facilitar, hacer más efectivas o permitir acciones de índole humanitaria o de uso civil, incluyendo a las operaciones de mantenimiento de la paz de las Naciones Unidas.

³⁰ Vid. artículos 4, 43 y 44 de la Convención sobre los Derechos de las Personas con Discapacidad; Corte Interamericana de Derechos Humanos, *Caso “La Última Tentación de Cristo” (Olmedo Bustos y otros) vs. Chile*“, Sentencia, op. cit., párr. 87; Corte Interamericana de Derechos Humanos, *Caso de los “Niños de la calle”*, op. cit., párr. 235; Tribunal Europeo de Derechos Humanos (Sección cuarta), *Caso de Hajduová contra Eslovaquia*, Sentencia, 30 de noviembre de 2010, párrs. 36-37.

Adicionalmente, algunos desarrollos pueden emplearse en investigaciones periodísticas o para obtener evidencia de violaciones y contribuir a identificar a los responsables o participantes en abusos, como permiten por ejemplo la información satelital o los datos biométricos (posibilidad que revela la identificación de agentes del Mossad que asesinaron a un miembro de Hamas); y las tecnologías para mejorar el tráfico y el transporte, para inspeccionar e identificar agresiones actuales o potenciales (estatales o no) contra individuos,³¹ para suministrar alimentos a poblaciones que padecen hambre o requieren servicios médicos de emergencia,³² para auxiliar a poblaciones e individuos afectados por situaciones de desastre causados por el hombre o por la naturaleza y para prestar servicios de rescate, entre otras posibilidades que favorecen la protección del ser humano. Inclusive, los deberes positivos (que son obligaciones de medio) de los Estados han de interpretarse teniendo en cuenta las capacidades ofrecidas por la tecnología cuando ello sea pertinente, toda vez que ellas hacen parte de los recursos

³¹ Ver Adam Taylor, "New Delhi's response to Uber rape? Drones with night vision cameras", *The Washington Post*, 12 de diciembre de 2014, disponible en http://www.washingtonpost.com/blogs/worldviews/wp/2014/12/12/new-delhis-response-to-uber-rape-drones-with-night-vision-cameras/?wpisrc=nl_wv&wpm=1 (última visita: 12 de diciembre de 2014); "La CNN utilizará 'drones' en sus investigaciones periodísticas con el permiso del Gobierno", *El Mundo*, 13 de enero de 2015; Emily Badger, "5 confounding questions that hold the key to the future of driverless cars", *The Washington Post*, 15 de enero de 2015; Kate Brannen, "To Catch a Spy", *Foreign Policy*, 6 de abril de 2015; Patrick Kroker, "Satellite imagery as evidence for international crimes", *#globalJUSTICE*, 23 de abril de 2015, disponible en: <https://ciccglobaljustice.wordpress.com/2015/04/23/satellite-imagery-as-evidence-for-international-crimes/> (última visita: 25 de abril de 2015).

³² Vid. Lisa Winter, "'Ambulance Drone' Could Drastically Increase Heart Attack Survival", *IFLSCIENCE!*, 5 de noviembre de 2014, disponible en : <http://www.iflscience.com/health-and-medicine/ambulance-drone-could-drastically-increase-heart-attack-survival> (última visita: 28 de noviembre de 2014); Shawn Du Bravac, "The exciting potential for sensors and drones to combat global hunger", *The Washington Post*, 27 de enero de 2015; Naciones Unidas, "USGs Announce Expert Panel on Technology and Innovation in UN Peacekeeping", Comunicado de prensa del 4 de junio de 2014 (disponible en: http://www.un.org/en/peacekeeping/documents/Expert-Panel_Technology-Innovation_UNPeacekeeping.pdf, última visita: 18 de marzo de 2015); UNifeed, "DRC / UAV LAUNCH", 3 de diciembre de 2014, donde se muestra un video corto y se dice que "UAVs (unmanned aerial vehicles) were launched in Goma, Democratic Republic of Congo by the United Nations to monitor the volatile border between DR Congo and Rwanda and movements by militias and armed groups in the east of the country, which has been stricken by conflict for the past three decades. MONUSCO" (disponible en: <http://www.unmultimedia.org/tv/unifeed/2013/12/drc-drones-launch/>, última visita: 18 de marzo de 2015); Naciones Unidas, "Amid New Risks Facing Blue Helmets, Delegates Call for Retooling Missions as Fourth Committee Concludes Annual Peacekeeping Operations Review", 31 de octubre de 2014, donde se recomienda el uso de innovaciones tecnológicas por parte de operaciones de mantenimiento de la paz (disponible en: <http://www.un.org/press/en/2014/gaspd570.doc.htm>, última visita: 18 de marzo de 2015); e información en Twitter al respecto publicada por "@UNPeacekeeping" en: <https://mobile.twitter.com/unpeacekeeping/status/559553066773397504>; "Using technology to protect civilians. More on technology and innovation in UN Peacekeeping" bit.ly/1BLScD3pic.twitter.com/Xy2cDiopTL (ambas referencias visitadas por última vez el 18 de marzo de 2015); <http://www.un.org/en/peacekeeping/forceforfuture/> (última visita: 18 de marzo de 2015).

disponibles que pueden emplearse y, en consecuencia, pueden determinar el nivel de diligencia exigible en tanto ellas han de emplearse para cumplir con lo requerido por normas del DIH u otras ramas del derecho internacional en la medida en que su uso sea pertinente, razonable y exigible. Al respecto, por ejemplo, Ana Beduschi ha dicho que en tanto la tecnología tiene un impacto sobre la capacidad estatal de identificar las necesidades de protección de los derechos humanos de los migrantes, “States may have a positive obligation to use available technologies to identify and assist vulnerable migrants”;³³ y en similar sentido el comentario de 2017 del CICR al art. 18 del II Convenio de Ginebra establece que:

“Depending on the available technology, such as satellites and unmanned aerial platforms, a Party to the conflict may also be able to carry out an assessment of the numbers and location of the shipwrecked, wounded, sick and dead [...] Since 1949, there have been considerable advances in underwater technology, such as remotely operated vehicles equipped with cameras, to locate and retrieve dead bodies [...] To the extent that a Party to the conflict has the required means at its disposal, both the technology and the knowledge described in the previous paragraph will have an impact on the interpretation of what are ‘possible measures’ in any given case with regard to the search for the dead. This would, however, be subject to the limits of reasonableness”.

Dicho esto, es recomendable ser precavido incluso con aquellos usos de la tecnología que estén orientados a auxiliar o ayudar, para evitar consecuencias adversas o que no haya efectividad de las operaciones. En este sentido, se ha mencionado que en cuanto al uso de *drones* para auxiliar a poblaciones afectadas por conflictos armados es imprescindible tener en cuenta el riesgo, por ejemplo, de que la población civil confunda los vehículos en cuestión con *drones* armados,³⁴ lo que dificulta las operaciones. Esto puede explicarse por temores generados por anteriores casos en los

³³ Ana Beduschi, “The Big Data of International Migration: Opportunities and Challenges for States Under International Human Rights Law”, *Georgetown Journal of International Law*, Vol. 49, 2018.

³⁴ Vid. Jules Frost, “Eyes in the are Inevitable: UAVs and Humanitarian Response”, *PHAP*, 13 de octubre de 2014, disponible en: <https://phap.org/thematic-notes/2014/october/eyes-sky-are-inevitable-uavs-and-humanitarian-response> (última visita: 13 de noviembre de 2014).

que civiles hayan sido lesionados o asesinados por ataques con *drones*, que lleven a la población a abstenerse de acudir a ciertos lugares e incluso de ejercer algunos de sus derechos, como derechos de reunión o de educación al decidir no enviar niños a las escuelas para evitar que se vean afectados por los eufemísticamente llamados “daños colaterales”, causados por ataques que a veces constituyen violaciones del derecho internacional humanitario y crímenes de guerra por ser desproporcionados o excesivos, considerándoseles indiscriminados.³⁵ Frente a los posibles temores que pueden interferir con operaciones de vehículos de uso civil confundidos con *drones* militares, conviene identificar de forma clara, simple y evidente los vehículos de uso civil con ciertos emblemas, teniendo en cuenta la importancia y el impacto positivo del uso de emblemas como los de la Cruz Roja, de la Media Luna Roja y del Cristal Rojo (cuyo uso universal se promueve convencionalmente por esos motivos) o de signos distintivos de organismos de protección civil.³⁶ Lógicamente, la prohibición de la perfidia haría ilícito el aprovechamiento de aquellos emblemas o insignias de identificación de artefactos destinados a usos de naturaleza civil por parte de combatientes que busquen engañar al enemigo o a civiles a los que se pretenda atacar de forma ilícita y criminal.³⁷

En los casos en los que el uso, desarrollo o adquisición de tecnología simplemente sea uno de los distintos medios con los que se pueden afectar fácticamente los derechos humanos, no siempre será indispensable una regulación o un pronunciamiento expreso o concreto sobre aquella tecnología. Dicho esto, en caso de haber ambigüedades o debates no resueltos sobre aspectos jurídicos y prácticas relevantes, será indispensable su *clarificación*, para cumplir con la exigencia de que el derecho haga frente a realidades sociales y prácticas.³⁸

³⁵ Ver, por ejemplo, el artículo 51.5.b) del Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales; Jean-Marie Henckaerts y Louise Doswald-Beck, *El derecho internacional humanitario consuetudinario, Volumen I: Normas*, Comité Internacional de la Cruz Roja, 2007, págs. 53-57.

³⁶ Ver el Protocolo III adicional a los Convenios de Ginebra de 1949 relativo a la aprobación de un signo distintivo adicional de 2005; y el siguiente texto del Comité Internacional de la Cruz Roja (CICR): <https://www.icrc.org/spa/resources/documents/misc/protocolo-iii.htm> (última visita: 13 de noviembre de 2014); artículo 66 del Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales de 1977.

³⁷ artículo 37 y 85.3.f) del Protocolo I adicional a los Convenios de Ginebra de 1949; Jean-Marie Henckaerts y Louise Doswald-Beck, op. cit., págs. 231-238.

³⁸ Vid. Antonio Remiro Brotons et al., *Derecho Internacional*, Tirant Lo Blanch, 2007, pág. 46.

El hecho de que la tecnología pueda hacer que sea más fácil incurrir en comportamientos sobre cuya licitud ya haya dudas, o que se produzcan efectos más intensos o frecuentes que aquellos que se generarían sin su uso, hará que sea apremiante codificar o dilucidar qué dice el derecho o qué se debe regular a futuro *de lege ferenda*. Ello puede contribuir a frenar el posible surgimiento futuro de costumbres inadecuadas o a respaldar dinámicas positivas, como por ejemplo las relativas al ejercicio de derechos humanos en internet.

Las discusiones referentes a los ataques contra grupos armados no estatales o grupos calificados como terroristas por medio de nuevas tecnologías ejemplifican estos análisis. Al respecto, se constata que hay discusiones sobre (i) la posibilidad de realizar acciones en legítima defensa contra actores no estatales; y sobre (ii) la calificación jurídica de ciertas acciones y la posibilidad de atacar lícitamente a determinados integrantes de grupos no estatales.

La cuestión sobre (i) la licitud o ilegalidad del uso de la fuerza contra grupos no estatales ubicados en el territorio de un tercer Estado sin que se alegue que éste ha realizado un uso mayor de la fuerza en perjuicio de otro ha sido muy debatida y ha cobrado una vigencia cada vez mayor, en virtud de distintos factores. Entre ellos se cuentan las crecientes operaciones contra grupos calificados como terroristas por parte de los Estados Unidos de América y otros Estados, con la peculiaridad de que los ataques se realizan en muchas ocasiones tras la supuesta adquisición de información de inteligencia obtenida gracias a la tecnología o por informantes cuya veracidad es en ocasiones dudosa. Algunos de aquellos ataques se realizan por medio de *drones* armados, cuyo uso ha afectado y victimizado a muchos civiles, y suelen rodearse de secretismo y falta de publicidad en cuanto a la toma de decisiones.³⁹ Ciertamente, es importante determinar la licitud (y sus condiciones) de aquel tipo de operaciones, pero

³⁹ Vid. UNOG, “Human Rights Council Holds Panel on Remotely Piloted Aircraft or Armed Drones in Counterterrorism and Military Operations”, 22 de septiembre de 2014, disponible en: http://www.unog.ch/unog/website/news_media.nsf/%28httpPages%29/BCE56ED914A46D40C1257D5B0038393F?OpenDocument (última visita, 13 de noviembre de 2014); Richard A. Clarke, *Sting of the Drone*, Thomas Dunne Books, 2014.

no todas las dudas obedecen a aspectos sobre la tecnología de los *drones*, pues hay operaciones contra actores no estatales realizadas sin ello se plantean idénticas dudas. En este sentido, es importante clarificar si la autorización de la legítima defensa prevista en la costumbre internacional y en la Carta de las Naciones Unidas incluye o no la posibilidad de atacar a actores no estatales,⁴⁰ y si esta posibilidad *debería* estar permitida para evitar la indefensión e impunidad y para permitir proteger a poblaciones atacadas por entes no estatales cuyas acciones no puede contrarrestar el Estado en cuyo territorio se alojan ni pueden ser atribuidas a dicho Estado (en sentido afirmativo, se han manifestado Bruno Simma, Rosalyn Higgins o P. H. Kooijmans)⁴¹ o si, por el contrario, aquella autorización no existe o es inconveniente por el hecho de que fomenta escaladas y generalizaciones de operaciones militares (que siempre afectan a los seres humanos).⁴² Creo que los temores de las dos posturas enfrentadas son válidos y tienen mérito, y no puede ignorarse que el objetivo de defenderse y defender frente a grupos no estatales puede usarse como excusa para perseguir otros fines. Sin embargo, estimo que es preferible permitir la posibilidad de la defensa en cuestión condicionándola, pues en caso contrario, cuando ella sea indispensable, muchas víctimas carecerán de posibilidades de protección efectiva frente a auténticas agresiones, lo que menoscaba la perspectiva de goce de sus derechos. Por el contrario, el condicionamiento de la licitud permite ofrecer protección a la vez que se proscriben abusos y desviaciones.

⁴⁰ Vid. Consejo de Seguridad de las Naciones Unidas, Resolución 1368 (2001); Siobhán O’Grady, “Legality Aside, International Community Accepts Syrian Airstrikes”, *Foreign Policy*, 23 de septiembre de 2014; Suhrith Parthasarathy, “Interpretation of International Law”, *The Hindu*, 24 de octubre de 2014.

⁴¹ Opinión separada del juez Kooijmans a la Sentencia de la Corte Internacional de Justicia del 19 de diciembre de 2005 en el caso sobre *Armed Activities on the Territory of the Congo (República Democrática del Congo contra Uganda)*, párrs. 26-32; Opinión separada del juez Simma a la Sentencia de la Corte Internacional de Justicia del 19 de diciembre de 2005 en el caso sobre *Armed Activities on the Territory of the Congo (República Democrática del Congo contra Uganda)*, párrs. 10-15; Opinión separada de la juez Higgins a la Opinión consultiva de la Corte Internacional de Justicia de 9 de julio de 2004 sobre “*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*”, párrs. 33-35.

⁴² Vid. Constantine Antonopoulos, “Force by armed groups as armed attack and the broadening of self-defence”, *Netherlands International Law Review*, Vol. LV, 2008; RT, “Russia warns US-led coalition: Those who carry out strikes in Syria face blowback”, 23 de septiembre de 2014, disponible en: <http://rt.com/news/189932-strikes-syria-russia-nato/> (última visita: 13 de noviembre de 2014).

De acuerdo con la postura de algunos Estados, jueces y académicos, las acciones examinadas serían lícitas si, además de cumplirse con las condiciones generales de la legítima defensa (de necesidad, proporcionalidad, etc.), el Estado en cuyo territorio está ubicado el ente no estatal que se quiere atacar es incapaz o no tiene la voluntad de hacer frente al grupo ubicado en su territorio (aunque otros discuten este criterio).⁴³

A pesar de la práctica creciente de algunos Estados de atacar a grupos no estatales ubicados en el territorio de otro Estado cuando las acciones de ellos equivalgan a usos mayores de la fuerza, sin que tal conducta pueda ser atribuida de forma directa al Estado en cuyo territorio están ubicados, el tema sigue siendo debatido y ha sido objeto de posiciones encontradas expresadas, por ejemplo, en pronunciamientos de Estados y organizaciones internacionales, como sucedió en el caso de un ataque colombiano contra un grupo guerrillero cuando integrantes de éste se encontraban en Ecuador, considerando unos que la legítima defensa permitía el ataque y otros que éste era contrario a la integridad territorial y a la soberanía del Estado en el que se realizó la operación.⁴⁴

En asuntos como el examinado, en los que las dudas no se deben al uso de *drones* u otros desarrollos tecnológicos, su empleo ciertamente puede incrementar los efectos o la posibilidad de realizar operaciones cuya licitud sea debatida, haciendo más urgente el despejar las incertidumbres, llenar vacíos o perfeccionar la regulación. Las aclaraciones pertinentes se pueden hacer mediante instrumentos (de *soft* o *hard law*) que *declaren* el contenido normativo pertinente; y la regulación para paliar vacíos o mejorar normas que sean inconvenientes o anticuadas exige un desarrollo progresivo, que puede además

⁴³ Vid. Tatiana Waisberg, "Colombia's Use of Force in Ecuador Against a Terrorist Organization: International Law and the Use of Force Against Non-State Actors", *ASIL Insights*, Vol. 12, 2008; Siobhán O'Grady, op. cit.; Opiniones separadas de los jueces Kooijmans, Simma y Higgins, op. cit. (en los párrafos citados en el pie de página anterior al precedente); Kevin Jon Heller, "Mea Culpa Regarding Israel's Attacks on Hezbollah in 2006", *Opinio Juris*, 10 de marzo de 2015; Jens David Ohlin, "The Unwilling or Unable Doctrine Comes to Life", *Opinio Juris*, 23 de septiembre de 2014; Kevin Jon Heller, "Do Attacks on ISIS in Syria Justify the 'Unwilling or Unable' Test?", *Opinio Juris*, 13 de diciembre de 2014; Kevin Jon Heller, "The Absence of Practice Supporting the 'Unwilling or Unable' Test", *Opinio Juris*, 17 de febrero de 2015; Kevin Jon Heller, "The Seemingly Inexorable March of 'Unwilling or Unable' Through the Academy", *Opinio Juris*, 6 de marzo de 2015; Kevin Jon Heller, "Eric Posner Rejects the 'Unwilling or Unable' Test!", *Opinio Juris*, 8 de octubre de 2012.

⁴⁴ Vid. Tatiana Waisberg, op. cit.

encauzar la práctica y *opinio juris* y cristalizar o generar una costumbre en determinado sentido. Debe tenerse en cuenta que en las soluciones deben tener en cuenta las necesidades de protección de todos los derechos humanos, la existencia de derechos absolutos (imperativos), las condiciones de su restricción y todas las inquietudes formuladas en los debates, con tal de ofrecer respuestas satisfactorias.

Por otra parte, también hay dilemas como el referente a (ii) si el DIH es aplicable en operaciones con *drones* u otras tecnologías contra grupos armados no estatales. La respuesta no depende del uso de la tecnología, sino que, por el contrario, según la situación la tecnología se podrá emplear de uno u otro modo.

Al respecto, ha de decirse que en ocasiones los Estados que han empleado *drones* para realizar ataques contra integrantes de grupos calificados de terroristas intentan escudar la legitimidad de sus acciones, entre otras, con argumentos jurídicos, diciendo que son realizadas en medio de conflictos armados no internacionales que se despliegan en un escenario transnacional⁴⁵ (aunque en la práctica, por razones políticas, son más proclives a desarrollar operaciones en ciertos territorios que en otros), en tanto (salvo en determinadas excepciones) los combatientes en los conflictos armados pueden ser atacados a la luz del DIH; y han llegado incluso a ofrecer argumentos que sugieren que todo el mundo es un potencial escenario de hostilidades o campo de batalla.⁴⁶ Según esa lógica, los ataques en cuestión serían lícitos en la medida en que se dirigen de forma directa contra combatientes. Frente a la pregunta sobre si los integrantes de grupos no estatales pueden ser combatientes, se invoca a su vez la noción de “función continua de combate” discutida por el Comité Internacional de la Cruz Roja, que ofrece una respuesta afirmativa.⁴⁷ Por otra parte, se dice que los eventuales daños a bienes o personas civiles que resulten de las operaciones no generarían responsabilidad siempre y cuando no sean causados de forma directa ni desproporcionados. Además, en

⁴⁵ Vid. Marko Milanovic, “Lessons for human rights and humanitarian law in the war on terror: comparing *Hamdan* and the Israeli *Targeted Killings* case”, *International Review of the Red Cross*, 2007, págs. 380-381.

⁴⁶ Ver, por ejemplo, esto ilustrado en una novela: Richard A. Clarke, op. cit.

⁴⁷ Vid. Nils Melzer, *Participación directa en las hostilidades: según el derecho internacional humanitario*, Comité Internacional de la Cruz Roja, 2010.

ocasiones se esgrime el argumento de que la tecnología empleada permite realizar ataques con mayor *precisión* y permite, asó, evitar mayores daños a civiles en comparación con el uso de armas y métodos tradicionales o no tan desarrollados; y que se posibilita el no exponer a riesgos a agentes estatales. Incluso en las Naciones Unidas se ha considerado que, *en algunas ocasiones* (enfaticándose que no siempre es así), los *drones* permiten obtener información que permite distinguir a los civiles de combatientes y tomar medidas de precaución, aunque en el seno de esa organización también se han cuestionado la precisión de algunos ataques con *drones* en algunos casos y otras supuestas ventajas de su uso, en virtud de posibles errores, por ejemplo relativos a la inteligencia. Adicionalmente, se debe anotar que hay información de que los *drones* se estrellan con mayor frecuencia que otros vehículos aéreos militares (considerándose su fiabilidad como su talón de Aquiles), y se ha debatido si acaso se corre el riesgo de que quienes manejan remotamente a los *drones* lo hagan con una mentalidad de "videojuego" o si, por el contrario, la mayor inteligencia e información y conocimiento de los afectados y las condiciones para que se autorice atacar con ellos podría, quizá, generar ciertas reticencias a atacar innecesariamente. Como contrapartida a los anteriores argumentos, otros esgrimen la presencia de errores que han costado la vida a civiles, bien sea por deficiencias en la inteligencia o en la implementación de ciertas operaciones; la excesiva facilidad de autorización para asesinar (¡a seres humanos, ni más ni menos!) con *drones* otorgada a sus agentes por actores como los Estados Unidos de América; el secretismo de operaciones realizadas con ellos que generan sospechas sobre ausencia de garantías y publicidad; o el hecho de que las tecnologías en cuestión ofrecen una tentación facilista de matar cuando podría haber alternativas no letales tales como la captura (necesaria salvo cuando haya riesgo inminente para la vida de otros, en caso de no el DIH).⁴⁸ Todos estos debates y cuestiones generan incertidumbres, no

⁴⁸ Vid. Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Philip Alston, *Study on targeted killings*, A/HRC/14/24/Add.6, 28 de mayo de 2010, párrs. 19, 81-82. Sobre si hay una mentalidad de "videojuego" o no en el uso letal de los *drones*, ver las siguientes posiciones encontradas: Mark Mazzetti, "Use of Drones for Killings Risks a War Without End, Panel Concludes in Report", *The New York Times*, 26 de junio de 2014 versus Philip Alston y Hina Shamsi, "A killer above the law?", *The Guardian*, 8 de febrero de 2010, y Richard A. Clarke, op. cit.; Craig Whitlock, "How crashing drones are exposing secrets about U.S. war operations", *The Washington Post*, 25 de marzo de 2015, donde se dice que "Reliability has long been the Achilles' heel of drones. Although they malfunction less often than they used to, they still crash at a higher rate than other military aircraft. Of the 269 Predators acquired by the Air Force over the past

paliadas por la falta de publicidad en muchas operaciones, y sugieren que la licitud del empleo de *drones* (así como de muchas tecnologías) dependerá de su uso concreto.

Aparte de la postura de aquellos Estados que despliegan las operaciones en cuestión, conviene ver las adoptadas por otros actores. Frente a las cuestiones comentadas puede decirse, en primer lugar, que aunque en la doctrina y la práctica del Comité Internacional de la Cruz Roja se considera que un conflicto que no sea entre Estados y no se desarrolle tan sólo en el territorio de un Estado, al estar “transnacionalizado”, está regulado por el derecho internacional de conformidad con las normas de los conflictos armados no internacionales, evitándose así vacíos.⁴⁹ Por su parte, algunos relatores de derechos humanos, activistas y académicos han puesto en tela de juicio que muchas acciones desplegadas contra supuestos terroristas se hayan realizado en un escenario de *hostilidades* que alcancen el nivel de intensidad de los conflictos armados transnacionales o mixtos. Algunos también han cuestionado si la noción de función continua de combate en un grupo no estatal es consistente con normas internacionales, por considerar que puede suponer la creación de una nueva categoría e ignorar límites sobre ataques contra civiles restringidos a la duración de una participación directa en hostilidades⁵⁰ (a mi juicio, la noción se apoya en la práctica y *opinio juris* y en el reconocimiento de que hay combatientes no estatales). Estos debates resaltan la importancia de despejar las dudas normativas u orientar la costumbre en determinado sentido, al igual que acontece con el debate sobre la legítima defensa; y de insistir en el respeto de estándares como aquellos que impiden los ataques que posibilita el DIH en caso de no haber un verdadero conflicto armado, evento en el cual no sería lícito atacar directamente de forma letal a los integrantes de grupos no estatales si ello no es

two decades, more than half have wrecked in major accidents, records show.”; Greg Miller, "Hostages' deaths raise wider questions about drone strikes' civilian toll", *The Washington Post*, 23 de abril de 2015; Scott Shane, "Drone Strikes Reveal Uncomfortable Truth: U.S. Is Often Unsure About Who Will Die", *The New York Times*, 23 de abril de 2015.

⁴⁹ Vid. Marko Milanovic, op. cit., pág. 381.

⁵⁰ Vid. Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, op. cit., párr. 65.

necesario para salvar de forma inminente la vida de alguien, como dispone el derecho internacional de los derechos humanos.⁵¹

En relación con estas cuestiones, debe hacerse hincapié en que toda operación contra el terrorismo u otras acciones que atenten contra la dignidad humana, que persiga proteger los derechos de quienes pueden ser agredidos por ellas, debe respetar los derechos humanos de los presuntos (o probados) terroristas y de todos los demás seres humanos que puedan verse afectados,⁵² incluso en cuanto al respeto de la privacidad de comunicaciones telefónicas o electrónicas de extranjeros (sin discriminarlos) y a la observancia de las estrictas condiciones de necesidad y proporcionalidad (entre otras) que se exigen para que sea lícito restringir derechos. Esto es algo que desafortunadamente no han tenido en cuenta algunos Estados. Lógicamente, aquellas exigencias son aplicables a las operaciones en las que se use o se responda a usos de la tecnología; y ponen de manifiesto la importancia de que sea claro qué exige y permite el derecho internacional (lo que se relaciona además con la previsibilidad y el principio de legalidad) y de que tal derecho responda a criterios meta-jurídicos sobre el respeto debido al ser humano.⁵³

La clarificación de qué dice el derecho internacional frente a conductas relevantes relacionadas (de forma necesaria o contingente) con el desarrollo, posesión o uso de determinadas tecnologías, y la regulación progresiva en caso de haber vacíos, pueden tener la capacidad o el designio impactar sobre ellas bien sea para condicionarlas, estimularlas, disuadirlas, frenarlas, tolerarlas o permitir las, incluso si no es imprescindible que se use la tecnología para incurrir en las conductas en cuestión. No obstante, los usos y desarrollos de la tecnología que puedan relacionarse con ellas deben

⁵¹ Vid. Philip Alston, op. cit., párr. 32; UNOG, “Human Rights Council Holds Panel on Remotely Piloted Aircraft or Armed Drones in Counterterrorism and Military Operations”, op. cit.

⁵² Vid. Corte Interamericana de Derechos Humanos, *Caso Castillo Petrucci y otros vs. Perú*, Sentencia, 30 de mayo de 1999, párr. 89; Comisión Interamericana de Derechos Humanos, *Informe sobre terrorismo y derechos humanos*, OEA/Ser.L/V/II.116, 22 de octubre de 2002, párrs. 2-5; Resolución 2178 (2014) del Consejo de Seguridad, Preámbulo y párrs. 5, 11 y 17.

⁵³ Sobre afectaciones de los Estados discutidas en el párrafo, ver: Consejo de Derechos Humanos de las Naciones Unidas, *El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, A/HRC/27/37, op. cit., párrs. 22, 35-36. En relación con el principio de legalidad, ver: Tribunal Europeo de Derechos Humanos (Gran Sala), *Caso Kononov Vs. Letonia*, Sentencia de 17 de mayo de 2010, párrs. 185, 187.

ser tenidas en cuenta a la hora de codificar o desarrollar progresivamente el derecho, sin que sea necesario enunciarlas expresamente.

Otra razón que hace que se justifique y recomiende (o que incluso deba exigirse) adoptar estándares de *soft law* o de *hard law* en la materia (o aplicables implícitamente a desarrollos tecnológicos) es la alusiva a la importancia de pronunciarse de forma expresa y directa sobre determinadas prácticas que se sirvan o puedan servir de la tecnología y sean contrarias a derechos humanos y otros derechos reconocidos internacionalmente, con el propósito de condenarlas, avergonzar a sus autores, y fomentar cambios en comportamientos y actitudes.

La expresión o confirmación formal de la ilicitud y prohibición de las conductas en cuestión puede perseguir distintos objetivos: en primer lugar, evitar la posibilidad de que se modifique la costumbre internacional de forma que se disminuyan los estándares dispositivos de protección de derechos humanos⁵⁴ (aquellos que sean imperativos no pueden ser menoscabados por la costumbre u otras fuentes salvo por normas que emerjan con carácter igualmente imperativo, algo difícil en el caso de reducción de estándares).⁵⁵ Por otra parte, los rechazos sirven para robustecer y servir de fundamento jurídico expreso de pretensiones y reclamos, lo que explica que distintos actores y autoridades (en distintos niveles, incluyendo el estatal,⁵⁶ pero no limitándose a él) tengan interés en activarlos (o desactivarlos, en el caso de quienes ilegítimamente se beneficien de estándares bajos por intereses económicos o bélicos ligados a posibilidades que les brinda la tecnología). En tercer lugar, sirve para llamar la atención a la sociedad, a distintas autoridades, a infractores potenciales, a activistas, a *stakeholders* y al público y destinatarios sobre el carácter ilícito de conductas que se

⁵⁴ Sobre esta posibilidad, ver, por ejemplo: Antonio Remiro Brotons et al., *Derecho Internacional: Curso general*, Tirant Lo Blanch, 2010, págs. 212-213.

⁵⁵ Vid. artículo 53 de la Convención de Viena sobre el Derecho de los Tratados de 1969, donde se dice que la modificación de normas de *ius cogens únicamente* puede hacerse por medio de normas con el mismo carácter. En lo relativo a la costumbre opuesta al *ius cogens*, ver: Comisión Interamericana de Derechos Humanos, *Caso 12.285 (Michael Domingues vs. Estados Unidos)*, Informe N° 62/02, 22 de octubre de 2002, párrs. 49-50; Comisión Interamericana de Derechos Humanos, *Caso 11.436 (Víctimas del barco remolcador "13 de marzo" vs. Cuba)*, Informe N° 47/96, 16 de octubre de 1996, párr. 79.

⁵⁶ Vid. Antonio Cassese, "Remarks on Scelle's Theory of "Role Splitting" (*dédoublement fonctionnel*) in International Law", *European Journal of International Law*, Vol. 1, 1990, págs. 226-231.

aprovechan de la tecnología o sobre cómo determinados usos y desarrollos tecnológicos o ciertas conductas que tengan un impacto en escenarios cibernéticos o digitales pueden afectar intereses y derechos. La regulación, que puede indicar no sólo a qué se tiene derecho sino además qué se debe proteger o qué se debe hacer o no hacer, puede tener distintos efectos, como los expresivos y los educativos; y puede generar el desencadenamiento de dinámicas de presión, socialización o internalización, los que pueden jugar un papel clave en la efectividad y garantía del derecho internacional.⁵⁷

Finalmente, los pronunciamientos normativos asignan rótulos que permiten evidenciar o intensificar y fortalecer las críticas a determinadas conductas relativas al uso, posesión o desarrollo de implementaciones tecnológicas, y pueden contribuir a inducir modificaciones en la cultura, conducta y actitudes de quienes puedan ser sus diseñadores o usuarios,⁵⁸ especialmente si están de acuerdo con el contenido normativo o temen posibles sanciones y estigmas. Evidentemente, las campañas e iniciativas de activistas también se podrán ver fortalecidas. Después de todo, hoy día hay un estigma frente a comportamientos *considerados* como contrarios a los derechos humanos (en ocasiones, incluso si no es clara aquella contradicción y sólo se invocan instrumentos de *soft law* o argumentos sin soporte normativo, lo cual tiene ciertos problemas de legitimidad y representación, habiendo incluso disputas *entre* integrantes de la llamada sociedad civil). De esta manera, la codificación y el desarrollo progresivo del derecho internacional pueden potenciar iniciativas de avergonzamiento o fomentar iniciativas corporativas o de científicos, ingenieros y quienes crean o emplean la tecnología motivadas por el deseo de demostrar que se respetan e incluso promueven los bienes jurídicos internacionales.⁵⁹ En este sentido, pueden generarse reacciones consistentes en

⁵⁷ Frits Kalshoven y Liesbeth Zegveld, "Constraints on the Waging of War", 3rd Edition, ICRC, 2001, págs. 70-71; Ryan Goodman y Derek Jinks, "Incomplete Internalization and Compliance with Human Rights Law", *European Journal of International Law*, Vol. 19, 2008, págs. 726, 735.

⁵⁸ Sobre ejemplos al respecto, y la relevancia de la cultura y actitud de los destinatarios, vid. Fred Halliday, "The Romance of Non-state Actors", en Daphné Josselin y William Wallace (eds.), *Non-state Actors in World Politics*, Palgrave, 2001, pág. 35; Harold Koh, "Why Do Nations Obey International Law?", *The Yale Law Journal*, Vol. 106, 1997, págs. 2600-2601; Consejo de Derechos Humanos de las Naciones Unidas, "Proteger, respetar y remediar: un marco para las actividades empresariales y los derechos humanos", A/HRC/8/5, 7 de abril de 2008, párrs. 27, 29-32, 105.

⁵⁹ En relación con algunos ejemplos sobre el papel, los límites y riesgos y la relevancia del *shaming* en el derecho internacional de los derechos humanos, y algunas estrategias diferentes al avergonzamiento, incluso no basadas en la confrontación, que pueden promover la observancia de normas internacionales,

pronunciamientos de compromisos y códigos de conducta, no vinculantes en sí mismos, que a su vez pueden tener efectos jurídicos indirectos en virtud de la protección de la buena fe o el papel de los actos unilaterales⁶⁰ o motivar futuras regulaciones vinculantes.

La importancia de la declaración de la ilicitud de determinados comportamientos se confirma por el reconocimiento de que el reconocimiento público de la ilicitud de una conducta en decisiones judiciales o por otros medios puede ser incluso una forma de dar satisfacción, que también puede obtenerse con la revelación de la verdad, el reconocimiento de la comisión de hechos ilícitos o el ofrecimiento de disculpas, entre otras posibilidades.⁶¹ El hecho de que Cortes y órganos internacionales publiquen sus decisiones, comunicados de prensa, recomendaciones, o transmitan sus audiencias en *streaming* en línea revela la consciencia sobre la importancia de estos procesos, que además permiten satisfacer la exigencia de que la actuación de órganos (internos e) internacionales tenga publicidad.⁶² Adicionalmente, la codificación y el desarrollo de normas sobre la tecnología puede servir como estrategia para impulsar la humanización del derecho internacional en relación con ciertos instrumentos tecnológicos; y puede ser

ver: Thomas Buergenthal, “The Evolving International Human Rights System”, *American Journal of International Law*, Vol. 100, 2006, Steven R. Ratner, “Law Promotion Beyond Law Talk: The Red Cross, Persuasion, and the Laws of War”, *European Journal of International Law*, Vol. 22, 2011, págs. 803; 483, 492, 505; David Capie, “Influencing Armed Groups: Are there Lessons to be Drawn from Socialization Literature?”, en: Geneva Call, *Exploring Criteria & Conditions for Engaging Armed Non-State Actors to Respect Humanitarian Law & Human Rights Law*, Conference Report, 2007, pág. 88; Olivier Bangerter, “The ICRC and Non-State Armed Groups”, en: Geneva Call, *Exploring Criteria & Conditions for Engaging Armed Non-State Actors to Respect Humanitarian Law & Human Rights Law*, Conference Report, 2007, pág. 83.

⁶⁰ Vid. Non-State Actors Committee of the International Law Association, *Preliminary issues for the ILA Conference in Rio de Janeiro*, Report, 2008, pág. 3; Antonio Remiro Brotons et al., *Derecho Internacional: Curso general*, op. cit., págs. 175-183.

⁶¹ Vid. Comisión de Derecho Internacional, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001, págs. 106-107 (párrs. 5 a 7 del comentario al artículo 37); Principios y directrices básicos sobre el derecho de las víctimas de violaciones manifiestas de las normas internacionales de derechos humanos y de violaciones graves del derecho internacional humanitario a interponer recursos y obtener reparaciones, párr. 22; Yasmin Naqvi, “El derecho a la verdad en el derecho internacional: ¿realidad o ficción?”, *International Review of the Red Cross*, N° 862, 2006, pág. 16.

⁶² Vid. Benedict Kingsbury, “The Concept of ‘Law’ in Global Administrative Law”, *European Journal of International Law*, Vol. 20, 2009, págs. 32-33, 39, 41, 48-50.

un factor importante en la prevención de la repetición o comisión de violaciones o afectaciones.⁶³

Quizás movidos por el afán de asegurar un uso de la tecnología humanizado y compatible con los derechos humanos, Estados como Alemania y Brasil apoyaron y promovieron la adopción de una resolución sobre “El derecho a la privacidad en la era digital” en la Asamblea General de las Naciones Unidas (dolidos, además, por el espionaje que sufrieron a manos de la NSA estadounidense).⁶⁴ En una resolución de la Asamblea General de la ONU del 18 de diciembre de 2013, se recalca la importancia del derecho humano a la privacidad y se reconoce que avances tecnológicos y la naturaleza de internet hacen que sea importante garantizar aquel derecho en este medio. En la resolución, que refleja aspectos discutidos en esta sección, también se llama a los Estados a proteger aquel derecho, incluso en lo relativo a las comunicaciones digitales (que se vieron afectadas por la conducta estadounidense y son expresamente mencionadas en cuanto a su protección), y a asegurarse de que su conducta, legislación y prácticas sean compatibles con las exigencias internacionales señaladas.⁶⁵ Esta resolución confirma la obviedad de que la vulneración de libertades ejercidas en un entorno digital o por medios tecnológicos, incluso si persigue intereses estatales (muchas veces egoístas) por medio del espionaje u otras acciones, es contraria a normas y principios jurídicos internacionales que encarnan e impulsan la humanización del derecho internacional. Debe resaltarse que en el seno de la Asamblea General de las Naciones Unidas se siguieron examinando las cuestiones discutidas, por ejemplo en cuanto a la necesidad e importancia de que haya recursos efectivos de protección y reparaciones para las víctimas. Por otra parte, las acusaciones de injerencia rusa en las elecciones presidenciales estadounidenses de 2016 también han sido discutidas por gobiernos y en la doctrina, en el entendido de que aquellas operaciones cibernéticas que

⁶³ Vid. Principios y directrices básicos sobre el derecho de las víctimas de violaciones manifiestas de las normas internacionales de derechos humanos y de violaciones graves del derecho internacional humanitario a interponer recursos y obtener reparaciones, párr. 23.

⁶⁴ Vid. Paul Meyer, “Cyber Security Takes the Floor at the UN”, [OpenCanada.org](http://opencanada.org), 12 de noviembre de 2013 (disponible en: <http://opencanada.org/features/the-think-tank/comments/cyber-security-takes-the-floor-at-the-un/>, última visita, 10 de marzo de 2015).

⁶⁵ Vid. Asamblea General de las Naciones Unidas, Resolución 68/167, aprobada el 18 de diciembre de 2013, párrs. párrs. 3 y 4.

supongan una verdadera intromisión pueden resultar contrarias al principio que prohíbe la intervención en los asuntos internos (y externos, añadido) de los Estados, afectando la soberanía.⁶⁶

Como se apuntó en la anterior subsección, mientras se adoptan y entran en vigor normas e instrumentos con un contenido recomendable o necesario para proteger adecuadamente a los seres humanos, es necesario acudir a la *lex lata*. Si un actor afectado o interesado o un operador jurídico identifica vacíos que exijan una nueva regulación, debe hacer lo mejor que pueda en el entretanto y anunciar *pública* y efectivamente a quienes están habilitados para hacerlo la necesidad de crear o modificar el derecho *de lege ferenda*, tal y como se señaló, en otro contexto, en los principios de Bangalore.⁶⁷ Por otra parte, quienes pueden adoptar estrategias o normas protectoras internas⁶⁸ o internacionales deben actuar cuando ello sea necesario o crucial (y lícito) para proteger a quienes puedan verse afectados por determinados usos de la tecnología. Las normas protectoras, a su vez, deben ser implementadas de forma efectiva. De esta forma, se pueden evitar situaciones de responsabilidad internacional generadas bien sea por la incompatibilidad entre disposiciones, prácticas y comportamientos internos y exigencias del derecho internacional; o por vacíos o la falta de desarrollos e implementación en cuanto a protección sustantiva; y además se puede perseguir el propósito de humanizar *tanto* el derecho como los desarrollos y usos de la tecnología.

En ocasiones, lidiar con desarrollos tecnológicos actuales es complejo desde el punto de vista de identificar la ley existente aplicable o de cuál es el desarrollo progresivo

⁶⁶ Vid. Ben Quinn, “United Nations human rights committee resolves to protect privacy”, *The Guardian*, 26 de noviembre de 2014, disponible en: <http://www.theguardian.com/law/2014/nov/26/united-nations-human-rights-privacy-security> (última visita: 12 de diciembre de 2014); Duncan Hollis, “Russia and the DNC Hack: What Future for a Duty of Non-Intervention?”, *Opinio Juris*, 25 de julio de 2016.

⁶⁷ *The Bangalore Principles: Report of Judicial Colloquium on the Domestic Application of International Human Rights Norms*, Bangalore, India, párr. 8.

⁶⁸ Ver, por ejemplo, la propuesta de normas estadounidenses sobre seguridad, apoyada por defensores de derechos relativos a la privacidad, que reconoce la posibilidad de que haya acciones cibernéticas contrarias a la integridad, salud o seguridad de seres humanos (no me expreso a favor o en contra de su extenso contenido en concreto, sino que llamo la atención sobre el reconocimiento de problemas sobre usos de la tecnología y la importancia de responder normativamente), según se describe en el *Bill H.R. 3696*, como se describe en: <http://docs.house.gov/billsthisweek/20140728/BILLS-113hr3696-SUS.pdf>; y David Francis, “Cybersecurity Bill Gets New Life in Senate”, *Foreign Policy*, 4 de diciembre de 2014 (última visita de ambas páginas: 5 de diciembre de 2014).

adecuado del derecho. Esto se ha discutido, por ejemplo, en relación con la identificación sobre la necesidad (o no) de prohibir el desarrollo y uso de armas autónomas y qué estrategia normativa es la más conveniente.

Sobre aquellas armas, debe comenzarse diciendo que ellas pueden tener distintos grados de autonomía. En la cúspide se encontrarían aquellas que se pudiesen activar sin comandos o instrucciones directas dadas por seres humanos; y en peldaños inferiores, por ejemplo, habría armas o artefactos que puedan sobrevolar un espacio de forma autónoma y automática sin que se pueda activar automáticamente la orden de ataque o empleo de armas equipadas, que por ejemplo no podría darse sin un comando, autorización o instrucción humana en determinado escenario.⁶⁹

Frente a la licitud de las armas autónomas, hay posiciones encontradas. La complejidad de la cuestión, y la necesidad de debatirla, se evidencian en campañas que promueven la prohibición de las armas con alto grado de autonomía y debates sobre su licitud, en foros como los de las Naciones Unidas. Ha habido posturas contrarias a ella, como algunas de Human Rights Watch y la *International Human Rights Clinic* de Harvard, que han afirmado que las incertidumbres sobre su desarrollo y los grandes riesgos de que puedan afectar fundamentos y garantías esenciales de los derechos humanos y del derecho internacional humanitario aconsejan la prohibición (preventiva) internacional de su desarrollo, producción y uso. Asumiendo una posición contraria, algunos autores sostienen que será el uso concreto de la tecnología, incluyendo el de esas armas, el que adolecerá o no de ilicitud; que las armas autónomas ofrecen ventajas de las que carecen otros desarrollos, como la capacidad de actuar instantáneamente para proteger frente a determinadas agresiones; y que puede concebirse su uso en algunos escenarios donde no habría riesgos probables de afectación de civiles.⁷⁰

⁶⁹ Vid. Kenneth Anderson et al., op. cit., págs. 389, 397.

⁷⁰ IHRC y Human Rights Watch, *Shaking the Foundations: The Human Rights Implications of Killer Robots*, 2014, págs. 2-4, 25; *versus* Kenneth Anderson et al., op. cit.; Guillermo Altares, “Los ‘robots asesinos’ salen de la ciencia ficción”, *El País (España)*, 9 de abril de 2015, disponible en: http://internacional.elpais.com/internacional/2015/04/08/actualidad/1428507664_013074.html (última visita: 9 de abril de 2015).

A lo anterior podría responderse que casi siempre será posible que haya presencia de civiles en uno de esos escenarios (ej. zonas despobladas), por accidente u otro motivo, sin que la tecnología necesariamente tenga la robustez suficiente para identificarlos, y que además de las posibles dificultades en la implementación de estándares por máquinas es ciertamente posible que haya presencia de errores en la programación o componentes de armas completamente autónomas que lleven a producir lesiones irremediables y contrarias al principio de proporcionalidad y de prohibición de ataque directo, en caso que sea aplicable el DIH, o de violación del derecho a la vida desde la perspectiva de los derechos humanos. Más aún, la determinación sobre la aplicación del DIH, o sobre si sería lícita determinada acción letal que busque proteger la vida de otros según el derecho internacional de los derechos humanos, a menudo entraña consideraciones jurídicas interpretativas con sutilezas o consideraciones caso por caso que no se aconseja confiar a una máquina. Por ello, considero que es aconsejable tener una aproximación basada en un principio de precaución frente a las armas en cuestión. Al respecto, puede decirse que los argumentos subyacentes a aquel principio no tienen por qué limitarse a cuestiones medioambientales y pueden ser ciertamente relevantes frente a desarrollos tecnológicos.⁷¹ Es interesante tener en cuenta que, desde un punto de vista filosófico e incluso científico, hay expertos que advierten sobre la importancia de ser precavidos frente a máquinas con autonomía muy desarrollada, que incluso tengan una elevada y verdadera inteligencia artificial, las cuales eventualmente podrían atacar o lesionar a seres humanos o errar con consecuencias nefastas. Además, no debe ignorarse que hay riesgos de que los *drones* y otros desarrollos tecnológicos sean

⁷¹ Sobre la discusión sobre la presencia de un principio de precaución presente o no en el derecho internacional general y sobre su implementación; y la defensa que hacen algunos de la relevancia del principio y sus argumentos no sólo frente a desarrollos científicos que puedan suponer una amenaza para el medio ambiente, sino además frente a otros bienes jurídicos internacionales y globales, ver: Jan Klabbers, *International Law*, Cambridge University Press, 2013, locations 8123-8130 (versión Kindle); Alberto Alemanno, “European Court of Justice Fails to Scrutinize Precautionary Principle”, *Penn Program on Regulation RegBlog*, 19 de septiembre de 2011; Opinión separada del juez Cançado Trindade a la sentencia de la Corte Internacional de Justicia de 20 de abril de 2010 en el caso *Pulp Mills on the River Uruguay (Argentina versus Uruguay)*, párrs. 62-94; Meinhard Schröder, “Precautionary Approach/Principle”, *Max Planck Encyclopedia of Public International Law*, 2014; IHRC y Human Rights Watch, op. cit., pág. 25.

adquiridos por terceros (estatales o no) de forma lícita o ilícita, y pueden ser incluso “hackeados” para ser usados de forma lesiva o ilícita.⁷²

Es interesante observar, además, que las dos posturas enfrentadas en cuanto a la prohibición preventiva (o en cuanto a la consideración de su prohibición implícita) o no de las armas autónomas esgrimen argumentos opuestos en relación con el papel de las emociones humanas y su carencia por parte de aquellas máquinas, cuestión que en ocasiones surge cuando se discute la conveniencia de permitir o no el uso de determinados desarrollos tecnológicos. Mientras que los detractores de su permiso argumentan que aquellas máquinas carecen de la posibilidad de tener empatía y realizar ciertos juicios, lo cual hace que sea conveniente dejar la toma de decisiones con posibles efectos letales sólo a los seres humanos; otros, que consideran que su uso puede ser lícito, enfatizan que, a diferencia de los individuos, ellas no tienen la capacidad de albergar rencor u odio, factores que a menudo influyen en decisiones humanas.⁷³

Como se ha indicado en este texto, además de dilucidar qué exige o permite el derecho frente a la tecnología y su impacto en los derechos humanos, en relación con ella también es posible desarrollar progresivamente, adoptar e implementar estándares procedimentales relativos a las competencias de órganos o mecanismos de cooperación, supervisión, promoción y vigilancia. Como ejemplo del reconocimiento de la importancia que pueden tener la creación y acción de órganos con competencias en la materia, pueden citarse la propuesta de creación de una agencia de las Naciones Unidas para protección y seguridad de datos confidenciales e información personal, formulada

⁷² Vid. Peter Holley, “Apple co-founder on artificial intelligence: ‘The future is scary and very bad for people’”, *The Washington Post*, 24 de marzo de 2015; Rory Cellan-Jones, “Stephen Hawking warns artificial intelligence could end mankind”, *BBC News Technology*, 2 de diciembre de 2014, disponible en: http://www.bbc.com/news/technology-30290540?utm_source=pocket&utm_medium=email&utm_campaign=pockethits (última visita: 10 de marzo de 2015); Stephen Luntz, “Scientists and Engineers Warn Of The Dangers Of Artificial Intelligence”, *IFLSCIENCE!*, 13 de enero de 2015, disponible en: <http://www.iflscience.com/technology/scientists-and-engineers-warn-artificial-intelligence> (última visita: 15 de enero de 2015); Taylor Hatmaker, “New malware makes drone hijacking a reality”, *The Daily Dot*, 28 de enero de 2015; Peter Holley, “Bill Gates on dangers of artificial intelligence: ‘I don’t understand why some people are not concerned’”, *The Washington Post*, 29 de enero de 2015.

⁷³ Vid. IHRC y Human Rights Watch, op. cit., págs. 10, 15-16, 25; versus: Kenneth Anderson et al., op. cit., págs. 393-394, 398.

por el comisionado europeo de economía digital; y la designación por parte del Consejo de Derechos Humanos de la ONU de un relator especial con competencia sobre el derecho a la privacidad que tenga en cuenta, entre otras y de forma especial, los desafíos que surgen para su goce y ejercicio en la “era digital”.⁷⁴ Ciertamente, los expertos con competencias concretas pueden brindar una mayor especialización en el examen de desafíos concretos y amenazas en la materia, pero es conveniente evitar una intra-fragmentación en el derecho internacional y promover la comunicación entre órganos generalistas y especializados.

Es el momento de pasar al estudio de otra clase de procesos jurídicos: ya no aquellos relacionados directamente con la identificación y regulación de normas, principios y estándares; sino aquellos que permiten orientar o influir (hasta cierto punto) en la actuación de los operadores jurídicos (de cualquier nivel: internacional o interno), de activistas, de los destinatarios de las normas y de sus beneficiarios frente a los desafíos generados por aquello que la tecnología permite hacer.

2. Procesos de interpretación, supervisión e implementación del derecho internacional para promover y procurar que el desarrollo, uso y adquisición de la tecnología respete los derechos humanos

La eventual necesidad de regular, *de lege ferenda*, la posibilidad de acudir a la *lex lata* para lidiar con desafíos para la protección de los derechos humanos, y el recurso a técnicas para procurar que se proteja en la mayor medida posible la dignidad humana frente a posibles riesgos tecnológicos, son procesos complementarios. En esta segunda sección se estudiará lo relativo a dichas técnicas, incluyendo aspectos relacionados con procesos de interpretación e implementación garantista del derecho internacional; y lo concerniente a la forma en que conviene que las autoridades y distintos actores se comporten para proteger a víctimas actuales y potenciales y abstenerse de conductas inadecuadas.

⁷⁴ Vid. Graeme Wearden y Jill Treanor, “UN needs agency for data protection, European commissioner tells Davos”, *The Guardian*, 22 de enero de 2015; Naciones Unidas, Asamblea General, *El derecho a la privacidad en la era digital*, A/HRC/28/L.27, 24 de marzo de 2015.

a. La toma de decisiones sobre la interpretación, norma o curso de acción a elegir para asegurar y promover el respeto de los derechos humanos frente a desafíos relacionados con el desarrollo, posesión y uso de la tecnología

Las decisiones sobre qué norma, interpretación o conducta se debe o recomienda elegir en caso de presentarse distintas alternativas aparentes, en relación con dilemas sobre qué se regula y cómo se puede proteger de mejor forma a los individuos frente a desafíos y posibilidades que ofrece la tecnología, deben tener en cuenta, en primer lugar, el principio *pro personae* o *pro homine*; el contenido actualizado y contextualizado de los derechos involucrados; la naturaleza, lógica, deberes y objetivos de las obligaciones de las autoridades y de quienes desarrollan o usan la tecnología; y los derechos de las posibles víctimas. Los ejemplos que se discutirán en esta sección ilustran el papel y la relevancia de estos tres elementos.

En cuanto al principio *pro homine*, puede decirse que él exige que en la interpretación e implementación del derecho y en la toma de decisiones se elija siempre la opción o norma aplicable más protectora.⁷⁵ A esto puede añadirse la exigencia de optar por las interpretaciones o conductas más respetuosas y garantes de los derechos humanos, incluso cuando las otras alternativas también sean lícitas *prima facie*. Quizás podría decirse que la “cláusula de Martens”,⁷⁶ por ejemplo, constituye un antecedente o manifestación de esta lógica y exigencia. Acudir al criterio *pro homine* será, por ello, muy útil ante situaciones en las que sea difícil responder al interrogante de cómo se debe actuar frente a usos y desarrollos tecnológicos cuando se dude si algo se permite o no; toda vez que aquel criterio obliga a optar por la opción más garante o respetuosa

⁷⁵ Vid. Mónica Pinto, “El principio *pro homine*. Criterios de hermenéutica y pautas para la regulación de los derechos humanos”, en Martín Abregú y Christian Curtis (eds.), *La aplicación de los tratados sobre derechos humanos por los tribunales locales*, 1997.

⁷⁶ La cláusula, incluida por primera vez en la Convención de la Haya (II) de 1899, dispone que “[m]ientras aguardan que un código más completo de las leyes de la guerra pueda ser dictado, las Altas Partes Contratantes juzgan oportuno hacer constar que, en los casos no comprendidos en las disposiciones reglamentarias adoptadas por ellas, las poblaciones y los beligerantes quedan bajo la salvaguardia y el imperio de los principios del derecho de gentes, tales como resultan de los usos establecidos entre las naciones civilizadas, de las leyes de humanidad y de las exigencias de la conciencia pública”. Ver: Jean-Marie Henckaerts y Louise Doswald-Beck, op. cit., págs. XXIX-XXX.

(según el caso), como sucede por ejemplo frente a la pregunta de si y cómo los “ataques cibernéticos” pueden justificar una pretendida legítima defensa o en lo concerniente al deber de las autoridades de proteger a los afectados frente a acciones abusivas, como el “ciber bullying”, que son contrarias a derechos humanos y se cometen aprovechándose de la tecnología.

Por otra parte, también se debe analizar la crucial cuestión del acceso a recursos efectivos de protección y reclamación de reparaciones frente a alegaciones de usos estatales o no estatales de las tecnologías que sean presuntamente contrarios a los derechos humanos. Esta cuestión no es baladí. Teniendo en cuenta que debe protegerse a todas las víctimas, cualquiera sea la identidad del agresor, como exigen el principio de igualdad y la prohibición de discriminación (de carácter imperativo),⁷⁷ no puede ignorarse la angustiante realidad de muchas de víctimas de Estados o entes no estatales que afectan sus derechos empleando desarrollos tecnológicos y que carecen de opciones eficaces para reclamar y presentar sus legítimas demandas, siendo el acceso a aquellas opciones en ocasiones muy complejo o inexistente por razones fácticas o jurídicas, como ha sucedido por ejemplo con personas afectadas directa o indirectamente en Pakistán por ataques de *drones*.⁷⁸ Esto confirma que el análisis sobre las aplicaciones y conductas más garantistas no puede restringirse a cuestiones sustantivas, sino que además es pertinente frente a aspectos procedimentales, que son cruciales para el goce y ejercicio de los derechos humanos.

Como ejemplo del papel de los criterios que han de orientar acciones y decisiones de respeto y protección, puede mencionarse el caso en el que una autoridad estatal se pregunte qué debe hacer frente a quienes sean víctimas del denominado matoneo

⁷⁷ Vid. Jessica Almqvist, “Facing the Victims in the Global Fight against Terrorism”, *Fride Working Papers*, N° 18, 2006, págs. 13-16; Corte Interamericana de Derechos Humanos, Opinión consultiva OC-18/03, *Condición Jurídica y Derechos de los Migrantes Indocumentados*, 17 de septiembre de 2003, párrs. 101, 137-154.

⁷⁸ Ver United Nations Office at Geneva (UNOG), “Human Rights Council Holds Panel on Remotely Piloted Aircraft or Armed Drones in Counterterrorism and Military Operations”, 22 de septiembre de 2014 (disponible en: http://www.unog.ch/unog/website/news_media.nsf/%28httpPages%29/BCE56ED914A46D40C1257D5B0038393F?OpenDocument, última visita: 10 de marzo de 2015); y el video sobre el evento, referenciado en el pie de página número 4, *supra*.

cibernético, acoso cibernético o *cyberbullying* (agresiones o intimidaciones por o en medios virtuales)⁷⁹ cuando advierte o le es puesto en su conocimiento que alguien está siendo hostigado de forma intensa en redes sociales (por ejemplo, cuando se amenaza con distribuir imágenes comprometedoras) sin que sea claro si se ha incurrido en un tipo penal o si se ha violado el derecho interno. En estos supuestos, la autoridad en cuestión debe, en primer lugar, advertir y reconocer si hay una violación o amenaza al goce y ejercicio de derechos humanos en algún ámbito normativo: sea internacional o interno, y además se exige que tenga en cuenta el contenido más garantista (de forma incluso híbrida: puede haber elementos más garantes en un nivel y otros en otro orden, debiendo combinarse en tales supuestos). Si al menos en *uno* de aquellos ámbitos normativos puede considerarse que un comportamiento atenta contra los derechos humanos, la autoridad debe esforzarse para que se protejan los derechos en cuestión.

Precisamente en cuanto al *cyberbullying*, el Comité de los Derechos del Niño ha advertido que el mismo es contrario a los derechos humanos de los niños⁸⁰ (y también de adultos, puede añadirse, algo que probablemente no afirmó por ser esta una cuestión que escapa a la competencia *ratione personae* de aquel Comité), al considerar que la violencia mental, contra la que se debe dar protección efectiva (según el artículo 19 de la Convención sobre los Derechos del Niño), puede manifestarse en la “intimidación y las novatadas de adultos o de otros niños, en particular por medio de tecnologías de la información y las telecomunicaciones (TIC) como los teléfonos móviles o Internet (la práctica llamada “acoso cibernético”)⁸¹.

Aunque el Comité dijo lo anterior en una observación general (número 13), que no es vinculante en términos formales, este tipo de opiniones expresadas por órganos con

⁷⁹ Vid. “Corte Constitucional pide al Gobierno una política contra el matoneo”, *El Tiempo* (Colombia), 19 de diciembre de 2014, disponible en: <http://www.eltiempo.com/politica/gobierno/matoneo-corte-constitucional-pide-al-gobierno-una-politica/14996048> (última visita: 19 de diciembre de 2014).

⁸⁰ Vid. Comité de los Derechos del Niño, Observación general N° 13, *Derecho del niño a no ser objeto de ninguna forma de violencia*, CRC/C/GC/13, 18 de abril de 2011, párrs. 21.

⁸¹ *Ibid.*

competencia en materia de derechos humanos (u otras cuestiones, según el caso) deben ser analizadas de buena fe a la luz de criterios de razonabilidad.⁸²

La opinión del Comité es muy persuasiva y se basa en el reconocimiento de que las personas pueden verse afectadas por acciones que se presenten en un entorno virtual, de internet o de mensajería, entre otros. Por ello, la autoridad que dude si su derecho interno ordena proteger a sus víctimas frente a aquellas conductas o sabe que la conducta en cuestión no está prohibida *internamente* debe entender que, al estar consagrada la obligación de proteger derechos humanos frente a terceros *directamente* en el derecho internacional, debe ofrecer aquella protección: esto se fundamenta, en primer lugar, en el deber de todo agente estatal para hacer que su Estado actúe diligentemente de conformidad con sus compromisos internacionales de protección de derechos internacionalmente reconocidos.⁸³ A esto se suma la posibilidad de que el derecho internacional regule *directamente* deberes y responsabilidades de actores no estatales, incluyendo a los individuos, y de que los Estados implementen las respectivas normas, como se vislumbra en los principios de Núremberg y se reconoce en la doctrina y en decisiones como la del Tribunal Europeo de Derechos Humanos en el caso *Kononov*.⁸⁴ Al respecto, puede añadirse que todo actor y toda conducta que pueda afectar derechos reconocidos y protegidos internacionalmente tiene una innegable

⁸² Ver una manifestación de estas consideraciones en: Corte Internacional de Justicia, *Caso Ahmadou Sadio Diallo (República de Guinea Vs. República Democrática del Congo)*, Sentencia, 30 de noviembre de 2010, párrs. 66-68.

⁸³ Vid. Corte Interamericana de Derechos Humanos, *Caso Almonacid Arellano y otros Vs. Chile*, Sentencia de 26 de septiembre de 2006, párrs. 124-125.

⁸⁴ Vid. Tribunal Europeo de Derechos Humanos (Gran Sala), *Caso Kononov Vs. Letonia*, Sentencia de 17 de mayo de 2010, párrs. 185-186, 207, 213, 230, 235-244; Comisión de Derecho Internacional, *Principles of International Law recognized in the Charter of the Nürnberg Tribunal and in the Judgment of the Tribunal, with commentaries*, Yearbook of the International Law Commission, 1950, Principio I y párrs. 98-99; Theodor Meron, *The Humanization of International Law*, Martinus Nijhoff, 2006, pág. 40; Theodor Meron, "The humanization of humanitarian law", *American Journal of International Law*, Vol. 94, 2000, pág. 253.

relevancia jurídica que exige una respuesta, como exigen el *rule of law*⁸⁵ y la protección *universal* (no sólo en términos geográficos) de los derechos humanos.⁸⁶

Dicho esto, si una autoridad estatal advierte que hay una amenaza en un entorno tecnológico o con medios tecnológicos, pero carece de la competencia o capacidad para ofrecer una protección efectiva (que debe ser suministrada por el Estado, tener perspectivas de éxito y no ser meramente formal o ilusoria),⁸⁷ tendrá el deber ineludible de poner la situación en conocimiento del órgano o agente con la capacidad de brindarla, para buscar que se cumpla con el deber estatal de velar por el respeto del derecho y por la garantía de los derechos humanos. Otro deber internacional pertinente es el relativo a asegurar la compatibilidad del derecho interno y su aplicación con los estándares internacionales sobre derechos humanos.⁸⁸ Esta obligación exige a las autoridades que conocen un caso de violación cibernética o de otra índole cuyo derecho interno no aborde expresa y directamente que informen a quienes pueden modificarlo sobre la necesidad de llenar los vacíos (o aplicar la ley) para lograr que se respeten aquellos estándares. En este sentido, en su observación general referida atrás, el Comité de los Derechos del Niño expresó que para garantizar los derechos de los niños (y que se cumpla el derecho internacional) puede ser necesario aprobar normas, políticas, programas y asociaciones de protección frente a la ciberdelincuencia.⁸⁹

Otro ejemplo que ilustra la importancia de que se tomen medidas para acabar con una situación de indefensión se refiere a las respuestas frente a casos de toma y divulgación electrónica de fotografías íntimas sin autorización en los Estados Unidos de América.

⁸⁵ Vid. Janne E. Nijman, “Non-state actors and the international rule of law: Revisiting the ‘realist theory’ of international legal personality”, *Amsterdam Center for International Law Research Paper Series*, 2010, págs. 7-19, 40.

⁸⁶ Nicolás Carrillo Santarelli, “Enhanced Multi-Level Protection of Human Dignity in a Globalized Context through Humanitarian Global Legal Goods”, *German Law Journal*, Vol. 13, 2012, págs. 850-851.

⁸⁷ Vid. Tribunal Europeo de Derechos Humanos (Sección Cuarta), *Caso Hajduová Vs. Eslovaquia*, Sentencia de 30 de noviembre de 2010, párr. 41; Corte Interamericana de Derechos Humanos, *Caso 19 Comerciantes Vs. Colombia*, Sentencia de 5 de julio de 2004, párrs. 184, 192.

⁸⁸ Vid. Corte Interamericana de Derechos Humanos, *Caso Suárez Rosero Vs. Ecuador*, Sentencia de 12 de noviembre de 1997, párrs. 96-99; Corte Interamericana de Derechos Humanos, *Caso “La Última Tentación de Cristo” (Olmedo Bustos y otros) vs. Chile*, Sentencia, op. cit., párr. 87, y voto concurrente del juez Cançado Trindade a la anterior sentencia, párrs. 1-27.

⁸⁹ Vid. Comité de los Derechos del Niño, Observación general N° 13, op. cit., párr. 76.

Al examinarlos, se observó que, según el derecho de algunos Estados federados, conductas de esa índole no eran consideradas ilícitas, lo que motivó a algunos Estados, como Massachusetts o Texas, a prohibirla y generó iniciativas de activismo y de crítica a la ley existente⁹⁰ (curiosamente, y de forma decepcionante, en Texas se estimó que la prohibición penal adoptada posteriormente era contraria a la primera enmienda de la Constitución estadounidense). En el Reino Unido hubo una iniciativa (fallida) en la misma línea.⁹¹

Este caso pone de relieve otros aspectos esenciales a la hora de tomar decisiones que puedan tener un impacto en la protección de los derechos humanos: el hecho de que pueden presentarse enfrentamientos o colisiones entre derechos y la posibilidad de realizar algunas restricciones de derechos de forma lícita. En ambos supuestos, es relevante la consideración de que la conducta de individuos, empresas u otros entes que se sirva de la tecnología puede afectar derechos de los demás e intereses públicos pertinentes, lo que exige indagar qué se debe hacer para protegerlos de forma proporcionada y que sea respetuosa con las condiciones jurídicas internacionales, entre las que se incluye la prohibición de violaciones de derechos humanos por parte de las autoridades incluso cuando ellas pretendan o digan intentar proteger otros derechos básicos.⁹² Desde la perspectiva de los actores privados, también se debe reconocer que los derechos humanos no justifican ni protegen su violación o la supresión de los derechos de los demás, como enuncia la Declaración Universal de los Derechos Humanos en su artículo 30.⁹³

⁹⁰ Vid. Caitlin Dewey, "Even at a national memorial, no one is safe from 'creepshots'", *The Washington Post*, 10 de octubre de 2014 (disponible en: <http://www.washingtonpost.com/news/the-intersect/wp/2014/10/10/even-at-a-national-memorial-no-one-is-safe-from-creepshots/>, última visita: 11 de marzo de 2015); Caitlin Dewey, "Some creep is prowling the D.C. Metro filming women for a porn site, and there's nothing you can do about it", *The Washington Post*, 30 de diciembre de 2014.

⁹¹ Ibid.; Peter Walker, "Tory MP Christopher Chope blocks progress of upskirting bill", *The Guardian*, 15 de junio de 2018.

⁹² Vid. Corte Interamericana de Derechos Humanos, *Caso del Penal Miguel Castro Castro Vs. Perú*, Sentencia de interpretación de 2 de agosto de 2008, párrs. 40-42; Comisión Interamericana de Derechos Humanos, *Informe sobre terrorismo y derechos humanos*, OEA/SER.L/V/II.116 Doc. 5 rev. 1 corr., 22 de octubre de 2002, párrs. 3-4, 22.

⁹³ Vid. Declaración Universal de Derechos Humanos, artículo 30.

En los supuestos en los que haya una aparente tensión entre ejercicios de derechos humanos, ha de acudir a criterios y análisis como el del test de proporcionalidad, evitando la negación total (en abstracto o en la práctica) de uno de los derechos involucrados y teniendo en cuenta las circunstancias de cada caso concreto,⁹⁴ asegurando la prevalencia de derechos absolutos o imperativos. Como ejemplo interesante de estas consideraciones se puede mencionar que, en relación con el acceso a internet que, según el relator especial de Naciones Unidas dedicado a las libertades de pensamiento y expresión, es un derecho humano, se ha considerado que la protección de derechos de propiedad intelectual no puede hacerse a costas de la eliminación absoluta de aquel acceso, que es importante para ejercer libertades fundamentales, pues ello sería desproporcionado; y que es importante tener en cuenta asuntos medioambientales relacionados que puedan verse afectados.⁹⁵

Además de acudir a las opciones interpretativas y normativas más garantistas, de aplicar criterios de proporcionalidad en eventos de colisión de derechos y de cumplir con los requisitos para poder restringir derechos cuando sea el caso, otro proceso de interacción con el derecho internacional pertinente es el consistente en presentar reclamaciones ante órganos judiciales (o cuasi-judiciales) internacionales de supervisión. Como ejemplo de estas dinámicas encontramos la decisión de Amnistía Internacional de llevar un caso relativo a la práctica británica de obtención de información de comunicaciones revelada por Edward Snowden ante el Tribunal Europeo de Derechos Humanos. Esta ONG manifestó que llevaría el caso ante aquel órgano judicial internacional tras conocerse la decisión del *Investigatory Powers Tribunal* que afirmó (tras un proceso que, de forma curiosa y decepcionante, no fue público en su totalidad, sin que tampoco fuesen públicas todas las afirmaciones y fuentes de información en que se basaba el gobierno

⁹⁴ Vid. Rita Joseph, *Human Rights and the Unborn Child*, Martinus Nijhoff Publishers, 2009, pág. 239; Andrew Clapham, *Human Rights Obligations of Non-State Actors*, op. cit., págs. 529-531; Andrew Clapham, *Human Rights: a Very Short Introduction*, Oxford University Press, 1997, págs. 92, 97-99; Dawn Oliver and Jörg Fedtke, *Human Rights and the Private Sphere: A Comparative Study*, Routledge, 2007, págs. 18, 508-509; Dawn Oliver, "Human Rights and the Private Sphere", *UCL Human Rights Law Review*, Vol. 1, 2008, págs. 10-15; Jonas Christoffersen, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights*, Martinus Nijhoff Publishers, 2009, págs. 108-111; Xiaobing Xu, "On Conflict of Human Rights", *Pierce Law Review*, Vol. 5, 2006, págs. 40-53.

⁹⁵ Vid. David Rothkopf, "Is Unrestricted Internet Access a Modern Human Right?", *Foreign Policy*, 2 de febrero de 2015; David Kravets, "U.N. Report Declares Internet Access a Human Right", *Wired*, 3 de junio de 2011.

británico) que hay suficientes límites jurídicos y controles para asegurar el respeto de derechos cuando se presente aquella práctica; algo rechazado por la ONG y que confirma el hecho de que sobre ella se conoce sólo como consecuencia de las revelaciones de Snowden.⁹⁶ En este caso, no sólo se discutía la licitud de posibles restricciones a los derechos (cuestión que puede emplearse en ocasiones cuando haya enfrentamientos en el ejercicio de derechos en relación con la tecnología), sino que además se revela la importancia de contar con posibilidades de cuestionar decisiones internas relativas a determinados usos de la tecnología o acciones en espacios digitales, para exigir la protección del ejercicio de derechos humanos. En el trámite de los procesos jurídicos de reclamo y solicitud de decisiones o recomendaciones internacionales se exige y permite ejercer la identificación de normas aplicables y su interpretación y aplicación *pro homine* (o que sea garantista de otra manera). La activación de tales procedimientos además permite que las distintas partes revelen sus argumentos, fomentando una dialéctica y exponiendo asuntos importantes ante el público, amén de permitir la protección en casos concretos.

Otro escenario que se relaciona con la aplicación humanizada del derecho internacional frente a aspectos relacionados con la tecnología es el relativo a la lucha (respetuosa de la legalidad internacional) contra actividades que aprovechan de la tecnología con el fin de facilitar o causar violaciones de derechos humanos. Como ejemplo, se encuentra la lucha contra el apoyo al terrorismo que se da en internet. Al respecto, se cuenta con la Resolución 2178 (2014) del Consejo de Seguridad, donde se expresa preocupación por el uso de internet por parte de terroristas y quienes los apoyan. En ella se manifiesta la disposición del Consejo a actuar por medio de inclusiones en una lista a personas físicas y jurídicas o a cualquier grupo o ente que apoye (por ejemplo, financiando, reclutando, suministrando armas o planificando) a entes relacionados con Al-Qaida, “incluso mediante tecnologías de la información y las comunicaciones, como Internet, los

⁹⁶ Vid. Amnistía Internacional, “UK court decision on government mass surveillance: ‘Trust us’ isn’t enough”, *News*, 5 de diciembre de 2014, disponible en: <http://www.amnesty.org/en/news/uk-court-decision-government-mass-surveillance-trust-us-isnt-enough-2014-12-05?linkId=10999428> (última visita: 5 de diciembre de 2014).

medios sociales, o por cualquier otro medio”.⁹⁷ En discusiones, los representantes de Francia, Jordania, China e Irak manifestaron su preocupación por el posible uso de internet por parte de terroristas para desarrollar sus estrategias y acciones.⁹⁸ En la resolución, afortunadamente, se mencionó que las acciones y cooperación de lucha contra el terrorismo deben respetar, entre otras, las obligaciones en materia de derechos humanos; y en concreto se manifestó que ellas deben observarse cuando se realicen acciones para contrarrestar e impedir el aprovechamiento de “tecnologías, comunicaciones y recursos, en particular de audio y vídeo, para incitar al apoyo de actos terroristas”.⁹⁹ Este ejemplo ilustra la importancia de optar por el criterio más protector, teniendo en cuenta el contenido de los derechos de forma actualizada a la luz los últimos desarrollos jurídicos y tecnológicos y de necesidades de protección (lo que nos remite a la primera sección), incluyendo aquellas a las que se refieren los deberes de protección y respeto de las autoridades; y acentúa cómo es posible y conveniente actuar para frenar posibles abusos que se cometen por actores que se sirven de la tecnología.

Un caso adicional que ilustra elementos mencionados en esta subsección que ha sido ampliamente discutido y complejo es el relativo a los ataques cibernéticos y la discusión sobre si es posible reaccionar en legítima defensa contra ellos.

A mi parecer, las reacciones admisibles frente a “ataques cibernéticos” son, por lo *general*, a lo sumo, contramedidas que han de cumplir con todos sus requisitos;¹⁰⁰ y sólo en casos excepcionales sería posible hablar de usos mayores de la fuerza cibernéticos que autoricen a responder en una legítima defensa, encarnada por su parte en acciones cibernéticas o cinéticas que cumplan con todos los requisitos de la legítima defensa, como la provisionalidad, necesidad o proporcionalidad.¹⁰¹ Estas dos últimas

⁹⁷ Vid. Resolución 2178 (2014) del Consejo de Seguridad, 24 de septiembre de 2014, Preámbulo y párr. 7.

⁹⁸ Vid. Naciones Unidas, “Security Council Unanimously Adopts Resolution Condemning Violent Extremism, Underscoring Need to Prevent Travel, Support for Foreign Terrorist Fighters”, *Meetings Coverage*, 24 de septiembre de 1997 (disponible en: <http://www.un.org/press/en/2014/sc11580.doc.htm>, última visita: 12 de marzo de 2015).

⁹⁹ Vid. Resolución 2178 (2014), op. cit., Preámbulo, párrs. 5, 11 y 17.

¹⁰⁰ Vid. Michael N. Schmitt (editor), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, pág. 52.

¹⁰¹ *Ibid.*, págs. 61-63.

condiciones, sumadas a la idea de que se ha de buscar la *defensa* frente a ataques que supongan un uso mayor de la fuerza, puede hacer que en ocasiones la respuesta a ellos deba ser necesariamente cibernética y no física, o que haya de dirigirse exclusivamente contra la fuente de las acciones cibernéticas que puedan generar afectaciones a la vida e integridad de las personas o de bienes militares. Adicionalmente, puede que la respuesta física que se permita en ocasiones excepcionales haya de dirigirse contra, por ejemplo, los equipos que permitieron la realización de las operaciones agresoras en cuestión¹⁰² (por ejemplo, que se usaron para un ataque cibernético que destruyó instalaciones y acabó con vidas). Estas consideraciones ciertamente se basan en el criterio de que las acciones bélicas han de ser excepcionales (lo cual es razonable considerando la afectación de los seres humanos en escenarios bélicos), lo que a su vez busca contribuir a la humanización de la regulación internacional y de la aplicación del derecho internacional.

Según mi criterio, incluso cuando sea lícito actuar en legítima defensa en un caso concret, puede considerarse que, en virtud de la proporcionalidad, si el acto al que se responde no lesionó ni causó la muerte de seres humanos, tampoco puede generar estas consecuencias un acto de legítima defensa lícita, en virtud de los deberes de los implicados, el criterio *pro personae* y la naturaleza de los derechos afectados. En este sentido, el requisito de proporcionalidad, mencionado atrás, es un elemento del derecho de la legítima defensa y del deber de respetar la regulación del uso de la fuerza, y se puede considerar que entraña una exigencia de *equivalencia* de naturaleza de los elementos de acción ofensiva (ej. si no se ataca a seres humanos sino sólo a bienes, sólo los ataques contra estos últimos de forma ponderada podrían ser proporcionales, jamás los dirigidos contra individuos). La implicación de la tecnología en cuestiones sobre uso de la fuerza revelaría entonces contornos antes ignorados de su regulación. Algunas cuestiones sobre la guerra cibernética se han discutido en el Manual de Tallin sobre el derecho internacional aplicable a la guerra cibernética (que, evidentemente, no es vinculante)¹⁰³ y en otros medios, reconociéndose la relevancia actual de la cuestión.

¹⁰² Vid. Antonio Remiro Brotons et al., *Derecho Internacional: Curso general*, op. cit., págs. 690-691.

¹⁰³ Vid. sección “International Acceptance and Applicability” de la entrada *Tallinn Manual* en Wikipedia (http://en.wikipedia.org/wiki/Tallinn_Manual#International_Acceptance_And_Applicability, última

En cuanto a la excepcionalidad de acciones cibernéticas que puedan ser consideradas usos mayores de la fuerza, conviene tenerse en cuenta que no todo acto de coerción supone un uso de la fuerza: por ejemplo, no lo sería ayudar a hackers que actúan contra un gobierno sin lesionar seres humanos o sin que generen consecuencias cinéticas que causen lesiones o daños a bienes militares. Sin embargo, frente a esas acciones y al apoyo a las mismas se ha de tener presente que hay actos que no son contrarios a la prohibición internacional del uso de la fuerza pero atentan contra otras normas como la prohibición de intervenir en los asuntos de otros Estados,¹⁰⁴ lo que puede ocurrir con determinados usos de la tecnología que, en consecuencia, adolecerían de ilicitud. Aunque en ciertas situaciones algunos Estados (por conveniencia, para tener una excusa de atacar o por otros motivos) pueden verse tentados o ser más proclives a calificar de usos de la fuerza muchas operaciones cibernéticas,¹⁰⁵ creo que en términos jurídicos para realizar esa calificación debe haber un ataque grave o de escala considerable realizado por cualquier medio,¹⁰⁶ incluso cibernético, con la *intención* y capacidad de que haya como efecto una lesión intensa de bienes o personas físicamente, por lo que acciones como el espionaje cibernético, careciendo del respectivo vínculo de causalidad, no facultarían para acudir a la legítima defensa.¹⁰⁷

Debe manifestarse que aunque algunos expertos están de acuerdo con el requisito de la intencionalidad del daño mencionado, otros no lo están y consideran que es suficiente con que los elementos de escala y efectos estén presentes.¹⁰⁸ Insisto en mi estimación de que sí debe darse la intencionalidad mencionada junto a los demás requisitos generales

visita: 12 de marzo de 2015); *Tallinn Manual on the International Law Applicable to Cyber Warfare*, op. cit.,

¹⁰⁴ Vid. Antonio Remiro Brotons et al., *Derecho Internacional: Curso general*, op. cit., págs. 100-103; *Tallinn Manual on the International Law Applicable to Cyber Warfare*, op. cit., pág. 46; Resolución 2625 (XXV) de la Asamblea General de la ONU, sección sobre “El principio relativo a la obligación de no intervenir en los asuntos que son de la jurisdicción interna de los Estados”, donde se expresa que “no solamente la intervención armada puede implicar una injerencia prohibida en el derecho internacional; Corte Internacional de Justicia, *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua Vs. Estados Unidos de América)*, Sentencia de fondo de 27 de junio de 1986, párrs. 202-205, 209.

¹⁰⁵ Vid. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, op. cit., págs. 48-52.

¹⁰⁶ *Ibid.*, págs. 54-55.

¹⁰⁷ *Ibid.*, pág. 55 (donde se muestra una postura que concuerda con mi consideración).

¹⁰⁸ *Ibid.*, pág. 57.

y específicos para que pueda haber legítima defensa frente a acciones cibernéticas. Esto busca evitar que se justifiquen a la ligera acciones que pueden causar grandes sufrimientos en perjuicio de muchos. Por otra parte, es curioso añadir que, si se acepta la posibilidad de actuar en legítima defensa contra actores no estatales (discutida en la sección 1, que cierta práctica parece apoyar), se colegiría que se podría responder en legítima defensa frente a aquellos ataques cibernéticos que constituyan usos mayores de la fuerza y sean atribuibles a Estados con un control efectivo sobre los actores no estatales que los cometen o sean imputables a entes no estatales sin que el Estado en cuyo territorio se encuentren puedan o deseen hacerles frente, cumplidas las restantes condiciones pertinentes.¹⁰⁹

Adicionalmente, a diferencia de los argumentos que buscan justificar la legítima defensa frente a toda acción cibernética que debilite capacidades militares de un Estado, creo que los “ataques” cibernéticos que no afecten la vida o integridad de individuos o no impliquen la destrucción de bienes militares (caso en el que sólo se podría atacar a otros bienes sin afectar a individuos) no se han de permitir respuestas que consistan en usos de la fuerza, que no obstante sí podrían darse como respuesta a ataques posteriores que causen violaciones al derecho a la vida e integridad personal de individuos o destruyan bienes militares aprovechándose del debilitamiento previo de las capacidades defensivas de un Estado obtenido por medio de acciones cibernéticas. A mi juicio, en caso contrario se afectarían derechos humanos y se victimizaría a seres que sienten y sufren por dar primacía a determinadas consideraciones sobre entes contingentes y construidos socialmente como lo son los Estados. En otras palabras, de darse una respuesta armada no habría una equivalencia de los derechos afectados. Es importante remitirse a la idea de que los derechos humanos tienen un carácter especial (cuasi-constitucional o constitucional en cuanto al contenido protegido por el derecho imperativo y obligaciones *erga omnes*).¹¹⁰

¹⁰⁹ Ibid., págs. 58-59.

¹¹⁰ Vid. Stefan Kirchner, “Relative Normativity and the Constitutional Dimension of International Law: A Place for Values in the International Legal System?”, *German Law Journal*, Vol. 5, 2004, págs. 56-61.

Con las consideraciones ofrecidas en esta subsección, en resumen, se sostiene que hay operaciones con herramientas tecnológicas que pueden generar problemas y dudas en autoridades y distintos actores sobre cómo se puede o debe actuar, y que en estos eventos se debe acudir a criterios como el de la elección de la norma o conducta más garante y/o respetuosa de los derechos humanos, entre otros, para identificar cuál es la *diligencia debida* en relación con la satisfacción de exigencias internacionales, entre las que se incluyen la reparación de los afectados y su acceso a recursos de protección, prevención y respuesta frente a desafíos tecnológicos, que será examinada en la siguiente subsección. Evidentemente, en ocasiones acudir a aquellos criterios será insuficiente. En estos casos, será necesario realizar estudios y procesos normativos (como los estudiados en la primera sección), recalándose la importancia de que distintos procesos jurídicos se complementen.

b. Recursos internos, no estatales e internacionales de protección y prevención y la reparación de las víctimas frente a riesgos y abusos permitidos, intensificados, facilitados o cometidos por el uso de tecnologías

Consideraciones éticas y jurídicas exigen que toda persona cuyos derechos humanos puedan ser afectados por usos indebidos de la tecnología atribuidos a cualquier ente sea protegida y pueda, además, exigir garantías preventivas y reparaciones. Esta exigencia general se concreta de diversas maneras: en el deber de todo sujeto al que se le impute la violación de una obligación internacional a su cargo de reparar a sus víctimas; en responsabilidades sociales de respetar y reparar (en ocasiones, incluso si no se violan preceptos jurídicos); en el derecho de las víctimas a recibir una reparación integral, cuya satisfacción frecuentemente exige que todo participante en las violaciones repare (por ejemplo, porque sólo los cómplices conocen parte relevante de la verdad, o porque se necesita que todo participante pida disculpas para que se satisfaga plenamente a las víctimas); en el deber de los Estados y sujetos responsables de proteger y poner a disposición de las víctimas recursos de reclamación y solicitud de protección; y en el

deber de las autoridades de proteger e investigar de oficio violaciones graves, entre otras manifestaciones y garantías.¹¹¹

La cuestión de la protección y la reparación es tan importante que constituye uno de los aspectos cardinales del derecho internacional de los derechos humanos. Por este motivo, se debe examinar de forma ineludible en caso de advertirse riesgos o la presencia de afectaciones de derechos humanos causados por el uso o desarrollo de aplicaciones tecnológicas.

La práctica confirma esta necesidad. Por ejemplo, el estudio sobre armas autónomas realizado por Human Rights Watch y la *International Human Rights Clinic* de la Universidad de Harvard examinó en un apartado específico cuestiones relativas a la reparación de las víctimas, y en él se expresó que el empleo de armas completamente autónomas puede obstaculizar la posibilidad de identificar *sujetos* responsables, lo que iría en detrimento de las víctimas y sus derechos.¹¹² Frente a esta inquietud considero que, en virtud de principios jurídicos y el interés de evitar que nadie responda y las víctimas queden desprotegidas en cuanto a su derecho de acceso a la justicia, el actor que decide emplear o ubicar armas u objetos con autonomía asume y crea un riesgo, lo que permite imputarle eventuales afectaciones de derechos según la doctrina de los deberes de prevención y protección que existen frente a riesgos creados, para evitar su materialización, siendo aquellos deberes son intensos. Por otra parte, creo que la responsabilidad o el contenido del deber de reparar sólo podría atenuarse o desaparecer si un tercer agente o actor, incluida muy excepcionalmente la víctima, decide o hace desencadenar una operación dañina con negligencia o conocimiento.¹¹³

¹¹¹ Vid. Corte Interamericana de Derechos Humanos, *Caso González y otras (“campo algodonero”) Vs. México*, Sentencia de 16 de noviembre de 2009, párrs. 288-294, 368.

¹¹² Vid. IHRC y Human Rights Watch, op. cit., págs. 19-22, 25.

¹¹³ Sobre estas cuestiones (diligencia y riesgo creado y comportamiento de la víctima), ver: Corte Interamericana de Derechos Humanos, *Caso de la Masacre de Pueblo Bello Vs. Colombia*, Sentencia de 31 de enero de 2006, párrs. 123, 126; Comisión de Derecho Internacional, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001, artículo 39 junto a su comentario, págs. 109-110.

Además de confirmar que el componente sobre garantías y reparaciones es ineludible en un análisis jurídico internacional humanizador sobre el uso de la tecnología, la preocupación de aquella ONG pone en evidencia distintos criterios que deben orientar todo análisis sobre la licitud internacional del uso de las tecnologías: la necesidad de que haya recursos efectivos (de prevención y protección o respuesta, según se haya cometido una violación o ella sea potencial) y de que se brinde una reparación integral a las víctimas, con el fin de perseguir los objetivos de evitar tanto la indefensión de las víctimas como la impunidad de la afectación negativa del goce y ejercicio de derechos humanos. En tanto el derecho internacional debe ofrecer esperanza de protección incluso si no es efectiva la protección de los derechos internos,¹¹⁴ aquellos objetivos hacen que sea importante contar, al menos, con un mínimo común denominador de protección encarnado en normas internacionales que determinen, cuando menos, *parámetros mínimos* de regulación interna y sirvan así para coordinar el enfrentamiento de problemas y desafíos y para evitar que haya soluciones aisladas, las que suelen ser ineficaces frente a problemas que distintos Estados y/o actores tengan en común.¹¹⁵

Todo esto explica el que, en numerosas discusiones sobre desarrollos y usos tecnológicos, como por ejemplo las relativas a vehículos aéreos no tripulados y operados a distancia que pueden realizar operaciones letales o de obtención de información, se preste atención de forma particularizada al tema de la reparación y los recursos a los que pueden acceder las víctimas. Por ejemplo, en un debate sobre *drones* que se realizó en Ginebra en el Consejo de Derechos Humanos, una de las cuestiones en las que se insistió fue la falta de *recursos* a los que pudieran acceder las víctimas de operaciones con *drones* en Pakistán, alegándose que ellas no podían litigar con facilidad en los Estados Unidos y que, pese a las promesas de algunos y a los esfuerzos y deseos de otros, no habían podido reclamar exitosamente contra el Estado estadounidense y

¹¹⁴ Ver el reconocimiento de *un* aspecto de esta exigencia en: Corte Interamericana de Derechos Humanos, *Caso Castillo Petruzzi y otros vs. Perú*, Sentencia de Excepciones Preliminares, 4 de septiembre de 1998, Voto concurrente del juez A. A. Cançado Trindade, párr. 35.

¹¹⁵ Vid. Anna Badia Martí, “Cooperación internacional en la lucha contra la delincuencia organizada transnacional”, en: Victoria Abellán Honrubia y Jordi Bonet Pérez, *La incidencia de la mundialización en la formación y aplicación del Derecho Internacional Público: los actores no estatales: ponencias y estudios*, Bosch editor, 2008, págs. 324-325, 337, 342-343.

tampoco se consideraba factible que pudieran obtener de forma exitosa reparaciones litigando en Pakistán.¹¹⁶

Otro análisis sobre cuestiones relativas a la tecnología y los derechos humanos nos permite identificar exigencias y consideraciones adicionales. La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, consciente de la posibilidad de que los Estados pidan u ordenen a las empresas que realicen acciones que puedan ser contrarias a la protección internacional de los derechos humanos, como ha sucedido con el derecho a la privacidad en internet y frente a comunicaciones electrónicas, ha señalado la importancia de los criterios de *publicidad* y de *facilitación* de la posibilidad de presentar reclamaciones sobre posibles daños y violaciones. En lo atinente al primero, se llama a las empresas en cuestión a comunicar e informar de forma transparente y oportuna sobre la forma en la que, por ejemplo, se almacenan y usan datos de los usuarios, lo que les permite a estos últimos tener conocimiento al respecto y advertir posibles irregularidades y afectaciones a sus derechos. En caso que estas existan, las empresas involucradas deben reparar, pudiendo hacerlo en el marco de procesos diseñados y gestionados por otros entes (como los Estados) o por ellas mismas, y se recomienda que dispongan de recursos propios que puedan activar los afectados (y complementen a los estatales) para facilitar la entrega rápida de medios de reparación, teniendo en cuenta la posibilidad de que haya Estados en los que “los derechos [humanos afectados por ellas, por instrucción estatal o no] no estén suficientemente protegidos o en que no se pueda acceder a recursos judiciales o de otra índole”.¹¹⁷ Conviene reiterar que entes como las empresas tienen actualmente, cuando menos, obligaciones jurídicas internacionales de no incurrir en violaciones (que afecten derechos humanos o distintos bienes jurídicos) de normas imperativas o que constituyan crímenes internacionales.¹¹⁸

¹¹⁶ Ver el pie de página 78, *supra*.

¹¹⁷ Vid. Consejo de Derechos Humanos de las Naciones Unidas, *El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, A/HRC/27/37, op. cit., párr. 46.

¹¹⁸ Vid. John H. Knox, “The Human Rights Council Endorses “Guiding Principles” for Corporations”, *ASIL Insights*, Vol. 15, 2011; Roland Portmann, op. cit., págs. 166-167, 280.

Además de lo relativo a la publicidad y facilitación de medios, la opinión comentada resalta el hecho de que puede haber entes no estatales (debe decirse que no sólo empresas, como se pone de manifiesto, por ejemplo, con las acciones grupos terroristas que reclutan en internet, cuestión que se discutió líneas atrás) implicados en actos contrarios al contenido y goce de derechos humanos que son realizados valiéndose de, o que son posibles gracias a, la tecnología; y que frente a tales actos y actores debe ofrecerse protección a las víctimas: también pero no sólo cuando el implicado sea un Estado (después de todo, la dignidad humana es incondicional, y a mi juicio una consecuencia lógica de ello es la idea de que su protección no puede hacerse depender de la identidad del agresor). Tal protección puede concretarse en normas y actos internacionales o internos, pero es importante que estos últimos sean, al menos, coordinados y exigidos por el derecho internacional (esta exigencia es tan sólo una de las tantas formas en las que el derecho internacional puede buscar la protección horizontal de los derechos humanos, pudiendo también regular obligaciones y procesos sobre entes no estatales directamente).¹¹⁹ La implicación del derecho internacional es importante y puede evitar vacíos o contradicciones y diferencias normativas internas de las que puedan aprovecharse entes abusadores en detrimento de las víctimas, quienes podrían quedar indefensas, caso en el que se incumplirían los objetivos de combatir la impunidad y la indefensión.

Por otra parte, aunque sólo se aborda sutilmente, la referencia a mecanismos y recursos ofrecidos por el propio ente implicado y la mención de los Principios Rectores sobre las empresas y los derechos humanos apuntan a otra consideración importante: que los recursos y garantías, para ser efectivos, deben cumplir con requisitos de legitimidad e inscribirse en un marco con múltiples niveles y actores y cooperación. Esto se refiere a la complementariedad entre distintos recursos, mecanismos, actores y autoridades; y entre mecanismos judiciales y no judiciales, estatales y no estatales (como se menciona en aquellos principios y el marco que desarrollan),¹²⁰ internacionales e internos,¹²¹

¹¹⁹ Vid. John H. Knox, “Horizontal Human Rights Law”, op. cit., págs. 18, 27-31.

¹²⁰ Vid. Naciones Unidas, *Principios Rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para “proteger, respetar y remediar”*, 2011, Principios 25 a 31, con sus respectivos comentarios, págs. 33-43; Consejo de Derechos Humanos de las Naciones Unidas,

jurídicos y sociales.¹²² Efectivamente, puede haber mecanismos de protección frente a usos tecnológicos contrarios a la dignidad humana que sean preventivos o *ex post facto*, algunos de los cuales pueden ser manejados por entes no estatales (por ejemplo, con procesos de supervisión interna), internacionales (por ejemplo, mediante medidas cautelares) o internos, como refleja la decisión de un tribunal británico que concluyó que hubo acuerdos de obtención e intercambio de información entre Estados Unidos y el Reino Unido que fueron contrarios a normas internacionales de derechos humanos.¹²³

Es importante asegurar que siempre haya un sustrato y fundamento jurídico (con un mínimo internacional concretado en disposiciones internas, que pueden ofrecer una protección que vaya más allá) de las exigencias de comportamiento y que siempre sea posible presentar reclamaciones judiciales, dada la incertidumbre de cumplimiento ligada a mecanismos voluntarios que, a pesar de poder promover procesos de socialización y aculturación, pueden usarse en algunos casos únicamente para mejorar la imagen sin que haya un compromiso real, o para desviar la atención de la sociedad civil de la necesidad de regular en términos vinculantes.¹²⁴ Estas consideraciones son aplicables no sólo frente a abusos empresariales de la tecnología sino además a los que sean atribuibles a los Estados u otros actores. Su objetivo es promover la protección (lícita y proporcionada) de la dignidad humana frente a cualquier amenaza, incluso las tecnológicas, sin que los formalismos sirvan de excusa para negar la protección requerida.¹²⁵

“Proteger, respetar y remediar: un marco para las actividades empresariales y los derechos humanos”, op. cit., párrs. 9, 26, 82-103.

¹²¹ Vid. Jean-Paul Costa, “Statement Issued by the President of the European Court of Human Rights concerning REQUESTS FOR INTERIM MEASURES (Rule 39 of the Rules of Court)”, 2011.

¹²² Vid. Amartya Sen, “Elements of a Theory of Human Rights”, *Philosophy & Public Affairs*, Vol. 32, 2004, págs. 325-328, 342-345, 349, 355-356; John H. Knox, “Horizontal Human Rights Law”, op. cit., pp. 43-44.

¹²³ Vid. Monica Moyo, “British Investigatory Powers Tribunal Rules Prior Intelligence Sharing Arrangements Between U.S. and U.K. Illegal”, *International Law in Brief*, 2015 (disponible en: <http://www.asil.org/blogs/british-investigatory-powers-tribunal-rules-prior-intelligence-sharing-arrangements-between-us>, última visita: 13 de marzo de 2015).

¹²⁴ Vid. Alexandra Gatto, “Corporate Social Responsibility in the External Relations of the EU”, *Yearbook of European Union Law*, 24, Oxford University Press, 2005, pág. 431.

¹²⁵ Vid. Elena Pariotti, “Non-State Actors, International Law, and Human Rights”, en Sanford R. Silverburg (ed.), *International Law: Contemporary Issues and Future Developments*, Westview Press, 2011, pág. 96.

El propósito de la implementación del derecho y de que haya prácticas consecuentes con, y guiadas por, la garantía y efectividad de los derechos humanos frente a desafíos tecnológicos, no puede ignorar la cuestión de los derechos económicos, sociales y culturales, tan olvidados (o desdeñados) por algunos. Al respecto, es necesario tener en cuenta que economistas y científicos debaten si las innovaciones y desarrollos tecnológicos a pasos agigantados afectarán, por ejemplo, al empleo (debido al reemplazo de algunos trabajadores por máquinas).¹²⁶ Esto exige pensar en estrategias sociales que debe perseguir el Estado (y en las que puedan cooperar distintos actores, relevantes para el suministro de bienes públicos globales¹²⁷) para procurar de forma diligente el goce y la efectividad de aquellos derechos, por todos los medios lícitos pertinentes y efectivos a su alcance, como recuerdan el Pacto y el Comité de Derechos Económicos, Sociales y Culturales.¹²⁸ A su vez, esto evidencia que los mecanismos de protección no son necesaria o exclusivamente judiciales o basados en reclamaciones, sino que deben incluir políticas públicas y distintas estrategias.

Las anteriores consideraciones resaltan la importancia de las víctimas y la centralidad de los seres humanos, quienes han de ser los protagonistas en cualquier análisis sobre protección, *reparaciones* y responsabilidad, incluso frente a violaciones o conductas no estatales, como podrían serlo las atribuibles a empresas que prestan servicios informáticos o de internet, a las que algunos les exigen mayor diligencia o supervisión para impedir que el uso de sus servicios pueda emplearse para discriminar o promover el terrorismo, por ejemplo; argumentando otros que ellas no deben imponer “mordazas” a la libertad de expresión, por ejemplo de quienes son bloqueados.¹²⁹ En últimas, es

¹²⁶ Vid. Lydia DePillis, “The definitive guide to whether or not a robot will take your job”, *The Washington Post*, 23 de marzo de 2015.

¹²⁷ Vid. Nicolás Carrillo Santarelli, “The Protection of Global Legal Goods”, *Anuario Mexicano de Derecho Internacional*, Vol. XIII, 2013, págs. 432-433; Nicolás Carrillo Santarelli, “Enhanced Multi-Level Protection of Human Dignity in a Globalized Context through Humanitarian Global Legal Goods”, op. cit., pág. 833.

¹²⁸ Vid. artículo 2 del Pacto Internacional de Derechos Económicos, Sociales y Culturales; Comité de Derechos Económicos, Sociales y Culturales, *La índole de las obligaciones de los Estados Partes (párrafo 1 del artículo 2 del Pacto)*, Observación general N° 3, 1990, párrs. 2-12.

¹²⁹ Vid. David Streitfeld, “Tech Giants, Once Seen as Saviors, Are Now Viewed as Threats”, *The New York Times*, 12 de octubre de 2017, disponible en: <https://www.nytimes.com/2017/10/12/technology/tech-giants-threats.html> (última visita: 23 de octubre de 2017); Theo van Boven, “The United Nations Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of

innegable que puede existir una relación (incluso causal en ocasiones) entre el goce y ejercicio de los derechos humanos y la tecnología tal como es empleada por Estados y otros actores.

Conclusiones

Es innegable que el rápido avance de la tecnología, que ha sobrepasado en ocasiones las expectativas de muchos y lo que se creía posible hasta hace poco, ha beneficiado de múltiples formas a la humanidad y permite a muchos individuos (quienes pueden pagar o son beneficiarios de servicios tecnológicos prestados por otros) gozar de una vida más cómoda y fácil en muchos aspectos (aunque también se generan problemas como adicciones). No obstante, es innegable que las posibilidades que permite la tecnología pueden ser aprovechadas por Estados u otros actores, incluyendo a autores de violaciones graves, masivas y sistemáticas (como, quizás, el Estado Islámico en Iraq y el Levante), para perseguir distintos objetivos, egoístas o no, lícitos y legítimos o no, y para realizar acciones que pueden ser abusivas y afectar a distintos entes.

Un caso curioso que pone de relieve algunos aspectos discutidos en este texto es el relativo a la sospecha (mencionada por oficiales de inteligencia estadounidenses y del FBI, entre otros, pero cuestionada por algunos otros) de que Corea del Norte (airada por el posible estreno de una película, llamada *The Interview*, en la que su líder es asesinado), o quizás otro actor, pudo haber robado información electrónica de *Sony Pictures Entertainment*, habiendo Sony ya sufrido acciones digitales lesivas anteriormente, como el robo de la información personal de jugadores en su *PlayStation Network*. Algunos propusieron que se diese una respuesta, cibernética o de otra naturaleza. Según los criterios expuestos en este texto, de *probarse* un hecho internacionalmente ilícito, la respuesta no podría ser armada en este supuesto. Es curioso, por otra parte, que Corea del Norte proclamó que la exhibición de una película sería un acto de guerra, lo que no sólo desconoce libertades sino que es además absurdo (y no creo que haya un elemento de *mens rea* o intencionalidad que permita hablar de

International Human Rights Law and Serious Violations of International Humanitarian Law”, *United Nations Audiovisual Library of International Law*, 2010, pág. 3.

incitación *-incitement* o *instigation*- a un crimen en este caso). Por otra parte, la sospecha de que Estados Unidos afectó el acceso a internet en Corea del Norte como respuesta a supuestas amenazas norcoreanas de que la exhibición de una película sería objeto de posibles ataques (lo que afectó inicialmente aquella exhibición), de comprobarse, también es problemática, pues la supuesta respuesta estadounidense pudo afectar el acceso a información y comunicaciones de muchos y el ejercicio de libertades en internet (aunque es probable que sólo los líderes norcoreanos o muy pocos otros tengan acceso libre a la red). Quizás, de ser cierta la sospecha de retaliación estadounidense, se pensó en contramedidas tomadas en beneficio de particulares afectados, lo que supondría un apoyo a la idea de que las contramedidas pueden tomarse por actores no afectados directamente (aunque no sería lícita en tanto violaría directamente derechos humanos, algo que no pueden hacer las contramedidas); aunque también se pudo considerar como una respuesta a un presunto daño al Estado, lo que no es claro en este caso. Adicionalmente, debe recordarse que se presentaron amenazas de posibles acciones atentatorias contra la integridad personal de espectadores de la película (que finalmente sí se exhibió, incluso en internet) y otros, las que suponen una intimidación contraria a las libertades de expresión y de acceso a la información.¹³⁰

¹³⁰ Sobre distintos aspectos relacionados con este complejo y en parte misterioso caso, ver: Brian Fung, "North Korea's internet is going suspiciously haywire", *The Washington Post*, 22 de diciembre de 2014; David Francis, "Obama Hammers Sony for Pulling 'The Interview'", *Foreign Policy*, 19 de diciembre de 2014; Wibke Kristin Timmermann, "Incitement in international criminal law", *International Review of the Red Cross*, Vol. 88, 2006, págs. 839, 841; David E. Sanger y Nicole Perlroth, "U.S. said to Find North Korea Ordered Cyberattack on Sony", *The New York Times*, 17 de diciembre de 2014, disponible en: http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?emc=edit_na_20141217&nlid=69013266&r=0 y Brooks Barnes y Michael Cieply, "Sony Pictures Cancels Holiday Release of 'The Interview' After Threats", *The New York Times*, 17 de diciembre de 2014, disponible en: http://www.nytimes.com/2014/12/18/business/sony-the-interview-threats.html?emc=edit_na_20141217&nlid=69013266 (última visita: 18 de diciembre de 2014); *The Independent*, "Isis releases drone footage of suicide bombings in Kobani", 11 de diciembre de 2014, disponible en: <http://www.independent.co.uk/news/world/middle-east/isis-release-drone-footage-of-suicide-bombings-in-kobani-9917198.html>; David Francis, "Did North Korea Finally Get Revenge for 'Team America: World Police?'" *Foreign Policy*, 2 de diciembre de 2014, disponible en: http://thecable.foreignpolicy.com/posts/2014/12/02/did_north_korea_finally_get_revenge_for_team_america_world_police?utm_content=bufferb6e41&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer (última visita: 3 de diciembre de 2014); David Francis, "Was the Sony Hack an Inside Job?" *Foreign Policy*, 5 de diciembre de 2014, disponible en: http://foreignpolicy.com/2014/12/05/was-the-sony-hack-an-inside-job/?utm_content=bufferd5a09&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer (última visita: 6 de diciembre de 2014); Isaac Stone Fish, "Should We Really Assume That North Korea Was Behind the Sony Attack?", *Foreign Policy*, 17 de diciembre de 2014, disponible en: http://foreignpolicy.com/2014/12/17/north_korea_sony_hack_interview/?utm_content=bufferc81c&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer (última visita: 18 de diciembre de 2014)

Este caso también refleja cómo los medios electrónicos pueden usarse para enviar mensajes de potenciales agresores e intimidar, lo que exige que se ofrezca protección a los agredidos potenciales, en virtud de los deberes positivos de los Estados, y que los actores privados se abstengan de irrespetar libertades y derechos, tanto los ejercidos en internet, como aquellos que podrían verse afectados por ciertos usos de la tecnología. En aquel caso también fue notable la petición estadounidense de cooperación china, lo que pone de relieve la importancia de la cooperación internacional para hacer frente a amenazas que se aprovechen de la tecnología, en vista de la insuficiencia e ineficiencia de acciones aisladas en un mundo interdependiente.¹³¹

Por otra parte, debe decirse que en tanto haya comportamientos que se sirvan de oportunidades e instrumentos tecnológicos y afecten a derechos e intereses jurídicos, el derecho y los operadores jurídicos han de responder para proteger a quienes puedan ser afectados, especialmente si ello conlleva la posible violación de derechos humanos, y así defender procesos de humanización jurídica. El derecho internacional puede ofrecer un mínimo común denominador que haga que se consideren ilícitas determinadas acciones con independencia de la cooperación de distintos Estados y la adecuación de sus derechos internos (que, en todo caso, debe darse) y que autorice a distintos actores a promover la protección de los afectados actuales y potenciales: por ejemplo, a través del avergonzamiento por parte de ONGs y de litigios basados en normas internacionales (o internas).

También se debe destacar que la facilidad de actuación que permite la tecnología puede poner en evidencia lagunas o incertidumbres normativas, y confirmar así la necesidad de clarificar qué se permite en ciertas situaciones y cuestiones, como por ejemplo en lo relativo a las acciones con *drones* u otras tecnologías (o sin ellas) permitidas contra

2014); David Francis, "Take That, Pyongyang: 'The Interview' to Get Limited Christmas Day Release", *Foreign Policy*, 23 de diciembre de 2014; David Francis, "'The Interview,' Once Pulled from Theaters, Can Now Be Watched from Your Couch", *Foreign Policy*, 24 de diciembre de 2014; Adam Taylor, "What if North Korea didn't hack Sony?", *The Washington Post*, 30 de diciembre de 2014; David Francis, "Obama Slams North Korea with Sanctions for Sony Hack", *Foreign Policy*, 2 de enero de 2015.

¹³¹ Vid. David E. Sanger, Nicole Perlroth y Eric Schmitt, "U.S. Asks China to Rein In Korean Hackers", *The New York Times*, 20 de diciembre de 2014.

actores no estatales que operan en el territorio de terceros Estados y realizan determinados ataques. Este caso refleja la importancia de ofrecer protección frente a lesiones a derechos y de que se indique qué es lícito y dentro de qué parámetros lo es, lo que además sirve para identificar posibles cambios requeridos *de lege ferenda* si se advierten deficiencias normativas o el derecho ha quedado rezagado frente a la práctica.

En algunas situaciones, los desarrollos jurídicos existentes demostrarán ser inadecuados y desactualizados o insuficientes e inacabados en algunos aspectos por sus vacíos, como por ejemplo en lo relativo al uso de armas nucleares (el que casi siempre sería contrario a principios de derechos humanos y DIH, algunos de los cuales tienen carácter imperativo). Frente a ellas y otras armas y tecnologías puede decirse, por ejemplo, que su proliferación entraña un riesgo: no sólo por el hecho de que puedan ser adquiridas por distintos actores con propósitos dañinos, sino además porque su presencia implica un riesgo de tentaciones o potenciales decisiones sobre su uso, con consecuencias nefastas.¹³² Todo esto hace que, según el caso, sea importante regular *de lege ferenda* aspectos no regulados o regulados de forma impropia; prohibir o limitar el uso de tecnologías antes toleradas; o tener en cuenta las particularidades de desarrollos tecnológicos para poder regular su uso y desarrollo de forma apropiada de conformidad con estándares humanizadores, por ejemplo permitiendo el uso civil de *drones* asegurándose de la seguridad aérea en lo relativo a vuelos con pasajeros para evitar colisiones, que evidentemente pueden afectar el goce de derechos humanos. Sin embargo, en tanto se adopten regulaciones necesarias, deben aplicarse principios y reglas existentes de forma evolutiva, aunque ello no elimina la necesidad de regulación más técnica o completa. En algunos casos, no obstante, acudir al derecho existente puede ser suficiente, como por ejemplo cuando el uso de la tecnología sólo suponga una dimensión o escenario adicional de ejercicio o riesgo en cuestiones que también se presentan sin aquel uso concreto.

¹³² Vid. Daniel Bodansky, “Non Liquef”, *Max Planck Encyclopedia of Public International Law*, Oxford University Press, 2006; Corte Internacional de Justicia, *Legalidad de la amenaza o el uso de armas nucleares*, Opinión Consultiva, 8 de julio de 1996, párrs. 78-100, 105; Opinión disidente del vicepresidente Schwebel a la anterior opinión consultiva.

En múltiples ocasiones, será una adecuada combinación de procesos de regulación, acción e identificación la conveniente para enfrentar problemas. Es importante que se vayan introduciendo mecanismos y preceptos que, de alguna forma, permitan adaptaciones de la regulación frente a desafíos y desarrollos que puedan surgir, como por ejemplo cláusulas sobre evolución y adaptación de la regulación a la luz de determinados criterios y parámetros,¹³³ en nuestro caso relativos al respeto y protección de la dignidad humana. La prevención de futuros abusos puede tener una vertiente tanto general, similar en cierta forma a criterios de precaución; y otra expresa y concreta, por ejemplo en tratados sobre desarme y armamento que prohíban determinados desarrollos hasta que se garanticen o establezcan pautas para evitar abusos contrarios al valor inherente del ser humano motivados por deseos de dar primacía a intereses como los militares,¹³⁴ que no sólo son invocados para defender sino también para doblegar, humillar, colonizar y abusar (siendo su invocación una triste faceta del DIH, que siempre los tiene en cuenta y pondera con criterios *verdaderamente* humanitarios).¹³⁵

Estas consideraciones suponen apenas un primer paso, y es indispensable realizar un análisis detallado y profundo de cada dilema, en tanto la humanización del uso de los avances tecnológicos no es siempre una tarea sencilla. Por ejemplo las prohibiciones totales preventivas pueden llevar a que se impidan usos que, o bien generen potencialmente, o bien eliminen o disminuyan potencialmente, el sufrimiento de muchos.¹³⁶ Por esta razón, juristas y diplomáticos deben ser humildes y consultar con

¹³³ Vid. Jean-Marie Henckaerts y Louise Doswald-Beck, op. cit., págs. XXIX-XXX; Corte Internacional de Justicia, *Caso Proyecto Gabčíkovo-Nagymaros (Hungría Vs. Eslovaquia)*, Sentencia de 25 de septiembre de 1997, párrs. 112, 140.

¹³⁴ Vid. IHRC y Human Rights Watch, op. cit., págs. 3-4, 25; “HRW: autonomous weapons should be banned by international convention”, *Jurist*, 13 de mayo de 2014 (disponible en: <http://jurist.org/paperchase/2014/05/hrw-autonomous-weapons-should-be-banned-by-international-convention.php>, última visita: 18 de marzo de 2015); Kenneth Anderson et al., op. cit., págs. 395-398 (donde se describen distintas propuestas de prohibición de armas con determinada autonomía, y se dice que las prohibiciones pueden dar ventajas a los Estados que no consientan o desaprovechar ciertas oportunidades, argumentos que tienen cierto tinte utilitarista o de competición entre Estados que por ello no asume una postura centrada en el individuo).

¹³⁵ Vid. artículo 51.5.b) del Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales de 1977; Frits Kalshoven y Liesbeth Zegveld, op. cit., págs. 46, 60, 103, 108-109, 182-183, 203-204; Theodor Meron, “The humanization of humanitarian law”, op. cit., pág. 239.

¹³⁶ Vid. IHRC y Human Rights Watch, op. cit., págs. 25-26; *versus* Kenneth Anderson et al., op. cit., pág. 398.

expertos en ciencia e ingeniería, aunque igualmente éstos deben respetar su ética profesional y las obligaciones internacionales e internas que existan, para que el derecho internacional sea eficaz y razonable: después de todo, su garantía radica en últimas en cómo se comportan los individuos y cómo se responde a conductas jurídicamente relevantes,¹³⁷ y el uso, desarrollo y adquisición de la tecnología por distintos actores pueden tener aquella relevancia.

En ocasiones, con su función expresiva, el derecho, el *soft law* y la práctica internacional de distintos actores pueden servir para inspirar y promover usos de la tecnología que sirvan para mejorar las condiciones de y la atención a los seres humanos, incluyendo a víctimas, por ejemplo promoviendo el uso de determinadas tecnologías en labores de rescate, asegurándose de que sean seguras y no generen riesgos para la prevalencia de principios y estándares humanitarios.

Los procesos de regulación e identificación de estándares no son los únicos pertinentes para buscar humanizar el uso de las tecnologías, pero son ciertamente importantes por su función de señalar conductas prohibidas o permitidas y porque contribuyen a que se puedan identificar normas que deban tenerse en cuenta en toda jurisdicción y que, eventualmente, en casos de seriedad potencial o identificada, obliguen directamente en términos jurídicos internacionales. En la práctica, tanto actores estatales como no estatales abusan de la tecnología perjudicando distintos bienes jurídicos, incluyendo los que protegen a seres humanos o al medio ambiente (como se ha visto en el caso de transacciones con créditos de carbón y *hacks* o manipulaciones a su sistema por grupos criminales o individuos que acaban perjudicando aquel sistema y afectando distintas normas e intereses internos e internacionales), entre otros, bien sea porque ellos se ven afectados directamente por sus desmanes o porque determinada conducta que se sirve de la tecnología afecta directa o indirectamente, por ejemplo, la economía o gobiernos

¹³⁷ Vid. Comisión de Derecho Internacional, *Principles of International Law recognized in the Charter of the Nürnberg Tribunal and in the Judgment of the Tribunal, with commentaries*, op. cit., párr. 99.

legítimos y acaba perjudicando a muchos individuos, como afirmó un grupo de expertos en la ONU.¹³⁸

Hacer frente a amenazas y desafíos sin afectar el goce y ejercicio de los derechos humanos ni restringir de forma ilícita los derechos de quienes empleen la tecnología es posible permitiendo el desarrollo tecnológico dentro de cauces infranqueables relativos al respeto de la dignidad humana, orientándose por criterios *pro personae* en la elección de normas, interpretaciones y conductas, y teniendo en cuenta la necesidad de efectuar juicios de ponderación, proporcionalidad y legitimidad de restricciones. Por ejemplo, en el caso sobre el “derecho al olvido”, el Tribunal de Justicia de la Unión Europea tuvo en cuenta consideraciones de esta índole frente a la tensión entre la libertad de información y la privacidad; y podría entenderse que por ello es relevante tener en ocasiones en cuenta un derecho de rectificación (reconocido expresamente en el sistema interamericano e implícito en los derechos a la reparación y de acceso a recursos efectivos en otros ámbitos), concebido de forma actualizada para que sea garantizado en un contexto digital.¹³⁹

¹³⁸ Vid. Asamblea General de las Naciones Unidas, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Developments in the field of information and telecommunications in the context of international security*, A/65/201, 30 de julio de 2010, párrs. 1 y 8, donde se dice que “Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. These threats may cause substantial damage to economies and national and international security. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole [...] Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. Such proxies, whether motivated by financial gain or other reasons, can offer an array of malicious services to State and non-State actors”; McKenzie Funk, “The Hack That Warmed the World”, *Foreign Policy*, 30 de enero de 2015.

¹³⁹ Vid. Tribunal de Justicia de la Unión Europea, (Gran Sala), *Procedimiento entre Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos, Mario Costeja González*, op. cit., párr. 99. Sobre el derecho de rectificación (que, al igual que otros derechos, debe protegerse en medios digitales o escenarios tecnológicos en los que sea relevante, se manifieste o esté expuesto a lesiones, como se menciona en este escrito), ver: artículo 14 de la Convención Americana sobre Derechos Humanos; Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-7/86, *Exigibilidad del derecho de rectificación o respuesta (arts. 14.1, 1.1 y 2 Convención Americana sobre Derechos Humanos)*, 29 de agosto de 1986; Daniel O’Donnell, *Derecho internacional de los derechos humanos: Normativa, jurisprudencia y doctrina de los sistemas universal e interamericano*, Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2004, págs. 521-523, 541-546.

Como se dijo atrás, muchas veces las decisiones o análisis no son nada fáciles, y es necesario combinar una aproximación general que vele por garantías que siempre deben respetarse con la consciencia de que hay elementos particulares, técnicos y sobre posibles errores de determinados avances y sistemas que deben ser tenidos en cuenta para que la regulación y acción internacionales seas adecuadas y no torpes, superficiales, insuficientes o simplemente fugaces. El derecho internacional de los derechos humanos y el respeto de la dignidad humana no deben ser serviles y apoyar cualquier uso o desarrollo tecnológico sólo por el hecho de serlo, y deberían ser considerados incluso como partes de la deontología de las disciplinas tecnológicas, para promover usos benéficos de sus aplicaciones y servir de base a la crítica de aquellos que sean contrarios a la dignidad humana y los derechos fundados en ella, por ejemplo las técnicas que impliquen la destrucción de un embrión, como se discutió judicialmente en la Unión Europea.¹⁴⁰

Después de todo, la humanización del derecho internacional, aún incompleta pero en marcha¹⁴¹ (por lo que debe siempre incrementarse), se basa en el reconocimiento del protagonismo del ser humano y la importancia de su protección, que debe ser tomada en cuenta para evitar que se haga de los individuos meros medios y del derecho un simple sirviente de cualquier innovación tecnológica incluso cuando afecte sus libertades y derechos fundamentales. Es mi creencia que tanto el derecho¹⁴² como la ciencia y la tecnología han de ser concebidos, en términos de *su regulación* (y frente al derecho, en

¹⁴⁰ Vid. Tribunal de Justicia de la Unión Europea, Comunicado de prensa nº 112/11, Sentencia en el asunto C-34/10 Oliver Brüstle/Greenpeace eV, *No es patentable un procedimiento que, al emplear la extracción de células madre obtenidas a partir de un embrión humano en el estadio de blastocisto, implica la destrucción del embrión*, 18 de noviembre de 2011, disponible en: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-10/cp110112es.pdf> (última revisión: 17 de marzo de 2015).

¹⁴¹ Vid. Theodor Meron, *The Humanization of International Law*, op. cit., págs. xv, 526; Voto concurrente del juez A.A. Cançado Trindade a la Opinión consultiva OC-17/2002, *Condición Jurídica y Derechos Humanos del Niño*, de la Corte Interamericana de Derechos Humanos, párrs. 48-50, 71; Voto concurrente del juez A.A. Cançado Trindade a la Opinión consultiva OC-18/03, *Condición Jurídica y Derechos de los Migrantes Indocumentados*, de la Corte Interamericana de Derechos Humanos, párrs. 25, 27, 88 y pie de página 106 en aquel voto.

¹⁴² Sobre la importancia de que todo derecho sirva y respete al ser humano, y de la centralidad que el individuo debe tener en él, ver: Voto concurrente del juez A.A. Cançado Trindade a la Opinión consultiva OC-17/2002, *Condición Jurídica y Derechos Humanos del Niño*, de la Corte Interamericana de Derechos Humanos, párr. 19; John Finnis, "The Priority of Persons", en John Finnis, *Intention and Identity: Collected Essays Volume II*, Oxford University Press, 2011.

cuanto a todo su uso), como instrumentos y creación que ojalá sirva pero, cuando menos, respete al ser humano, y no como fines en sí mismos de forma abstracta o irrestricta, a diferencia de lo que podría parecer a un positivista o “tecnologista” extremo que ignore o no preste atención a los daños que pueden causarse dadas las imperfecciones y limitaciones de muchos procesos y desarrollos normativos y tecnológicos. Claro está, muchos daños dependerán del usuario y el uso concreto y no de un elemento intrínseco a innovaciones tecnológicas. La ciencia no se debe frenar por argumentos banales o irracionales, pero errores del pasado frente a la ciencia no deben hacer pensar que todo lo que ella haga posible es necesariamente loable: nunca debe olvidarse el fundamento de la dignidad humana, que es límite y condición jurídica y ética.

Ver el rostro de quienes han sufrido y pueden sufrir ataques de *drones* (como, por ejemplo, se observa en una recomendable galería de *Foreign Policy*)¹⁴³ u otros abusos que se aprovechan de la tecnología es necesario para movernos y sentir empatía y solidaridad con ellos, las cuales son piezas fundamentales del dinamismo de los derechos humanos.¹⁴⁴

En últimas, la tecnología puede servir para potenciar dinámicas que permitan mejorar la protección de los derechos humanos o, por el contrario, desarrollarse y emplearse en formas que generen riesgos para su goce y ejercicio, por lo que dependerá de los desarrollos y empleos concretos su valoración a la luz del fin en estas líneas descrito. A esto aludió Amnistía Internacional en 2017 cuando, a propósito de la inteligencia artificial, describió los puntos principales de su programa de trabajo sobre tecnología y derechos humanos (denominación que refleja la consciencia sobre la importancia de la cuestión), diciendo que:

¹⁴³ Vid. *Foreign Policy*, “The Undisclosed: Haunting portraits of the victims of America’s drone war in Pakistan”. Fotografías de Massimo Berruti, disponibles en: http://www.foreignpolicy.com/articles/2014/09/23/the_undisclosed_drone_strike_victims_pakistan_wazir_istan (última visita: 13 de noviembre de 2014).

¹⁴⁴ Vid. Andrew Clapham, *Human Rights: a Very Short Introduction*, op. cit., págs. 11, 28, 30, 131; Andrew Clapham, *Human Rights Obligations of Non-State Actors*, op. cit., pág. 107.

“In terms of the beneficial uses of AI for human rights, we are piloting the use of machine learning in our human rights investigations [...] In terms of the existing and potential negative impacts of AI on human rights, we base our work on well-grounded research and investigations, combined with constructive engagement with companies and policy makers. Our areas of focus are accountability, transparency and access to remedies in the following contexts: The potential for discrimination within the use of machine learning, particularly as it relates to policing, the criminal justice system and access to essential economic and social services; The potential development of autonomous weapons systems; The impact of automation on society including the right to work and livelihood”¹⁴⁵ (subrayado en el texto original).

Bibliografía y fuentes de conocimiento

Alexandra Gatto, “Corporate Social Responsibility in the External Relations of the EU”, *Yearbook of European Union Law*, 24, Oxford University Press, 2005.

Amartya Sen, “Elements of a Theory of Human Rights”, *Philosophy & Public Affairs*, Vol. 32, 2004.

Ana Beduschi, “The Big Data of International Migration: Opportunities and Challenges for States Under International Human Rights Law”, *Georgetown Journal of International Law*, Vol. 49, 2018.

Andrew Clapham, *Human Rights Obligations of Non-State Actors*, Oxford University Press, 2006.

Andrew Clapham, *Human Rights: a Very Short Introduction*, Oxford University Press, 1997.

Anna Badia Martí, “Cooperación internacional en la lucha contra la delincuencia organizada transnacional”, en: Victoria Abellán Honrubia y Jordi Bonet Pérez, *La incidencia de la mundialización en la formación y aplicación del Derecho Internacional Público: los actores no estatales: ponencias y estudios*, Bosch editor, 2008.

Antonio Cassese, “Remarks on Scelle’s Theory of “Role Splitting” (*dédoublement fonctionnel*) in International Law”, *European Journal of International Law*, Vol. 1, 1990.

Antonio Remiro Brotóns et al., *Derecho Internacional*, Tirant Lo Blanch, 2007.

Antonio Remiro Brotóns et al., *Derecho Internacional: Curso general*, Tirant Lo Blanch, 2010.

Asamblea de la Organización de Aviación Civil Internacional, Resoluciones A37-22 y A37-23.

Asamblea General de las Naciones Unidas, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Developments in the*

¹⁴⁵ Sherif Elsayed-Ali, “Artificial intelligence and the future of human rights”, *Amnistía Internacional*, 19 de octubre de 2017, disponible en: <https://medium.com/amnesty-insights/artificial-intelligence-and-the-future-of-human-rights-b58996964df5> (última visita: 19 de octubre de 2017).

field of information and telecommunications in the context of international security, A/65/201, 30 de julio de 2010.

Benedict Kingsbury, “The Concept of ‘Law’ in Global Administrative Law”, *European Journal of International Law*, Vol. 20, 2009.

Carlos M. Ayala Corao, “La ejecución de las sentencias de la Corte Interamericana de Derechos Humanos”, Año 5, N° 1, 2007.

Comisión de Derecho Internacional, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001.

Comisión de Derecho Internacional, *Principles of International Law recognized in the Charter of the Nürnberg Tribunal and in the Judgment of the Tribunal, with commentaries*, Yearbook of the International Law Commission, 1950.

Comisión Interamericana de Derechos Humanos, *Caso 11.436 (Víctimas del barco remolcador “13 de marzo” vs. Cuba)*, Informe N° 47/96, 16 de octubre de 1996.

Comisión Interamericana de Derechos Humanos, *Caso 12.285 (Michael Domingues vs. Estados Unidos)*, Informe N° 62/02, 22 de octubre de 2002.

Comisión Interamericana de Derechos Humanos, *Informe sobre terrorismo y derechos humanos*, OEA/SER.L/V/II.116 Doc. 5 rev. 1 corr., 22 de octubre de 2002.

Comisión Interamericana de Derechos Humanos, *Libertad de expresión e internet*, OEA/SER.L/V/II.CIDH/RELE/INF.11/13, 31 de diciembre de 2013.

Comisión Internacional de Juristas, *Complicidad empresarial y responsabilidad legal: Volumen 1, Afrontar los hechos y establecer un camino legal*, Informe del Panel de Expertos Juristas sobre Complicidad Empresarial en Crímenes Internacionales, Ginebra, 2010.

Comité de Derechos Económicos, Sociales y Culturales, *La índole de las obligaciones de los Estados Partes (párrafo 1 del artículo 2 del Pacto)*, Observación general N° 3, 1990.

Comité de Derechos Humanos Económicos, Sociales y Culturales, Observación General N° 21, *Derechos de toda persona a participar en la vida cultural (artículo 15, párrafo 1 a), del Pacto Internacional de Derechos Económicos, Sociales y Culturales*, E/C.12/GC/21/Rev.1, 17 de mayo de 2010.

Comité de Derechos Humanos, Observación general N° 34, *Artículo 19: Libertad de opinión y libertad de expresión*, CCPR/C/GC/34, 12 de septiembre de 2011.

Comité de los Derechos del Niño, Observación general N° 13, *Derecho del niño a no ser objeto de ninguna forma de violencia*, CRC/C/GC/13, 18 de abril de 2011.

Consejo de Derechos Humanos de las Naciones Unidas, “Proteger, respetar y remediar: un marco para las actividades empresariales y los derechos humanos”, A/HRC/8/5, 7 de abril de 2008.

Consejo de Derechos Humanos de las Naciones Unidas, *El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, A/HRC/27/37, 30 de junio de 2014.

Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Philip Alston, *Study on targeted killings*, A/HRC/14/24/Add.6, 28 de mayo de 2010.

Constantine Antonopoulos, “Force by armed groups as armed attack and the broadening of self-defence”, *Netherlands International Law Review*, Vol. LV, 2008.

Convención de la Haya (II) de 1899.

Convención de Viena sobre el Derecho de los Tratados.

Convención sobre los Derechos de las Personas con Discapacidad.

Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional, hecho en Beijing el 10 de septiembre de 2010.

Convenio sobre Aviación Civil Internacional; la Declaración de los principios jurídicos que deben regir las actividades de los Estados en la exploración y utilización del espacio ultraterrestre.

Convenio sobre la responsabilidad internacional por daños causados por objetos espaciales.

Corte Constitucional de Colombia, Sentencia T-121/18, 9 de abril de 2018; John Herrman y Charlie Savage, “Trump’s Blocking of Twitter Users is Unconstitutional, Judge Says”, *The New York Times*, 23 de mayo de 2018.

Corte Interamericana de Derechos Humanos, *Caso “La Última Tentación de Cristo” (Olmedo Bustos y otros) vs. Chile*, Sentencia, 5 de febrero de 2001.

Corte Interamericana de Derechos Humanos, *Caso 19 Comerciantes Vs. Colombia*, Sentencia de 5 de julio de 2004.

Corte Interamericana de Derechos Humanos, *Caso Almonacid Arellano y otros Vs. Chile*, Sentencia de 26 de septiembre de 2006.

Corte Interamericana de Derechos Humanos, *Caso Castillo Petruzzi y otros vs. Perú*, Sentencia, 30 de mayo de 1999.

Corte Interamericana de Derechos Humanos, *Caso Castillo Petruzzi y otros vs. Perú*, Sentencia de Excepciones Preliminares, 4 de septiembre de 1998.

Corte Interamericana de Derechos Humanos, *Caso de la Masacre de Pueblo Bello Vs. Colombia*, Sentencia de 31 de enero de 2006.

Corte Interamericana de Derechos Humanos, *Caso de los “Niños de la calle” (Villagrán Morales y otros) Vs. Guatemala*, Sentencia, 19 de noviembre de 1999.

Corte Interamericana de Derechos Humanos, *Caso del Penal Miguel Castro Castro Vs. Perú*, Sentencia de interpretación de 2 de agosto de 2008.

Corte Interamericana de Derechos Humanos, *Caso González y otras (“campo algodonero”) Vs. México*, Sentencia de 16 de noviembre de 2009.

Corte Interamericana de Derechos Humanos, *Caso Suárez Rosero Vs. Ecuador*, Sentencia de 12 de noviembre de 1997.

Corte Interamericana de Derechos Humanos, Opinión consultiva OC-18/03, *Condición Jurídica y Derechos de los Migrantes Indocumentados*, 17 de septiembre de 2003.

Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-21/14, *Derechos y garantías de niñas y niños en el contexto de la migración y/o en necesidad de protección internacional*, 19 de agosto de 2014.

Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-7/86, *Exigibilidad del derecho de rectificación o respuesta (arts. 14.1, 1.1 y 2 Convención Americana sobre Derechos Humanos)*, 29 de agosto de 1986.

Corte Internacional de Justicia, *Accordance with International Law of the Unilateral Declaration of Independence in respect of Kosovo*, Opinión Consultiva, 22 de julio de 2010, Declaración del juez Simma.

Corte Internacional de Justicia, *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua Vs. Estados Unidos de América)*, Sentencia de fondo de 27 de junio de 1986.

Corte Internacional de Justicia, *Caso Ahmadou Sadio Diallo (República de Guinea Vs. República Democrática del Congo)*, Sentencia, 30 de noviembre de 2010.

Corte Internacional de Justicia, *Caso Proyecto Gabčíkovo-Nagymaros (Hungría Vs. Eslovaquia)*, Sentencia de 25 de septiembre de 1997.

Corte Internacional de Justicia, *Legalidad de la amenaza o el uso de armas nucleares*, Opinión Consultiva, 8 de julio de 1996.

Daniel Bodansky, “Non Liqueur”, *Max Planck Encyclopedia of Public International Law*, Oxford University Press, 2006.

Daniel O’Donnell, *Derecho internacional de los derechos humanos: Normativa, jurisprudencia y doctrina de los sistemas universal e interamericano*, Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2004.

David Capie, “Influencing Armed Groups: Are there Lessons to be Drawn from Socialization Literature?”, en: Geneva Call, *Exploring Criteria & Conditions for Engaging Armed Non-State Actors to Respect Humanitarian Law & Human Rights Law*, Conference Report, 2007.

Dawn Oliver and Jörg Fedtke, *Human Rights and the Private Sphere: A Comparative Study*, Routledge, 2007.

Dawn Oliver, “Human Rights and the Private Sphere”, *UCL Human Rights Law Review*, Vol. 1, 2008.

Declaración Universal de Derechos Humanos.

Declaración y Programa de Acción de Viena, Aprobados por la Conferencia Mundial de Derechos Humanos el 25 de junio de 1993.

Edmund F. Byrne, “Business Ethics Should Study Illicit Businesses: To Advance Respect for Human Rights”, *Journal of Business Ethics*, Vol. 103, 2011.

Elena Pariotti, “Non-State Actors, International Law, and Human Rights”, en Sanford R. Silverburg (ed.), *International Law: Contemporary Issues and Future Developments*, Westview Press, 2011.

Eric A. Posner, *The Perils of Global Legalism*, The University of Chicago Press, 2009.

Eric A. Posner, *The Twilight of Human Rights Law*, Oxford University Press, 2014.

Fred Halliday, “The Romance of Non-state Actors”, en Daphné Josselin y William Wallace (eds.), *Non-state Actors in World Politics*, Palgrave, 2001.

Frits Kalshoven y Liesbeth Zegveld, “Constraints on the Waging of War”, 3rd Edition, ICRC, 2001.

Hahrie Han, “Put the debate about slacktivism to rest”, *OUPblog*, 19 de noviembre de 2014.

Harold Koh, “Why Do Nations Obey International Law?”, *The Yale Law Journal*, Vol. 106, 1997.

- IHRC y Human Rights Watch, *Shaking the Foundations: The Human Rights Implications of Killer Robots*, 2014.
- Jan Klabbers, *International Law*, Cambridge University Press, 2013.
- Janne E. Nijman, “Non-state actors and the international rule of law: Revisiting the ‘realist theory’ of international legal personality”, *Amsterdam Center for International Law Research Paper Series*, 2010.
- Jean d’Aspremont, “Softness in International Law: A Self-Serving Quest for New Legal Materials”, *European Journal of International Law*, Vol. 19, 2008.
- Jean-Marie Henckaerts y Louise Doswald-Beck, *El derecho internacional humanitario consuetudinario, Volumen I: Normas*, Comité Internacional de la Cruz Roja, 2007.
- Jean-Paul Costa, “Statement Issued by the President of the European Court of Human Rights concerning REQUESTS FOR INTERIM MEASURES (Rule 39 of the Rules of Court)”, 2011.
- Jennifer Zerk, “Corporate liability for gross human rights abuses: Towards a fairer and more effective system of domestic law remedies”, *Report prepared for the Office of the UN High Commissioner for Human Rights*.
- Jessica Almqvist, “Facing the Victims in the Global Fight against Terrorism”, *Fride Working Papers*, N° 18, 2006-
- John Finnis, *Intention and Identity: Collected Essays Volume II*, Oxford University Press, 2011.
- John H. Knox, “Horizontal Human Rights Law”, *American Journal of International Law*, Vol. 102, 2008.
- John H. Knox, “The Human Rights Council Endorses “Guiding Principles” for Corporations”, *ASIL Insights*, Vol. 15, 2011.
- Jonas Christoffersen, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights*, Martinus Nijhoff Publishers, 2009.
- Jordan J. Paust, “The Reality of Private Rights, Duties, and Participation in the International Legal Process”, *Michigan Journal of International Law*, Vol. 25, 2004.
- José E. Alvarez, “Are Corporations “Subjects” of International Law?”, *Santa Clara Journal of International Law*, Vol. 9, 2011.
- Kenneth Anderson et al., “Adapting the Law of Armed Conflict to Autonomous Weapon Systems”, *International Law Studies*, Vol. 90, 2014.
- Mark Klamberg, “The Legality of Rebel Courts during Non-International Armed Conflicts”, *Journal of International Criminal Justice*, Vol. 16, 2018.
- Marko Milanovic, “Lessons for human rights and humanitarian law in the war on terror: comparing *Hamdan* and the Israeli *Targeted Killings* case”, *International Review of the Red Cross*, 2007.
- Michael N. Schmitt (editor), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.
- Monica Moyo, “British Investigatory Powers Tribunal Rules Prior Intelligence Sharing Arrangements Between U.S. and U.K. Illegal”, *International Law in Brief*, 2015.
- Mónica Pinto, “El principio *pro homine*. Criterios de hermenéutica y pautas para la regulación de los derechos humanos”, en Martín Abregú y Christian Courtis (eds.), *La aplicación de los tratados sobre derechos humanos por los tribunales locales*, 1997.

- Myres S. McDougal y Harold D. Lasswell, “The Identification and Appraisal of Diverse Systems of Public Order”, *The American Journal of International Law*, Vol. 53, 1959.
- Myres S. McDougal, “Some basic theoretical concepts about international law: a policy-oriented framework of inquiry”, *The Journal of Conflict Resolution*, Vol. IV, 1960.
- Naciones Unidas, Asamblea General, *El derecho a la privacidad en la era digital*, A/HRC/28/L.27, 24 de marzo de 2015.
- Naciones Unidas, *Principios Rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para “proteger, respetar y remediar”*, 2011.
- Naciones Unidas, United Nations Office at Geneva (UNOG), “Human Rights Council Holds Panel on Remotely Piloted Aircraft or Armed Drones in Counterterrorism and Military Operations”, 22 de septiembre de 2014.
- Nicolás Carrillo Santarelli, “Enhanced Multi-Level Protection of Human Dignity in a Globalized Context through Humanitarian Global Legal Goods”, *German Law Journal*, Vol. 13, 2012.
- Nicolás Carrillo Santarelli, “La influencia “artística” de las emociones y la empatía en el contenido, la interpretación y la efectividad del derecho internacional”, *Anuario Mexicano de Derecho Internacional*, Vol. XVII, 2017.
- Nicolás Carrillo Santarelli, “The Links between the Responsibility of International Organizations and the Quest towards a More Reasonable and Humane International Legal system”, *International Organizations Law Review*, Vol. 7, 2010.
- Nicolás Carrillo Santarelli, “The Protection of Global Legal Goods”, *Anuario Mexicano de Derecho Internacional*, Vol. XIII, 2013.
- Nils Melzer, *Participación directa en las hostilidades: según el derecho internacional humanitario*, Comité Internacional de la Cruz Roja, 2010.
- Non-State Actors Committee of the International Law Association, *Preliminary issues for the ILA Conference in Rio de Janeiro*, Report, 2008.
- Oliver Sensen, “Human Dignity in Historical Perspective: The Contemporary and Traditional Paradigms”, *European Journal of Political Theory*, Vol. 10, 2011.
- Olivier Bangerter, “The ICRC and Non-State Armed Groups”, en: Geneva Call, *Exploring Criteria & Conditions for Engaging Armed Non-State Actors to Respect Humanitarian Law & Human Rights Law*, Conference Report, 2007.
- Opinión separada de la juez Higgins a la Opinión consultiva de la Corte Internacional de Justicia de 9 de julio de 2004 sobre “*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*”.
- Opinión separada del juez Cançado Trindade a la sentencia de la Corte Internacional de Justicia de 20 de abril de 2010 en el caso *Pulp Mills on the River Uruguay (Argentina versus Uruguay)*.
- Opinión separada del juez Kooijmans a la Sentencia de la Corte Internacional de Justicia del 19 de diciembre de 2005 en el caso sobre *Armed Activities on the Territory of the Congo (República Democrática del Congo contra Uganda)*.

Opinión separada del juez Simma a la Sentencia de la Corte Internacional de Justicia del 19 de diciembre de 2005 en el caso sobre *Armed Activities on the Territory of the Congo (República Democrática del Congo contra Uganda)*.

Pacto Internacional de Derechos Económicos, Sociales y Culturales.

Principios y directrices básicos sobre el derecho de las víctimas de violaciones manifiestas de las normas internacionales de derechos humanos y de violaciones graves del derecho internacional humanitario a interponer recursos y obtener reparaciones.

Protocolo adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales (“Protocolo de San Salvador”).

Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales de 1977.

Protocolo III adicional a los Convenios de Ginebra de 1949 relativo a la aprobación de un signo distintivo adicional de 2005.

Resolución 1368 (2001) del Consejo de Seguridad de las Naciones Unidas.

Resolución 2178 (2014) del Consejo de Seguridad de las Naciones Unidas.

Resolución 2625 (XXV) de la Asamblea General de las Naciones Unidas.

Resolución 68/167 de la Asamblea General de las Naciones Unidas.

Rita Joseph, *Human Rights and the Unborn Child*, Martinus Nijhoff Publishers, 2009.

Robert Dufresne, Review of: Liesbeth Zegveld, *The Accountability of Armed Opposition Groups in International Law*, *European Journal of International Law*, Vol. 15, 2004.

Roland Portmann, *Legal Personality in International Law*, Cambridge University Press, 2010.

Ryan Goodman y Derek Jinks, “Incomplete Internalization and Compliance with Human Rights Law”, *European Journal of International Law*, Vol. 19, 2008.

Santiago Villalpando, “The Legal Dimension of the International Community: How Community Interests Are Protected in International Law”, *European Journal of International Law*, Vol. 21, 2010.

Stefan Kirchner, “Relative Normativity and the Constitutional Dimension of International Law: A Place for Values in the International Legal System?”, *German Law Journal*, Vol. 5, 2004.

Stephan Hobe, “Individuals and Groups as Global Actors: The Denationalization of International Transactions”, in Rainer Hofmann (ed.), *Non-State Actors as New Subjects of International Law*, Duncker & Humblot (ed.), 1999.

Steven R. Ratner, “Law Promotion Beyond Law Talk: The Red Cross, Persuasion, and the Laws of War”, *European Journal of International Law*, Vol. 22, 2011.

Tatiana Waisberg, “Colombia's Use of Force in Ecuador Against a Terrorist Organization: International Law and the Use of Force Against Non-State Actors”, *ASIL Insights*, Vol. 12, 2008.

The Bangalore Principles: Report of Judicial Colloquium on the Domestic Application of International Human Rights Norms, Bangalore, India.

Theo van Boven, “The United Nations Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law”, *United Nations Audiovisual Library of International Law*, 2010.

Theodor Meron, *The Humanization of International Law*, Martinus Nijhoff, 2006, pág. 40; Theodor Meron, “The humanization of humanitarian law”, *American Journal of International Law*, Vol. 94, 2000. Thomas Buergenthal, “The Evolving International Human Rights System”, *American Journal of International Law*, Vol. 100, 2006.

Tribunal de Justicia de la Unión Europea (Gran Sala), *Procedimiento entre Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos*, Mario Costeja González, Sentencia sobre petición de decisión prejudicial, 13 de mayo de 2014.

Tribunal de Justicia de la Unión Europea, Comunicado de prensa n° 112/11, Sentencia en el asunto C-34/10 Oliver Brüstle/Greenpeace eV, *No es patentable un procedimiento que, al emplear la extracción de células madre obtenidas a partir de un embrión humano en el estadio de blastocisto, implica la destrucción del embrión*, 18 de noviembre de 2011.

Tribunal Europeo de Derechos Humanos (Gran Sala), *Caso Kononov Vs. Letonia*, Sentencia de 17 de mayo de 2010.

Tribunal Europeo de Derechos Humanos (Sección cuarta), *Caso de Hajduová contra Eslovaquia*, Sentencia, 30 de noviembre de 2010.

Tribunal Europeo de Derechos Humanos (Sección Cuarta), *Caso Hajduová Vs. Eslovaquia*, Sentencia de 30 de noviembre de 2010.

Tribunal Europeo de Derechos Humanos, *Caso Al-Adsani Vs. el Reino Unido*, Sentencia, 21 de noviembre de 2001.

Tribunal Internacional para juzgar a los presuntos responsables de graves violaciones del derecho internacional humanitario cometidas en el territorio de la ex-Yugoslavia a partir de 1991, *Prosecutor v. Anto Furundzija*, Sentencia, 10 de diciembre de 1998.

Xiaobing Xu, “On Conflict of Human Rights”, *Pierce Law Review*, Vol. 5, 2006.

Yasmin Naqvi, “El derecho a la verdad en el derecho internacional: ¿realidad o ficción?”, *International Review of the Red Cross*, N° 862, 2006.