Impactos de las nuevas tecnologías en los derechos humanos

Documento de trabajo no. 1

Este primer documento de trabajo del Institut de Drets Humans de Catalunya (IDHC) tiene como objetivo establecer de una manera clara y ordenada cuáles son los impactos que tienen las llamadas nuevas tecnologías en cada uno de los derechos humanos reconocidos en la Declaración Universal de los Derechos Humanos (DUDH).

Se trata de un ejercicio que busca alejarse de los lugares comunes a los que se acude cuando se habla de tecnologías y derechos humanos que, por una parte, suelen centrarse únicamente en el análisis o consideración de las tecnologías digitales y, por otra parte, aunque hacen referencia de manera genérica a los derechos humanos, en realidad solo se centran en algunos de ellos. Por tanto, es un documento que busca servir para futuros análisis a partir de un estudio introductorio que establece las bases generales y un análisis detallado, pero abierto a evolución, de veintisiete derechos humanos y de algunas tecnologías que impactan en ellos.

Autor/as: Anna Pont, María Agostina Passera y Karlos Castilla

Fecha: Enero 2022

Edición:
Institut de Drets Humans de Catalunya
Av. Meridiana 32, entr. 2a. Esc B
08018 Barcelona
www.idhc.org

Diseño y maquetación: nadiasanmartin.com

Institut de Drets Humans de Catalunya

OPEN SOCIETY FOUNDATIONS

Índice

Índice

cap. 1

Análisis introductorio[1]

1 Este apartado ha sido desarrollado por Karlos Castilla.

Este primer *documento de trabajo* del Institut de Drets Humans de Catalunya (IDHC) es el resultado de un proceso de investigación de varios meses, que ha tenido como objetivo establecer de una manera clara y ordenada, cuáles son los impactos que tienen las llamadas nuevas tecnologías en cada uno de los derechos humanos reconocidos en la Declaración Universal de los Derechos Humanos (DUDH).

Esto es, se trata de un ejercicio que busca alejarse de los lugares comunes a los que se acude cuando se habla de *tecnologías y derechos humanos* que, por una parte, suelen centrarse únicamente en el análisis o consideración de las tecnologías digitales y, por otra parte, aunque hacen referencia de manera genérica a los derechos humanos, en realidad solo se centran en el análisis de algunos de ellos (casi de manera general a: derecho a la privacidad, libertad de expresión, derecho a la protección de datos personales y no discriminación).

Somos conscientes de lo difícil que es abarcar e incluir todas las tecnologías existentes en la actualidad, pues ni siquiera porque nos encontramos en Europa y podría suponerse por diversas razones que estaríamos en posibilidad de conocer todas las tecnologías disponibles, lo hemos conseguido. No solo por lo inaccesible de algunas de ellas en la vida cotidiana, sino también por la velocidad con la que avanzan y son creadas.

También somos conscientes de que centrarse solo en los derechos antes mencionados tiene una estrecha relación con la forma en la que se ejercen los derechos humanos por medio o con el uso de tecnologías, por la cercanía que hoy en día tienen las conocidas como tecnologías digitales o tecnologías de la información y comunicación (TIC) con esos derechos en muchas de nuestras actividades diarias, en casi cualquier parte del mundo.

Pero aun con esa conciencia, queremos hacer un esfuerzo por mostrar la forma en la que diferentes tecnologías que se han podido conocer, directa e indirectamente, impactan en todo el listado de derechos y libertades contenido en el documento de derechos humanos traducido a más idiomas en el mundo.

A fin de dar orden a este estudio introductorio y establecer las bases de análisis que permitirán comprender de mejor forma el análisis concreto de derechos que se hace en este documento de trabajo, partiremos de algunas preguntas a las cuales consideramos que es esencial responder para la mejor comprensión de la relación tecnologías-derechos humanos.

¿De qué derechos humanos hablamos?

Para entrar en materia, lo primero que debe quedar establecido es que cuando en este documento de trabajo nos referimos a *derechos humanos*, son únicamente los veintisiete derechos y libertades contenidos en la Declaración Universal de los Derechos Humanos (DUDH)[2], que son los siguientes:

Artículo 1: todos/as nacemos libres e iguales
Artículo 2: derecho a ser libre de discriminación
Artículo 3: derecho a la vida, la libertad y la seguridad
Artículo 4: derecho a ser libre de la esclavitud
Artículo 5: derecho a ser libre de la tortura
Artículo 6: derecho a ser reconocida como persona ante la ley
Artículo 7: derecho a la igualdad ante la ley
Artículo 8: derecho de acceso a la justicia y la reparación
Artículo 9: derecho a ser libre de detención arbitraria
Artículo 10: derecho a un juicio justo
Artículo 11: derecho a la presunción de inocencia
Artículo 12: derecho a la privacidad y a la vida privada
Artículo 13: derecho a la libertad de movimiento, residencia y circulación
Artículo 14: derecho a buscar asilo
Artículo 15: derecho a la nacionalidad
Artículo 16: derecho al matrimonio y a fundar una familia
Artículo 17: derecho a la propiedad (individual y colectiva)
Artículo 18: libertad de pensamiento, de conciencia y de religión
Artículo 19: libertad de opinión y expresión
Artículo 20: libertad de reunión y asociación pacífica
Artículo 21: derecho a la participación política y elección de gobierno
Artículo 22: derecho a la seguridad social
Artículo 23: derecho al trabajo
Artículo 24: derecho al descanso y al tiempo libre
Artículo 25: derecho a un nivel de vida adecuado
Artículo 26: derecho a la educación
Artículo 27: derecho a la vida cultural, artística y científica
Artículo 28: derecho a un mundo libre y justo

2 La Declaración Universal de Derechos Humanos está integrada por 30 artículos, pero sus tres últimos artículos, más que derechos específicos, establecen principios generales que deben permear a todos los derechos y libertades como: la necesidad de la existencia de un Estado de Derecho para la efectividad de dichos derechos (art. 28); los deberes que tenemos frente a la comunidad y límites que se pueden establecer a los derechos para asegurar su reconocimiento y respeto (art. 29) y la forma en la que deben ser interpretados para evitar su supresión (art. 30).

Nos limitamos al contenido de la DUDH por ser considerada generalmente el fundamento de las normas internacionales sobre derechos humanos. Esto es, por ser y servir de inspiración de un valioso conjunto de tratados internacionales de derechos humanos a nivel regional y universal, así como por ser un referente de dichos derechos en muchas constituciones nacionales en el mundo.

La DUDH supone el primer reconocimiento pretendidamente universal de que los derechos básicos y las libertades fundamentales son inherentes a todos los seres humanos, inalienables y aplicables en igual medida a todas las personas; y que todas y cada una de nosotras hemos nacido libres y con igualdad de dignidad y de derechos. Independientemente de nuestra nacionalidad, lugar de residencia, género, origen nacional o étnico, color de piel, religión, idioma o cualquier otra condición.

¿Qué es tecnología?

Definir *tecnología* no es una labor sencilla. Los elementos de definición que suelen incluir algunas propuestas existentes incluyen:

a) Ciencia, procesos, conocimientos, teorías, técnicas (habilidades), instrumentos, métodos, sistemas, dispositivos.
que

b) Aplicados, utilizados, desarrollados, creados.
de forma

c) Lógica, ordenada, coordinada.

d) Permiten, facilitan, son usados.
para

e) Resolver problemas, crear soluciones, inventar herramientas útiles, aprovechar el conocimiento científico; facilitar la vida humana, modificar el entorno humano, resolver los problemas y las necesidades del ser humano.

A partir de todas esas ideas es posible integrar más de diez definiciones que, aunque similares, podrían hacernos pensar en algunas cosas y no en otras según las experiencias vitales de cada persona. Posiblemente algunas de esas definiciones nos podrían parecer insuficientes, otras poco claras y unas agradarnos más por ser compatibles con lo que hoy entendemos en nuestro ámbito personal como tecnología.

Ante eso, parecería que lo más sencillo es establecer qué no es tecnología, para que así, asumiendo las dos principales miradas de observación, podamos tener un poco de claridad de lo que es o se puede entender por tecnología.

De esa manera, lo obvio parece ser que no es tecnología todo aquello que, sin modificación humana intencionada, se encuentra en nuestro entorno. Entendimiento demasiado amplio, pero que da muestra que de una u otra forma, casi todo lo que nos rodea puede ser considerado tecnología.

Así, por ejemplo, un vaso de cristal para introducir líquidos y poder beberlos, hoy seguramente no nos parece que sea una tecnología, pero aplicando los elementos de definición antes señalados, algún día lo fue. Hoy ese vaso nos parecerá tecnología si es capaz de mantener el líquido en una determinada temperatura, si nos avisa cuando esté por terminarse el líquido en él depositado o si al mismo tiempo sirve para escuchar música por un dispositivo que tenga integrado. Pero todo esto último son avances o modificaciones tecnológicas de esa base que en algún momento se consideró novedosa. Y así podríamos hablar de muchos más objetos con los que tenemos contacto desde hace mucho tiempo y tal vez nos cueste catalogar como tecnología. Piense quien lee estas líneas, por ejemplo, en una "máquina simple" como lo es una bicicleta y sus múltiples avances hasta hoy.

Pero en todo caso, lo que aquí nos interesa destacar por ahora es que la tecnología ha estado presente en nuestras vidas desde que surgió y se formalizó la idea de los derechos humanos que aquí analizamos (1948), pero también antes de ese momento. Por poner un ejemplo claro, con la llamada primera Revolución Industrial (1760-1840). Es decir, que la relación *tecnología-derechos humanos* debía haber llamado nuestra atención desde el origen de estos, y de hecho, si se analizan los trabajos preparatorios de la DUDH y su preámbulo, parece que efectivamente se tiene presente cuando se dice expresamente en el texto final que "los pueblos de las Naciones Unidas se han declarado resueltos a promover el progreso social y a elevar el nivel de vida dentro de un concepto más amplio de la libertad". Como también, cuando en el artículo 27 de la DUDH se reconoce el derecho a "participar en el progreso científico y en los beneficios que de él resulten". Sobre esto, volveremos más adelante.

Para intentar concretar con ejemplos más claros lo que hoy, en el año 2022 occidental, consideramos casi sin cuestionamientos como tecnología, se podrían señalar: máquinas complejas, máquinas simples y/o herramientas que son principalmente de naturaleza física, como vehículos, naves espaciales, utensilios, equipamientos, robótica, infraestructura energética, computadoras, aparatos electrónicos, sensores, armas, instrumentos científicos y tecnología arquitectónica, ambiental, etc.

Pero también sin naturaleza física como muchas de las TIC, relacionadas con el conocimiento, la automatización, el procesamiento de transacciones, la *gamificación*, el *geofencing*, el internet de las cosas, el análisis predictivo, la inteligencia artificial, los algoritmos, el *big data*, el *blockchain*, los metadatos y otros tantos usos no físicos de la información.

De cada una de las ideas antes referidas, que no son todos los ejemplos existentes, se pueden derivar aplicaciones o derivaciones mucho más concretas de cada una en muy diversos ámbitos, de manera que, tener una lista cerrada de lo que es tecnología, es casi imposible pues siempre habrá algo que agregar a ese listado.

Por lo que, lo único que podemos hacer en este momento para intentar ejemplificar toda la tecnología que nos rodea es pedir a quien lee estas líneas que haga un alto en este momento de lectura y observe a su alrededor, pues aun cuando se encuentre en un lugar aislado rodeado de naturaleza, alguna tecnología encontrará, y si se encuentra en una ciudad, sin duda observará unos cuantos ejemplos y seguramente le rodean otros más de los que no había tomado conciencia de su presencia.

¿Qué preocupa de la relación tecnologías-derechos humanos?

Parece obvio que lo que nos puede preocupar de los efectos o impactos de las tecnologías en los derechos humanos son todos aquellos usos, aplicaciones, creaciones o efectos/resultados que impiden, afectan, violan, reducen, limitan o excluyen el efectivo ejercicio, goce, respeto, garantía y disfrute de dichos derechos y libertades.

Pues toda tecnología que, por el contrario, promueva, facilite, agilice o sirva para acceder, respetar, proteger o garantizar los derechos humanos será siempre bienvenida a fin de cumplir con ese entendimiento amplio del progreso social y la mejora del nivel de vida de todas las personas del que se habla en el preámbulo de la DUDH.

De esa manera, lo preocupante serían las "malas tecnologías" o, mejor dicho, el "mal uso" de las tecnologías en el ejercicio, goce y disfrute de los derechos humanos. En principio, se podría decir que por sí sola ninguna tecnología es mala, sino que será el para qué, cómo y quién la use, lo que puede generar los efectos negativos.

Así, siguiendo con el ejemplo del vaso que poníamos antes, por sí mismo no podemos considerar que tiene o puede tener un efecto negativo en los derechos humanos, sino por el contrario, podríamos decir más bien, con creatividad, que puede servir para el ejercicio del derecho a la propiedad, a la salud o a un nivel de vida adecuado. Ya sea el vaso simple original, o ese otro con capacidad de conservar una determinada temperatura o reproducir música. De hecho, según sus características, también podría considerarse como un elemento del ejercicio del derecho a la cultura, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten.

Su impacto negativo podría empezar a verse si se analizan los materiales con los que está hecho, pues estos más bien podrían afectar ese mismo derecho a la salud o el derecho al medio ambiente (sin olvidar, en este ámbito, la contaminación ambiental que se genera por el uso de las TIC). Y peor aún sería, si ese vaso es utilizado como un objeto para infligir torturas o afectaciones a la integridad personal.

Pero no en todos los casos de efectos negativos pueden estar relacionados con sus usos, sino también, con los procesos previos a la posibilidad de disponer de dicho vaso. Por una parte, cuando los procesos, conocimientos, teorías o técnicas se piensan para excluir o afectar, o no se piensa en la diversidad de las sociedades en las que se desarrolla o a las que se dirige. Por ejemplo, si justamente se diseñan vasos de un material que afecte la salud o vasos que solo pueden ser sostenidos por manos grandes, impidiendo o dificultando que hagan uso de ellos personas con manos pequeñas o aquellas personas que no tienen una o ambas manos.

En este supuesto de un vaso, puede parecer absurdo el ejemplo anterior porque hoy en día hay vasos de todo tipo y características, pero lo hacemos de esta manera para que se piense en otras tantas tecnologías que, por las personas o el lugar desde el que se diseñan, podrían intencionadamente o no, afectar de una u otra forma derechos y libertades.

Por otra parte, puede haber impacto negativo, cuando los procesos de producción de ese vaso, es decir, en las fases de obtención, desarrollo y puesta a disposición de dicho vaso se violan derechos humanos como podría ser el derecho al trabajo, el derecho al descanso, la prohibición de esclavitud o el derecho al medio ambiente.

Se podría afirmar que esto último no tiene nada que ver con el vaso, viéndolo en abstracto y sin conocer su proceso de creación y producción, pero si queremos hablar de los impactos de las tecnologías en los derechos humanos, no basta su análisis a partir de su resultado final, sino que hace falta observar todo lo que implica contar con esa tecnología. De otra forma, quedaríamos siempre con miradas parciales.

Bajo esta perspectiva, lo que en principio nos puede preocupar de toda tecnología respecto a los derechos humanos son:

a) Procesos de creación y diseño de tecnologías que:

— Excluyan
— Restrinjan
— Discriminen
— Anulen
— Menoscaben
— Impidan
— Reduzcan

el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos humanos y libertades fundamentales.

b) Usos, aplicaciones, creaciones, efectos o resultados de las tecnologías que:

— Excluyan
— Restrinjan
— Discriminen
— Anulen
— Menoscaben
— Impidan
— Reduzcan

el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos humanos y libertades fundamentales.

Este ejercicio de evaluación y análisis, aunque puede ser complejo, es relativamente sencillo de observar en todas las tecnologías con naturaleza física. Pues así como hacíamos con el vaso, se puede hacer un ejercicio similar con infinidad de objetos que entran en la definición de tecnología: máquinas, armas, vehículos, utensilios, sensores, computadores, etc.

Si de todas esas tecnologías vemos su aplicación en ámbitos como la educación, la salud, el trabajo de los tribunales, los medios de información, la participación política, el desarrollo de diversas actividades laborales, la arquitectura, la alimentación, el entretenimiento, el transporte público, el uso de los espacios públicos, las actividades policiales o cualquier otra, podemos identificar un derecho humano y analizar si algo de lo anterior se presenta.

Sin embargo, los problemas se hacen más complejos con todas aquellas tecnologías no físicas relacionadas con el conocimiento, la automatización, el procesamiento de transacciones, el internet de las cosas, el análisis predictivo, la inteligencia artificial, los algoritmos, el *big data*, los metadatos y otros usos no físicos de la información, ya que, por una parte, es más complejo poder observarlas o seguirlas y, por otra parte, para poder cumplir con sus fines requieren de un conocimiento o información más a detalle de la persona que hace uso de ellas consciente o inconscientemente.

En esto último pondremos especial atención en el siguiente punto. Por lo que concluimos recordando que, no hay tecnologías buenas y malas para los derechos humanos, sino más bien procesos de creación, diseño, uso y aplicación que, intencionadamente o no, pueden tener efectos negativos en el ejercicio y goce de los derechos humanos. Como también muchos efectos positivos se les puede dar para hacer de estos una realidad para toda persona.

¿Por qué la relación de los derechos humanos con las TIC preocupa más en la actualidad?

Una respuesta que se niega muchas veces pero que es real, e incluye lo que a continuación estableceremos es que existen muchos libros, relatos y películas de ciencia ficción en las que las máquinas, computadoras, teléfonos, robots y otras tecnologías toman el dominio de la vida humana, controlándonos, sometiéndonos y volviéndonos prácticamente sus esclavas. Esto es, el miedo o desconocimiento de los alcances reales de la tecnología, aunque al mismo tiempo, muchas personas busquen tener la última tecnología a su disposición.

Una respuesta más racional que se puede dar, si olvidamos las realidades de todas las regiones del mundo y pensamos solo en algunas, es que, como tenemos acceso amplio y cercano a dichas tecnologías por medio de teléfonos, tabletas y computadores en general, percibimos más directamente sus efectos. Esto es, aunque desde prácticamente toda nuestra vida hemos tenido contacto con cosas u objetos que pueden ser considerados como tecnología, ahora, esos aparatos, máquinas y objetos tecnológicos (especialmente TIC) están más cerca de nuestros ámbitos personales e incluso íntimos. Lo que no ocurre, ni ocurría con muchas otras tecnologías antes.

Vinculado con lo anterior, otra respuesta posible es que, para poder ejercer varios derechos necesitamos de dichas TIC. Es decir, que solo si tenemos acceso a estas y/o les proporcionamos nuestra información personal, así sea la más general y básica como podría ser nuestro nombre, identidad de género

o edad, podemos ejercer algunos derechos. Sin hacer eso, en algunos casos parece ya imposible, por ejemplo, piénsese en cualquier aplicación para acceder a servicios públicos o privados en la que nos hayamos registrado en los últimos meses o la información que se nos ha pedido para abrir una cuenta en cualquier red social.

Una respuesta más es que, teniendo acceso a dichas tecnologías, se percibe que estas se producen y renuevan todos los días, que sus avances y desarrollos son muy acelerados y no paran, por lo que quienes nos encontramos ajenas a su diseño y creación, parece que nos estamos quedando relegadas, que las leyes vigentes son insuficientes para regularlas y que ante su complejidad y amplitud, ya es prácticamente imposible controlarlas, por lo que nos acercamos a lo que describíamos en esa primera respuesta.

A partir de esos aspectos y otros análisis desarrollados, se puede establecer que las razones que pueden justificar un mayor interés en estas tecnologías, frente a otras, radica en cinco elementos:

a)	Se están convirtiendo en (o se les está asignando la condición de) imprescindibles para el ejercicio de derechos y libertades.
b)	Para ejercer los derechos y libertades debemos dejar registro explícito de que lo hacemos.
c)	Para ejercer los derechos y libertades debemos proporcionar información que un ejercicio ordinario (*offline*) no requiere.
d)	Es muy difícil conocer con detalle cómo se diseñan, crean y gestionan la información y datos que recogen.
e)	Se da una potenciación del analfabetismo legal con el analfabetismo digital para el ejercicio de derechos y libertades.

Para explicar esto, pondremos el ejemplo del ejercicio de la libertad de expresión y las redes sociales. Antes de la existencia de dichas tecnologías digitales teníamos, entre otras, las siguientes maneras de ejercer esa libertad: una, expresando nuestras ideas en un espacio público o privado que podía ser una plaza pública, un medio de comunicación o frente a un grupo de amigos o personas conocidas o desconocidas.

Si lo hacemos en una plaza pública o con un grupo de personas, por regla general, simplemente tenemos que expresarnos. Solo nos reconocerá o sabrá quién somos quien tenga un conocimiento previo de nosotras o quien a partir de esas expresiones se interese. Pero en todo caso, será información básica o incluso superficial. La repercusión de esas expresiones llegará hasta donde quien nos escuche nos preste atención, nos replique o transmita a otras personas lo que de nosotras haya escuchado.

Si lo hacemos en un medio de comunicación, la primera diferencia frente a la anterior es que muy probablemente deberemos pedir que se nos dé acceso a esos medios o bien se nos invite expresamente (salvo si somos el objeto de la información). La segunda diferencia, es que muy probablemente quedará un registro de lo que expresemos, así como algunos aspectos vinculados con nuestros datos personales si el medio de comunicación mantiene un registro al menos básico de quienes participan en él. Y la

tercera, que los alcances de nuestras expresiones serán los alcances y público al que se dirige, sigue o tenga acceso al referido medio de comunicación.

En las redes sociales, la primera gran diferencia es que, si queremos hacer uso de ellas, debemos registrarnos, como paso previo. Aun sea con información falsa, pero debemos hacerlo, o no podremos ejercer nuestra libertad de expresión en ellas. La segunda gran diferencia es que se nos hace aceptar una serie de cláusulas de uso de dichas redes. Conjunto de cláusulas que muy pocas veces hemos leído por completo o al menos en su contenido esencial. Con lo que, sin saberlo, ya se puede estar condicionando el ejercicio de nuestra libertad de expresión. La tercera gran diferencia radica en que el alcance de nuestras expresiones es poco previsible: tan posible es que quienes sigan nuestra cuenta no se enteren de lo que hemos expresado en un momento determinado, como que personas totalmente ajenas a nuestros ámbitos cotidianos se puedan enterar de nuestras expresiones.

Si comparamos las expresiones en un medio de comunicación y en redes sociales, en principio estas últimas parecen más democráticas pues, como en una plaza pública, permiten que cualquiera lo pueda hacer. Si vemos lo que se necesita para hacer uso de esas redes, parece que ya no son tan democráticas sino exclusivas de personas que tienen un acceso previo a computadoras, tabletas o teléfonos conectados a servicios de Internet.

Las redes sociales, frente a las otras dos posibilidades, también parece que ofrecen un anonimato que facilita expresar cuestiones que dando la cara podrían no expresarse. Con lo positivo y negativo que ese hecho puede tener, además de que el anonimato es relativo y de inicio, pues en muchos casos existen formas de identificar el lugar o dispositivo desde donde han sido emitidas.

De esta manera, las tres opciones posibles del ejercicio de la libertad de expresión ofrecen ventajas y desventajas. La gran diferencia que hay en todas y que determina esos aspectos positivos o negativos es el medio, vía o plataforma por la cual se ejerce la libertad. Pues de eso depende la mayor o menor información y datos que se obtienen de nosotras para el ejercicio del derecho, lo demás es variable y depende de los factores ahora mencionados y de algunos más.

Así, por las ventajas que ofrecen las redes sociales frente a las otras formas de ejercer la libertad de expresión, en muchos casos parece que son imprescindibles para el ejercicio de dicha libertad, que sin ellas, no se puede ejercer en plenitud, ni tener alcances importantes. Especialmente cuando se observa que figuras públicas de todos los niveles las utilizan más que los medios tradicionales o cuando éstos mismos medios acuden a ellas para obtener la información que transmitirán a sus audiencias.

Al priorizarse los supuestos alcances, a veces se pierde de vista que para ejercer la libertad, necesariamente debemos registrarnos, con lo que siempre hay posibilidad de dejar constancia del ejercicio de la libertad, incluso creyéndonos anónimas. Lo que no ocurre necesariamente en una plaza pública o frente a un grupo de personas.

También nos vemos obligadas a dar información o datos que en otros medios para el ejercicio de esa libertad no son necesarios. Datos respecto a los cuales puede ser que nunca hayamos tomado conciencia, por más anónimas que nos creamos, al existir la posibilidad de conocerse el dispositivo que utilizamos, el servidor que utilizamos, el lugar en el que nos encontramos, los horarios en los que la utilizamos, nuestros intereses o preferencias políticas, ideológicas o deportivas, entre otras tantas más.

Nuevamente el ejemplo opuesto más claro es la plaza pública o un grupo de personas con las que nos reunimos, en donde toda esa información y datos personales no son necesarios, y seguramente no interesen, para ese o posteriores ejercicios de la libertad de expresión.

Por el contrario, muy probablemente no sabemos ni siquiera quién está detrás de esa red social. Mucho menos, si efectivamente hay posibilidad real de anonimato, ni de cuáles son los datos que obtienen a partir de que ingresamos a ellas, ya que esos datos son justamente lo que nutre y permite el desarrollo de dichas redes. De igual manera que no sabemos con precisión las razones por las cuales nuestra mejor reflexión intelectual que expresamos solo obtiene dos reacciones, mientras que una expresión sin mucho sentido tiene gran repercusión o audiencia. Como tampoco tenemos certeza plena de los datos que se recogen cada vez que expresamos algo, cada vez que ingresamos a la red social, cada vez que interactuamos con alguien, cada vez que creemos ejercer la libertad de expresión en plenitud.

Todo lo cual es, en una parte importante, resultado de nuestro analfabetismo digital. Que no se refiere a que no sepamos leer, ni escribir, sino más bien a nuestra ignorancia respecto a cómo se crean, diseñan y funcionan las tecnologías de la información. Analfabetismo digital que se suma al ya previamente existente analfabetismo jurídico, que implica que grandes capas de la sociedad no conocen sus derechos básicos y mucho menos las normas existentes que, en el ejemplo que tenemos, regulan el ejercicio de la libertad de expresión. Con lo que se cree que no hay regulación aplicable a dichas redes sociales, que nos encontramos en total desprotección, cuando lo único que en esencia está cambiando es la vía, medio o plataforma en que se ejerce la libertad y, por tanto, muchas de las regulaciones existentes deberían interpretarse y aplicarse evolutivamente. Dándose una potenciación entre los dos tipos de analfabetismo al aceptar sin leer las cláusulas de uso de dichas redes sociales, las solicitudes para acceder a nuestra información y otras “normativas” que se nos imponen para el ejercicio de derechos y libertades en esas plataformas digitales.

Pero también, por el analfabetismo digital de autoridades y tribunales, ya que les genera temor o incertidumbre aplicar y utilizar la normativa vigente a esas tecnologías de la información por la ignorancia que se tiene respecto a lo que son, por las falsas creencias de lo que implican o la justificación de que requieren una regulación específica y especializada, cuando insistimos, el principal cambio es la vía, medio o plataforma en que se ejercen los derechos y libertades.

Que sí, regulaciones específicas ayudarían, pero también mucho de lo existente en leyes de protección de datos y acceso a la información, propiedad intelectual, códigos civiles e incluso principios generales del derecho, aunque no mencionen expresamente a las TIC, podrían servir para establecer orden. Esto es así, porque los hechos y actos jurídicos de base son idénticos en *online* y en *offline*, el cambio sustantivo está en el medio por el que se llevan a cabo, con lo que solo hace falta interpretar evolutivamente las normas existentes, teniendo siempre presentes esos factores base de los hechos y actos jurídicos.

Por todo esto, cuando se habla de *nuevas tecnologías y derechos humanos* la tendencia es poner la mirada en las tecnologías de la información (la inteligencia artificial, los algoritmos, las automatizaciones, la gamificación, el *geofencing*, el internet de las cosas, el análisis predictivo, etc.), ya que, como vemos, generan importantes retos, dudas y preocupaciones. Especialmente porque, como en el ejemplo que antes se ha dado, aunque lo principal sea la libertad de expresión, derechos como la protección de datos, vida privada, derecho a la privacidad y/o derecho a la trasparencia se ponen al mismo tiempo en el centro del debate, al ser condicionantes importantes del ejercicio de los derechos y libertades.

Esto es, que al usarse nuevas vías, medios o plataformas para ejercer derechos y libertades, estas ya no solo involucran al derecho específico que se quiere ejercer, sino al mismo tiempo inciden en derechos que antes de esas vías, medios o plataformas eran irrelevantes o residuales. Siendo justo eso en donde radica mucho del interés/preocupación, como veremos a continuación.

¿Qué ha cambiado entre el ejercicio de derechos humanos *offline* y *online*?

Aquí se ha usado como ejemplo la libertad de expresión, pero piénsese en cualquier otro derecho humano y ocurre lo mismo. Solo ha cambiado la vía, medio o plataforma en que se ejerce y, con ello, los requisitos y condiciones para hacerlo.

Requisitos y condiciones que no se piden, por regla general, en el ejercicio *offline*, sino solo en el *online*. Esto es, datos e información que requieren las tecnologías de la información para funcionar, servir y crecer.

Si en el mundo *offline* para acceder a la justicia solo tenemos que presentar una denuncia ante un juzgado o tribunal, dando nuestra información básica de identificación y contacto, en el ejercicio *online* de ese mismo derecho daremos esa información, más toda aquella que la plataforma que utilicemos requiera para procesar e identificar lo que pedimos, pero también muy posiblemente obtendrá información respecto a dónde nos conectamos, el horario exacto en el que lo hacemos y otras variables que puedan resultar de interés para quien ha diseñado la plataforma que utilizamos. Siendo, por tanto, el primer obstáculo, el poder acceder a esas plataformas, vías o medios de ejercicio del derecho.

Si en el mundo *offline* para ejercer la libertad de movimiento y circulación simplemente debemos trasladarnos de un lugar a otro con los conocimientos que tengamos del lugar o referencias de las que dispongamos, en el ejercicio *online* deberemos indicar el lugar exacto en el que nos encontramos, la forma o medio en el que nos trasladaremos, además de los datos previos que muy posiblemente ya hayamos proporcionado al registrarnos para que se nos indique la ruta que, para no fallar, deberemos de seguir. Generando en muchos casos que si no se tienen esas indicaciones o referencias, se prefiera no ejercer la libertad, al provocar incertidumbre su ausencia.

Si en el mundo *offline* para ejercer el derecho a la educación es suficiente con inscribirse, proporcionando información básica, además de asistir regularmente a una escuela o centro de formación, en el ejercicio *online* del derecho a la educación, adicionalmente a la información antes referida, también se podría aportar información respecto a dónde accedemos, en qué horarios, cuantas veces al día o cuál fue la última vez que accedimos. Pero también, como ha ocurrido con motivo de la pandemia Covid19, en donde muchas escuelas de todos los niveles tuvieron clases por medio de plataformas digitales, se ha podido acceder a la privacidad de las casas de estudiantes y profesorado, con todo lo que eso puede significar. Evidentemente, lo primero para el ejercicio de ese derecho es, de nuevo, poder acceder a esas plataformas, vías o medios por los que se ejerce, que nuevamente, la realidad nos mostró que en muchas casos fue un obstáculo para estudiantes de todos los niveles de estudio.

Mismo ejercicio podríamos hacer con la libertad de reunión, el derecho al trabajo, el derecho al tiempo libre, el derecho a la vida cultural o cualquier otro de los reconocidos en la DUDH. Pero en todos los casos lo importante es destacar que la mayor diferencia está en las plataformas, vías o medios por los cuales se debe hacer el ejercicio de derechos y, con eso, las condiciones que estas imponen para poder ejercer derechos y libertades efectivamente, así como los datos e información que requieren para poder funcionar. Como antes ya decíamos, al usarse nuevas vías, medios o plataformas para ejercer derechos y libertades, estas ya no solo involucran al derecho específico que se quiere ejercer, sino al mismo tiempo inciden en derechos que antes eran irrelevantes o residuales para el ejercicio de derechos y libertades.

Todo esto sin olvidar que, por la forma en la que se ejercen los derechos, muchas veces se genera la sensación de incertidumbre al no conocer quién nos autoriza o limita nuestros derechos, quién nos condiciona nuestras libertades, quién nos autoriza o niega el uso de una plataforma, quién nos censura nuestras expresiones o efectivamente ante quién estamos ejerciendo nuestros derechos y libertades. Es decir, con esta manera de ejercer derechos parece que se difumina la responsabilidad, que se entra en un mundo paralelo (virtual) en donde no hay orden, contención ni control por lo que todo se puede y vale, ya que, por regla general, no hay seres humanos en la inmediatez de ese ejercicio de derechos y libertades.

Pero no nos confundamos, eso no ha cambiado aunque muchas veces nos lo parezca: siempre detrás de toda tecnología existe y existirá la responsabilidad de un ser humano, como persona física o moral. Por eso es importante, antes de dar “aceptar” a las condiciones y registros que se nos exigen para ejercer derechos y libertades, intentar al menos conocer quién es la otra parte firmante, quién nos obliga a aceptar y, sobre todo, qué estamos aceptando dar, ceder, no hacer o hacer.

Bajo esta perspectiva, es claro que no es mucho lo que ha cambiado ni cambiará en el ejercicio de derechos y libertades *online* respecto al mundo *offline*, aunque nuestras percepciones generales puedan ser distintas. Los hechos y actos jurídicos que dan origen al ejercicio de derechos y libertades son en esencia los mismos de siempre, solo que para muchos se nos exige usar vías, medios o plataformas que antes no se tenían o no existían y eso altera nuestra percepción de las cosas.

¿Cuál es el problema del ejercicio *online* de derechos humanos?

El primer problema que tiene el ejercicio *online* de derechos humanos es que en muchas regiones del mundo, incluidas algunas zonas de países que se consideran desarrollados, no se tiene acceso a las plataformas, vías o medios por los cuales se deben ejercer esos derechos y libertades. Si ya en el mundo *offline* existen muchas personas que no tienen acceso a derechos básicos, dar el paso al *online* para el ejercicio de esos derechos parece que olvida muchas realidades que existen en el mundo. Este problema suele llamarse “brecha digital”, pero nosotras preferimos denominarlo “privilegio digital”, en la medida de que, el ejercicio *online* se construye desde el privilegio occidental y lleva a olvidar que muchas regiones del mundo antes que internet o tecnologías digitales, quisieran tener salud, libertad de expresión, alimentos, juicios justos, condiciones mínimas de trabajo o paz.

El segundo problema tiene que ver con ese necesario registro para el ejercicio de derechos y libertades, pues si bien, como ya se veía antes, existen muchos derechos que para ejercerse ya piden información personal básica, en las TIC sin ese registro no hay posibilidad alguna de ejercer los derechos y libertades. Esto tiene relación con el primer problema, pero se agrava especialmente en aquellos derechos en los que no se pide registro en el mundo *offline* para su ejercicio, muchos de ellos derechos y libertades de naturaleza civil y política. Esto puede ser un problema al dejarse registro en el ejercicio *online*, ya que, por una parte, se podría poner en riesgo a las personas en regímenes autoritarios y, por otra parte, se podría impedir o negar el ejercicio de esos derechos "apagando la plataforma", negando el registro indispensable para poder hacer uso de ellas, bloqueando de alguna forma su posibilidad de uso o "apagando" el ejercicio de derechos y libertades.

El tercer gran problema son los datos e información que se requieren para ejercer cualquier derecho o libertad *online*. Especialmente porque en la gran mayoría de los casos van más allá de datos e información vinculados directamente con el derecho o libertad que se pretende ejercer, para llegar a aspectos más íntimos, personales o privados de quien pretende ejercitar un derecho o libertad. Sería menos problemático si existiera transparencia no solo respecto a todos los datos e información que se recogen, sino también de la forma en la que se procesan, los usos adicionales que se les dan y las repercusiones que eso puede tener en otros derechos y libertades.

El cuarto y último problema tiene que ver con la privatización del ejercicio de derechos y libertades, ya que la mayoría de desarrollos de tecnologías de la información se hacen por empresas o entes privados, que aunque puedan poner a disposición de entes públicos la administración y gestión de las plataformas, vías o medios por los cuales se debe hacer el ejercicio de derechos y libertades, el origen y control siempre estará vinculado, e incluso puede ser dependiente de entes privados con intereses, objetivos y fines que no necesariamente pueden ser compatibles con el efectivo ejercicio de derechos y libertades para toda persona, ni con una concepción básica de democracia. De esta manera, el controlador o responsable último de la garantía y respeto de los derechos humanos está controlado y sometido a los designios privados. Por eso, más que leyes nuevas, lo que ha pasado es que se ha cedido el poder de orden y control a entes privados. Pero frente a eso, ya existen leyes civiles, penales, mercantiles, administrativas, etc. que podrían controlar las actividades de dichos entes privados. Lo que más falta es voluntad y ejercicio correcto del poder de autoridad.

Estrechamente vinculado con esto y el "privilegio digital" está el hecho de tener la posibilidad de conocer quiénes son los dueños de los lugares en donde se diseña y crea la tecnología, en dónde se distribuye y quién tiene efectivamente acceso a ella; pues de eso dependerá no solo quién puede tener el control último del ejercicio de derechos y libertades, sino también de sus fines, alcances y usos que se pueda autorizar darle. Situación que no es menor pero que, al interactuarse con "máquinas" en el mundo *online*, también se difumina al momento de identificar quién está detrás o simples explicaciones de las razones por las cuales las TIC funcionan de una forma y no de otra.

Todo lo anterior sin olvidar lo que venimos diciendo respecto al analfabetismo digital que se potencia con el analfabetismo legal, la aparente difuminación de responsabilidades y lo acelerados que son muchos procesos tecnológicos.

A pesar de todo esto, no podemos perder de vista que al menos los últimos tres aspectos que aquí planteamos como problemas no lo son, ni lo serían o lo serían menos, si todo eso se utiliza y gestio-

na siguiendo estándares mínimos de derechos humanos (transparencia, no discriminación, protección vida privada, tutela judicial, etc.) y con el fin de alcanzar la pretendida universalidad, interdependencia y efectividad de todos los derechos humanos para toda persona en el mundo.

Con lo que, bajo esa mirada positiva, el único problema real sería el "privilegio digital" que olvida que los desarrollos tecnológicos no están presentes en todas las regiones del mundo. Privilegio que, también de manera clara ha quedado muy presente con motivo de la pandemia Covid19, cuando vemos en dónde y cómo se han desarrollado las vacunas, dónde están siendo aplicadas, cómo están siendo distribuidas y dónde grandes sectores de la población siguen sin acceso a dichas vacunas mientras hay países con más del 80% de su población vacunada.

Pero no solo eso, por desgracia los temores se mantienen también porque al final de cuentas, las tecnologías en general (no solo las TIC) son creadas por los seres humanos, por lo que éstas son un reflejo más de la realidad en la que vivimos. Realidad que nos muestra muerte, desigualdad, injusticias, atrocidades, guerra y otras calamidades. Que si bien no son generalizadas, tampoco nos permiten pensar que es posible hoy que todo eso desaparezca, sino por el contrario, que por desgracia las tecnologías pueden seguir sirviendo para esas situaciones que actualmente sufre una parte importante de la humanidad.

Tecnologías y derechos humanos ¿sí o no?

La respuesta no puede ser otra que: sí. En primer lugar, porque como antes se ha señalado, el artículo 27 de la Declaración Universal de Derechos Humanos reconoce el derecho a "participar en el progreso científico y en los beneficios que de él resulten." Siendo evidente que uno de esos beneficios tiene que ver directamente con las tecnologías que son uno de los productos del progreso científico.

Pero no solo eso, el artículo 26 de la Declaración al hablar de educación, establece que "[l]a instrucción técnica y profesional habrá de ser generalizada". Con lo que el acceso a formaciones técnicas y profesionales que permitan una correcta participación en el progreso científico y sus beneficios, debería estar garantizada en todos los países.

Así, la relación entre ciencia (tecnologías) y derechos humanos, podríamos decir que viene dada desde la misma Declaración Universal de Derechos Humanos. Y evidentemente no podría ser de otra manera, pues todo lo que sume y permita la pretendida universalidad de los derechos humanos siempre debe ser más que bienvenida.

Cómo negarse a la existencia de una máquina que nos permitiera poner fin a las diversas discriminaciones al facilitar el entendimiento, comprensión y tolerancia de las personas ante la diversidad. Así como son bienvenidas todas esas máquinas (tecnologías) que ayudan a mantener o salvar la vida de las personas cuando ésta está en peligro o al detectar enfermedades.

De igual forma que serán bienvenidas tecnologías que ayuden a identificar y denunciar casos de tortura, esclavitud o detenciones arbitrarias; como aquellas que permitieran, de manera efectiva, que toda persona sin importar en el lugar en el que se encuentre y sin discriminación, pueda acceder a la justicia, a la educación, a la vida cultural y artística o a ejercer su derecho a la nacionalidad.

Sin duda, a eso no podemos negarnos. De hecho, eso debería ser un objetivo. Evidentemente, sin perder de vista todo lo que antes se ha señalado respecto a los problemas que plantea el ejercicio de los derechos humanos por medio de algunas tecnologías y los impactos negativos que puede tener si se olvida que en la realidad humana de muchas partes del mundo, el acceso a tecnologías está muy lejos de ser posible, al no tenerse garantizados siquiera derechos básicos que permiten hablar de respeto de la dignidad y un nivel de vida adecuado.

Con lo que la apuesta por que las tecnologías sean parte del ejercicio de derechos y libertades no debería descartarse de entrada, pero siempre se deben tener presentes sus riesgos, que en mucho son también los riesgos que tenemos en lo que aquí se ha denominado como mundo *offline*, pues la tecnología no aparece de forma espontánea ni es neutral en muchos de sus aspectos, es una creación humana más, con todo lo que eso implica en positivo y negativo.

Tal vez la principal advertencia que, incluso en aspectos que parezcan integralmente positivos, se debe hacer, es que las tecnologías en todo caso deben ser herramientas, simplificadoras o agilizadoras de procesos, facilitadoras de actividades humanas, pero no decisoras únicas y finales. Las decisiones vinculadas con el ejercicio de derechos y libertades pueden apoyarse en las tecnologías, pero no ser su única base ni la única razón que justifique el ejercicio o la restricción de derechos y libertades; como tampoco pueden ser el único medio por el cual se pueda ejercer o buscar la garantía de derechos fundamentales.

Lo anterior, por su influencia actual, se dirige especialmente a las TIC. Pero no solo se debe poner atención a estas, ya que desde mucho antes de su creciente desarrollo, otras tecnologías también han impactado e impactan en el ejercicio, goce y garantía de los derechos humanos.

Esto debe ser siempre una línea insuperable por más que en una tecnología encontremos solo bondades y beneficios, pues la realidad humana en el ejercicio de derechos y libertades no se trata de A o B ni de blanco o negro, requiere de muchos matices que solo se podrán tener en cuenta con el trabajo conjunto-colaborativo de seres humanos y tecnologías.

cap. 2

Impactos de las tecnologías en los derechos humanos[3]

3 Este apartado y los siguientes han sido desarrollados esencialmente por Anna Pont, con colaboración de María Agostina Passera y Karlos Castilla.

Con los elementos que se establecieron en el análisis introductorio, ahora es momento de concretar los impactos que las tecnologías pueden tener en cada uno de los derechos humanos reconocidos en la DUDH.

Para ese fin, a continuación, en primer lugar, se cita de manera textual el contenido de cada uno de esos derechos humanos. En segundo lugar, se hace mención de algunos usos positivos y negativos que pueden tener algunas tecnologías en el derecho respectivo, así como se exponen ejemplos específicos que se han identificado en esta investigación, para dar muestra de algunos de los impactos que reciente cada derecho humano. Finalmente, cuando existen, se citan opiniones, recomendaciones u observaciones que han formulado órganos de Naciones Unidas con relación a algunos derechos.

La primera advertencia que debemos hacer es que, en muchos casos, las tecnologías que más se ponen de relieve son TIC. También, que lo que más existe y está disponible son las muestras de los efectos negativos de las tecnologías, de los aspectos positivos poco se habla en infinidad de documentos, investigaciones académicas y periodísticas, así como en trabajos especializados existentes. De igual forma debemos señalar que, aunque buscamos hacer análisis específicos por cada uno de los 27 derechos reconocidos en la DUDH, a fin de evitar repeticiones innecesarias, se han tenido que agrupar algunos para facilitar la lectura y mostrar de mejor forma los impactos que se han identificado hasta ahora.

Por otra parte, debemos advertir de que los análisis que ahora se presenta respecto a qué tecnologías existen, sus impactos y posibilidades, se desarrollan desde la visión de tres personas residentes en Barcelona. Las tres con estudios de posgrado en Derecho, dos de origen latinoamericano y una europeo, dos mujeres y un hombre, dos de piel blanca y una morena, con edades entre los 25 y 42 años. Un dato que queremos se tenga en consideración, ya que ante la magnitud de información existente, a pesar de los sesgos y privilegios de los que partimos, hemos intentado tener visiones inclusivas de realidades que nos son ajenas en nuestra vida cotidiana.

La última advertencia es que, como se ha señalado desde el inicio, este es un *documento de trabajo*, lo que significa que tan solo es la base a partir de la cual queremos desde el IDHC desarrollar otros análisis en la materia. Como tal, es tan solo la base inicial, inacabada y abierta para incluir todas las tecnologías posibles y no solo los impactos negativos. Sin embargo, por ahora, teníamos que establecer unas bases mínimas y una limitación temporal, ya que de otra forma, por todo lo que existe y se descubre día con día, nunca íbamos a tener un documento base que nos sirva de referencia en todos los desarrollos posteriores.

Establecido esto, entramos en materia:

Artículo 1: todos/as nacemos libres e iguales

> Todos los seres humanos nacen **libres e iguales en dignidad y derechos** y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros.

Artículo 2: derecho a ser libre de discriminación

> Toda persona tiene **todos los derechos y libertades** proclamados en esta Declaración, **sin distinción alguna** de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición. Además, no se hará distinción alguna fundada en la condición política, jurídica o internacional del país o territorio de cuya jurisdicción dependa una persona, tanto si se trata de un país independiente, como de un territorio bajo administración fiduciaria, no autónoma o sometida a cualquier otra limitación de soberanía.

Toda máquina, infraestructura, equipamiento, instrumento, aplicación, etc., que sea diseñada teniendo presente la diversidad de nuestras sociedades locales, nacionales, regionales y mundiales, sin duda, puede generar un **impacto positivo** en la igualdad y no discriminación que deben estar presentes en el ejercicio de todos los derechos y libertades reconocidos en la DUDH.

Vinculado directamente con esto, además, está necesariamente la posibilidad de que toda persona pueda acceder, usar y disfrutar de las tecnologías, pues de no hacer estos dos aspectos posibles, como base para el resto de derechos, parecería muy difícil hablar de impactos positivos cuando solo una parte muy reducida o región de la comunidad internacional tiene acceso a dichas tecnologías.

Así, parecería que solo podremos hablar de impactos positivos de las tecnologías en la medida en que toda persona pueda gozar de ellas, cuando ninguna tecnología se diseñe teniendo como parámetros exclusivos solo a un tipo de persona, ni buscando dirigirse a un grupo específico para identificarle y discriminarle. Si esto se tiene en cuenta, para limitar o reducir sus efectos perjudiciales, los impactos de las tecnologías podrían ser muy positivos.

El contenido de estos dos artículos (1 y 2) tendrá efectos similares en todos aquellos artículos donde la problemática de la tecnología radica en la discriminación. También, en relación con el concepto "libres" podría incluirse lo referente a todas aquellas tecnologías de la información y comunicación (TIC) que pueden ser usadas con el fin de manipular, desinformar y polarizar a sus usuarias[4].

Por otra parte, en el uso de tecnologías que requieren de una base de datos generada e introducida por un humano, siempre existirá el riesgo de que la información esté contaminada de los sesgos y prejuicios de quien los introduce. Por ejemplo, si la información insertada en la tecnología (*data*) fomenta la discriminación, de cualquier índole, la tecnología va a aprender y a establecer patrones discriminatorios, los va a normalizar. Consecuentemente, se corre el riesgo de que poner en duda dichas tecnologías sea más complicado.

A modo de ejemplo, en lo que se refiere a la discriminación por sexo y género, la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de la ONU analiza los procesos de moderación de contenidos utilizados por las plataformas digitales dominantes y concluye en la necesidad de prestar más atención al papel de los algoritmos y las decisiones de diseño de estas empresas. Explica que los algoritmos están diseñados en base a normas que han sido delineadas por personas con sesgos de género, prejuicios y visiones del mundo homogéneas (que no admiten diversidad) y elitistas. Estos sesgos generan un discurso nocivo hacia mujeres y personas de género no conforme, y hasta operan en contra de ellas, eliminando automáticamente imágenes y contenidos producidos por mujeres por considerarlos contrarios a sus políticas. Requiere expresamente que estos modelos de moderación de contenidos se adecúen a las normas internacionales de derechos humanos.

Asimismo, la Relatora Especial explica que existe una fuerte disparidad en el acceso a Internet de las mujeres, asegurando que esta desigualdad implica un obstáculo para su empoderamiento, especialmente de las que están excluidas de otros espacios públicos, como las personas de género no conforme o jóvenes de sociedades tradicionales. Afirma que, a nivel mundial, solo el 48% de las mujeres tienen acceso a la tecnología de la información y las comunicaciones, proporción que en África desciende al 23%. Este "privilegio digital" de género es un gran obstáculo para la igualdad de derechos de las mujeres y las niñas a la libertad de expresión[5].

Por su parte, el Comité para la Eliminación de la Discriminación contra la Mujer, en su Recomendación General No. 34, indica que, en el caso de las mujeres y niñas rurales, esta brecha digital se acentúa en razón de la pobreza, el aislamiento geográfico, las barreras lingüísticas, la falta de conocimientos informáticos y los estereotipos de género discriminatorios.

Y como un reflejo más transversal, bien vale tener en cuenta lo establecido por el Comité para la Eliminación de la Discriminación Racial de la ONU, que en su Observación General No. 36 estable-

4 En los últimos años ha surgido el debate alrededor de cómo las redes sociales influyen en la radicalización ideológica de sus usuarios. Al respecto, e intentando mostrar opiniones diversas, véase, por ejemplo: Berger, JM., Strathearn, B., "Who Matters Online: Measuring influence, evaluating content and countering violent extremism in online social networks", *The international center for the study of radicalization and political violence* (2013); Ledwich, M., Zaitsev, A., "Algorithmic Extremism: Examining Youtube's Rabbit Hole of Radicalization", *First Monday*, 25(3), (2020).

5 Véase: Informe A/76/258 de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan, 30/07/2021.

ció que: “la utilización cada vez mayor de nuevas herramientas tecnológicas, incluida la inteligencia artificial, en ámbitos como la seguridad, el control de fronteras y el acceso a los servicios sociales, puede profundizar el racismo, la discriminación racial, la xenofobia y otras formas de exclusión. […]. Aunque es consciente de que, en algunos ámbitos, la inteligencia artificial puede contribuir a una mayor eficacia en una serie de procesos de adopción de decisiones, el Comité también comprende que existe un riesgo real de sesgo algorítmico cuando se utiliza la inteligencia artificial en la adopción de decisiones en el contexto de la aplicación de la ley. La elaboración de perfiles algorítmicos plantea serias preocupaciones y las consecuencias con respecto a los derechos de las víctimas podrían ser muy graves”[6].

Con lo que parece evidente que las nuevas tecnologías, sean del tipo que sean, no podrán generar impactos positivos en la igualdad y no discriminación, mientras nuestras sociedades no avancen en su eliminación y mientras no se combatan efectivamente las estructuras de inequidad, exclusión y discriminación que seguimos teniendo en todas las regiones del mundo, aunque agravadas cuando, como expusimos antes, se comparan regiones del mundo entre sí.

Si en eso no hay progresos, las tecnologías solo serán un reflejo más de la desigualdad y discriminación.

Artículo 3: derecho a la vida, la libertad y la seguridad

> Todo individuo tiene **derecho a la vida, a la libertad y a la seguridad** de su persona.

Estos derechos pueden abarcar un muy importante ámbito de aspectos de la vida, lo cual nos permite pensar en varios desarrollos tecnológicos que generan tanto efectos positivos como negativos.

Dentro de los impactos positivos, podríamos pensar en todas aquellas tecnologías de la **vida diaria** que promueven la salud: porta medicamentos que te envía recordatorios, equipos o aplicaciones en móviles que mejoran la rutina de ejercicios y la personalizan, servicio de videollamadas con profesionales de la salud, etc.

Pero también, **prótesis** inteligentes e implantes para personas con discapacidad; tecnologías que asisten al **ritmo cardíaco**: holter implantable (que registra la actividad del corazón para detectar anomalías), marcapasos (aparato que se coloca quirúrgicamente junto al corazón y que, mediante señales eléctricas, regula la estimulación del corazón y mantiene la frecuencia cardíaca adecuada a las necesidades de cada momento), GPS cardíaco (que ofrece visión espacial y tridimensional de la anatomía del corazón), tele asistencia (dispositivos colocados en el corazón que envían notificaciones constantes a los médicos sobre el ritmo cardíaco del paciente); **respiradores, rayos x, resonancias magnéticas** o la **cirugía robótica** que permite a los médicos hacer muchos tipos de procedimientos complejos con ma-

6 Véase: Recomendación General No. 36 (2020), relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden, Comité para la Eliminación de la Discriminación Racial, párr. 12.

yor precisión, flexibilidad y control en comparación con las técnicas convencionales. La cirugía robótica generalmente está asociada con la cirugía de invasión mínima (procedimientos realizados a través de pequeñas incisiones). Algunas veces se utiliza también en determinados procedimientos quirúrgicos abiertos tradicionales.

En otro ámbito podríamos pensar en tecnologías empleadas en el espacio para **observar la Tierra** (EO – *earth observation*), que podrían usarse con el objetivo de observar vulneraciones de derechos humanos/conflictos humanitarios y también detectar cuestiones climáticas y ambientales.

Pero también se podría pensar en **técnicas de reproducción humana asistida**: inseminación intrauterina, fecundación in vitro (FIV). Otras técnicas como preservación de embriones congelados o vitrificados (para implantarse luego) o diagnóstico genético preimplantacional (para detectar enfermedades genéticas en embriones), surgieron como consecuencias del desarrollo de las FIV.

De igual manera en **automóviles** inteligentes que utilizan Inteligencia Artificial (IA) tomando como base decisiones humanas, analizando variables y permitiendo minimizar daños. Disminuyen la tasa de accidentalidad y reducen las emisiones contaminantes. Pero en general, muchas tecnologías que se han ido incorporando a diversos medios de transporte para mejorar la seguridad y la vida. Y podríamos seguir con muchos más ejemplos.

En la parte negativa, se podría mencionar el **uso excesivo** de la tecnología (*smartphones, tablets* y otros dispositivos) que puede dañar los sistemas cerebrales encargados de procesar emociones, de mantener la atención y de tomar decisiones. Puede provocar ansiedad, depresión severa, intentos de suicidio[7]; la **contaminación** producida por desechos tecnológicos, el uso de **armas** sin intervención humana directa como los ataques armados con **drones**, las armas autónomas (lo desarrollamos en artículo 5), pero también sistemas de vigilancia que más que seguridad producen acoso e intimidación, etc.

De manera más concreta, se podría establecer, por ejemplo, que las TIC han contribuido, en menor o mayor grado, a la polarización de la sociedad y han facilitado y fomentado los discursos de odio, alimentando así la discriminación. En el caso de Myanmar, por ejemplo, el uso de esta tecnología, concretamente de las redes sociales (***social networking service*** o *social media*) y, en especial, de Facebook, permitió la publicación de propaganda racista (incluso por parte de las autoridades birmanas), fomentando el odio y la violencia contra la minoría rohinyà. Esto pudo desembocar en una desinformación de la población e incitación a realizar una "limpieza étnica", causando al final muertes y migraciones forzadas, hechos constitutivos del delito de genocidio. Los propietarios de esta plataforma admitieron su responsabilidad en el asunto, asumiendo que no se preocuparon en verificar el contenido que circulaba por esta red en el país. A todo esto, Facebook es considerada por la mayoría de habitantes de Myanmar la única fuente fiable de información. Así, mientras que en 2014 únicamente el 1% de la población de Myanmar tenía acceso a internet, en 2016 ya tenía más personas usuarias de Facebook que cualquier otro país asiático. En 2018 más del 26% de su población usaba Facebook[8].

7 Vése para más información: https://www.bbc.com/mundo/vert-fut-42628812 y http://ciencia.unam.mx/leer/893/como-las-redes-sociales-pueden-causarte-depresion

8 Véase para más información: https://www.theguardian.com/world/2018/apr/03/revealed-facebook-hate-speech-exploded-in-myanmar-during-rohingya-crisis

En 2019, otra red social, Twitter, suspendió la cuenta de un militar de Myanmar (se calcula que bajo su mando, 700.000 rohinyá se vieron forzados a migrar). Este fue acusado de complot para llevar a cabo un genocidio contra la minoría musulmana rohinyá tras recibir quejas referidas al uso de su cuenta personal para propagar discursos de odio. Su cuenta de Facebook fue eliminada en 2018 después de que Naciones Unidas reconociera los hechos sucedidos en el país como genocidio[9].

Otra cuestión es el uso de esta tecnología (las redes sociales) como medio para llevar a cabo actos dañinos con mayor facilidad y mayor alcance. Es el caso, por ejemplo, del acoso. Con las redes sociales se ha creado un nuevo concepto: el **ciberacoso**, esto es, el uso de medios digitales con fines de acoso a una o varias personas. Ello se lleva a cabo, a menudo, mediante la divulgación de información personal o falsa. Si bien es cierto que el acoso, como tal, ya existía, los medios digitales permiten el anonimato, ofrecen un elevado número de personas usuarias y acceso a ellos y, por lo tanto, mayor número de posibles víctimas.

También ha surgido otro nuevo concepto: el **delito digital** (*cybercrime*), es decir, el uso de los medios digitales con el fin de cometer cualquier acción antijurídica. Hay ocasiones donde la comisión de estos ciberdelitos atenta contra la vida y seguridad de las personas (ver *infra* artículo 4). Así, por ejemplo, en 2017, varios hospitales de Reino Unido fueron víctimas de un ciberataque a gran escala que bloqueó sus ordenadores y que exigía el pago de cierta suma de *bitcoins*. Debido a esta situación, la atención sanitaria se vio suspendida durante algunas horas y ello obligó a los centros sanitarios afectados a desviar pacientes de urgencias, pudiendo colapsar el sistema[10].

Los drones o los vehículos aéreos no tripulados (UAV), incluidos en la robótica (si bien es cierto que se sirven de otras tecnologías, como, por ejemplo, GPS) también pueden suponer un riesgo para la salud, la libertad y la seguridad de las personas, dependiendo del uso que se les dé. Estos instrumentos se pueden usar con fines de contrabando o con fines terroristas (drones kamikaze, *lotering munition, suicide drones*)[11].

Otro aspecto que pone en riesgo la vida, la libertad y la seguridad de las personas es la contaminación provocada por las tecnologías en sus fases de:

- **Fabricación de los dispositivos tecnológicos** (móviles, ordenadores, baterías, etc.), cuya elaboración exige la extracción de materias primas (como el zinc, el litio, el cobre, el coltán, etc.). Más allá de la contaminación derivada de la extracción de estos elementos, las condiciones laborales de las personas que se dedican a ello son precarias y atentan contra los derechos humanos (en relación también con los artículos 4 y 23 DUDH). Un claro ejemplo de ello sucede en Ruanda y en la República Democrática del Congo, donde se extrae coltán artesanalmente mediante el sistema de explotación. En muchos casos son menores los que se dedican a ello. Además, muchas

9 Véase para más información: https://www.theguardian.com/world/2019/may/16/myanmar-army-chiefs-twitter-account-suspended-over-anti-rohingya-hate-speech

10 Véase para más información: https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html

11 Véase para más información: https://paxforpeace.nl/media/download/paxviolentskies_0.pdf y https://eandt.theiet.org/content/articles/2021/04/conflict-groups-arm-consumer-drones-to-deliver-death-and-terror/

de las minas de coltán son "propiedad" de grupos armados, que mantienen a sus trabajadores en condiciones inhumanas, sin cumplir con las normas básicas de prevención, seguridad y respeto al medioambiente ni al trabajador[12].

- **Consumo de datos y calentamiento global:** cuando se usan los dispositivos tecnológicos (por ejemplo, para hacer fotografías, para enviar mensajes, para usar aplicaciones, para descargar archivos de música, fotografías, documentos, etc.), se produce tráfico de datos. A mayor uso, mayor tráfico. Para ello es necesaria la creación de instalaciones adaptadas para almacenar todo este tráfico de datos, los llamados centros de datos (*data centers*). Por tanto, cuanto más uso se da a los dispositivos, mayor tráfico de datos y, consecuentemente, aumenta la necesidad de instalar más centros de datos o de adaptar las instalaciones de los ya existentes. Estos centros de datos consumen mucha electricidad (en 2020, por ejemplo, suponía el 2% de la producción eléctrica mundial), requieren sistemas de almacenamiento y de refrigeración (que también consumen electricidad). Todo ello, finalmente, se traduce en la emisión de gases de efecto invernadero[13], que pone en riesgo la vida y la seguridad de las personas[14].

- **Desechos tecnológicos (*e-waste*)**[15]: cuando los dispositivos tecnológicos llegan al fin de su vida útil, se convierten en desechos que terminan en determinadas zonas y no en otras (en relación también con los artículos 1, 2 y 25). Además, las empresas a menudo programan la obsolescencia de los dispositivos tecnológicos para así poner fin a su vida útil de forma anticipada y aumentar el consumo, hecho que aumenta el impacto que tienen los puntos anteriores en los derechos humanos (mayor número de dispositivos tecnológicos implica más peligros).

Siguiendo la línea de la contaminación provocada por las tecnologías y cómo esto puede afectar a los derechos humanos (en relación también con el artículo 25): el auge de las **criptomonedas** o monedas digitales ha contribuido a ello[16]. Un ejemplo es el *bitcoin* (BTC) que utiliza tecnología de ***blockchain*** (cadena de bloques) y ***data***; y para obtener bitcoins se usa una técnica llamada "mining" o minado.

Un estudio realizado por la Universidad de Cambridge evidencia que esta criptomoneda consume más electricidad anualmente (2021) que Argentina y que Países Bajos, por ejemplo[17]. Para minar *bitcoins* se usan ordenadores para resolver complejos problemas matemáticos, por lo que requiere que se consuma energía eléctrica constantemente.

12 Véase para más información: https://reliefweb.int/report/democratic-republic-congo/coltan-and-conflict-drc, así como http://www.relec.es/RECICLADO_ELECTRONICO/Minerales/coltanreporten.pdf y https://www.newsecuritybeat.org/2008/12/coltan-cell-phones-and-conflict-the-war-economy-of-the-drc/

13 Véase para más información: P. Bertoldi, M. Avgerinou, L. Castellazi, Trends in data centre energy consumption under the European Code of Conduct for Data Centre Energy Efficiency (2017); JRC, The European Programme for Energy Efficiency in Data Centres: The Code of Conduct (2019); L. Belkhir, A. Elmeligi, "Assessing ICT global emissions footprint: Trends to 2040 and Recommendations", *Journal of Cleaner Production* (2018); A.S.G. Andrae, "Hypothesis for primary energy use, electricity use and CO2 emissions of global computing and its shares of the total between 2020 and 2030", *Wseas Transactions on Power Systems*, Volume 15 (2020), pp. 50 – 59.

14 Véase para más información: https://www.computerworld.com/article/3431148/why-data-centres-are-the-new-frontier-in-the-fight-against-climate-change.html, así como: https://www.vox.com/2017/11/8/16621512/where-does-my-smartphone-iphone-8-x-go-recycling-afterlife-toxic-waste-environment y https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662906/IPOL_STU(2021)662906_EN.pdf

15 Véase para más información: https://hablandoenvidrio.com/la-contaminacion-tecnologica-ejemplos-y-su-impacto/

16 Véase para más información: https://builtin.com/blockchain/blockchain-applications

17 Véase para más información: https://cbeci.org/cbeci/comparisons

En términos generales y de manera breve, existe un número limitado de *bitcoins* (25M), y conforme se van minando, el problema matemático a resolver para minarlos se vuelve más complejo. A mayor complejidad, un ordenador *average* no puede minar, se requieren ordenadores y equipos especiales para procesar toda la energía que ello consume. Estos equipos informáticos requieren, por tanto, más electricidad. Se comenta que el "minaje" de *bitcoins* se realiza, en la mayor medida de lo posible, mediante electricidad que procede de energías renovables, pero quienes critican esta tecnología afirman que los "mineros" se establecen donde la electricidad es más barata y, en muchas ocasiones, se usa el carbón. A día de hoy, como no se hace un control, desde los gobiernos, de dónde proviene la energía que se usa para minar *bitcoins*, es difícil afirmar o negar que se trate de fuentes renovables. Un elevado consumo de energía eléctrica se traduce en emisiones de dióxido de carbono[18].

En una parte positiva, para no mirar solo los aspectos que nos preocupan, también se puede decir que las **TIC** han contribuido a mejorar la calidad de vida de las personas con discapacidad. Un informe realizado en España en 2021 refleja que el 70% de las personas con discapacidad encuestadas asegura que las nuevas tecnologías han mejorado su calidad de vida global, facilitando su formación, acceso al empleo, ocio o comunicación. Sin embargo, dicho análisis también refleja que el 48% de los encuestados encuentra barreras en el acceso, uso y manejo de las nuevas tecnologías. A un 29% les parece complejo y avanzado su uso, un 24% afirma carecer de recursos económicos para acceder a las mismas, y un 16% desconfía de lo digital por temor a ser engañado o a ser víctima de fraude[19].

Aunque siguen presentando desafíos a la hora de adaptarlas y hacerlas accesibles a toda persona, las nuevas tecnologías son un apoyo fundamental para las personas con discapacidad. Así lo ha resaltado la Convención sobre los derechos de las Personas con Discapacidad adoptada en 2006 en el marco de Naciones Unidas. La misma establece la necesidad de que los Estados adopten medidas para asegurar a las personas con discapacidad tecnologías de apoyo, dispositivos técnicos y ayudas para la movilidad de calidad. Ello a fin de lograr una forma de vida independiente y un pleno ejercicio de sus derechos, incluido el derecho al trabajo, a la libertad de expresión, al derecho a participar de la vida política, etc. La Convención reconoce a las nuevas tecnologías como uno de los medios para alcanzar la igualdad de condiciones de las personas con capacidades diferentes.

En todas aquellas cuestiones relacionadas con la tecnología y su incidencia en la vida del ser humano, ya en 2005 la UNESCO puso el foco en la necesidad de aprovecharse de los avances científicos, sin perder de vista los principios básicos consagrados por las normas que rigen el respeto por la dignidad de la persona, los derechos humanos y las libertades fundamentales. En este sentido, aprobó la **Declaración Universal sobre Bioética y Derechos Humanos** que se encarga de delinear los límites éticos que conlleva el desarrollo científico y tecnológico, como son el respeto por la integridad personal, la privacidad y confidencialidad, la equidad en el acceso, la no discriminación y no estigmatización, entre muchos otros.

18 Véase para más información: https://pubs.acs.org/doi/10.1021/acs.est.9b05687 y https://www.cell.com/joule/fulltext/S2542-4351(19)30255-7?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435119302557%3Fshowall%3Dtrue

19 Véase: "Informe Tecnología y Discapacidad", Fundación Adecco, con la colaboración de Keysight Technologies, Julio 2021. Conclusiones basadas en una encuesta realizada a 700 personas con discapacidades físicas, sensoriales, intelectuales y psíquicas residentes en España, entre 18 y 50 años.

Artículo 4: derecho a ser libre de la esclavitud

> Nadie estará sometido a **esclavitud ni a servidumbre**, la esclavitud y la trata de esclavos están prohibidas en todas sus formas.

En este derecho, las tecnologías podrían aportar mucho. Por desgracia, un importante número de sus usos actuales no han ido especialmente en ese sentido. Si bien la **IA** y el ***Big data*** pueden ser utilizadas para **rastrear** a los traficantes de personas así como para crear herramientas para la **transparencia** en las cadenas de suministro, son pocos aún los desarrollos en esta materia. Más se ha hecho con las **redes sociales** para reportar situaciones de abuso y de **maquinarias que reemplazan** a las personas en el desarrollo de trabajos forzados y trabajos peligrosos.

Sin embargo, por desgracia, las **TIC** han facilitado la aparición de nuevas vías para someter a esclavitud y servidumbre. Es el caso, por ejemplo, de las ***darkweb*** (redes que se superponen a la internet pública y requieren de *softwares* específicos y configuraciones o autorización para acceder, y forman parte de la ***deep web***). Esta tecnología ha sido y está siendo usada por algunas personas con fines de esclavitud, explotación y tráfico humano (en relación también con el artículo 3 DUDH, *supra*). Todo esto sin olvidarnos de que las tecnologías, por sí solas, no son "malignas", todo depende del uso que le dé el usuario.

Un ejemplo de *darkweb*, muy popular, es Tor (*TheOnionRouter*), que permite que el encaminamiento de los mensajes intercambiados entre los personas usuarias no revele su identidad (IP) y que se mantenga la integridad y el secreto de la información que viaja por ella. Un estudio[20] encontró que esta plataforma se utiliza comúnmente para solicitar pornografía infantil, abuso (en general, de menores) y tráfico humano[21]. También puede considerarse el tráfico ilegal de órganos.

Este tipo de plataformas puede facilitar la identificación y el "reclutamiento" de potenciales víctimas; el alquiler de locales para alojar a las víctimas; el transporte de estas; el control y la coacción a las víctimas; anunciar los servicios; la explotación de las víctimas; para comunicarse con los depredadores o personas usuarias; y para realizar transacciones económicas[22].

Otro estudio ha evidenciado[23] que las plataformas digitales también están siendo usadas con la finalidad de reclutar y facilitar el tráfico de personas, sobre todo mediante o a través de páginas web de entretenimiento adulto, anuncios, aplicaciones, juegos de ordenador, *darkweb*, correo electrónico, aplicaciones o páginas de citas *online*, fórums *online*, redes peer to peer y redes sociales.

20 Véase para más información: https://www.cigionline.org/sites/default/files/no20_0.pdf

21 Véase para más información: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf

22 Véase para más información: https://www.osce.org/files/f/documents/9/6/455206_1.pdf

23 Véase para más información: https://www.trilateralresearch.com/wp-content/uploads/2018/02/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL.pdf

Los anuncios *online* se han convertido en una herramienta esencial para la explotación sexual, que permiten a los traficantes conectar con posibles víctimas. Un estudio realizado por Thorn[24] muestra que el 63% de los menores de edad víctimas de tráfico-sexual fueron publicitados online y que el 42% de las víctimas de sextorsión conocieron a sus depredadores online.

Otra evidencia de esta problemática es el fenómeno ***Webcam Child Sex Tourism*** (WCST). Consiste en una forma de explotación infantil en la que adultos pagan para presenciar en vivo y dirigir vídeos de menores manteniendo relaciones sexuales frente una webcam (sucedido especialmente en Filipinas). Se trataría, pues, de una forma de esclavitud. Es interesante mencionar que se llevó a cabo una iniciativa para detectar y localizar a depredadores y personas usuarias de WSCT mediante IA[25]. Se crearon Sweetie y Sweetie 2.0, simulaciones de potenciales víctimas para poder rastrear a las personas usuarias[26]. Por tanto, tal y como se viene comentando, la peligrosidad de esta y de las demás tecnologías que se mencionan depende del uso que se les dé.

El mal uso de las redes sociales también se ha traducido en otras problemáticas. Por ejemplo, se ha llegado a hacer uso de ellas para publicitar y poner a "subasta" a una menor de edad con la finalidad de encontrar a alguien con quien casarla. Ello puede derivar en matrimonio forzado. Un caso concreto sucedió en 2018, cuando, mediante la plataforma Facebook, el progenitor de una menor de edad sudanesa publicó una fotografía suya "poniéndola a subasta" para casarla con "el mejor postor". El anuncio permaneció publicado en Facebook durante dos semanas[27].

También se pone de manifiesto el uso que puede darse a tecnologías como el GPS en los coches de las personas trabajadoras, u otras tecnologías biométricas, como sería el reconocimiento facial, la huella dactilar o del iris, para llevar a cabo un control del horario laboral y de la localización de las personas trabajadoras con fines de explotación.

Otro riesgo de esclavitud gira en torno a lo que se ha comentado anteriormente, a la extracción de materiales necesarios para la fabricación de dispositivos tecnológicos. Como se ha puesto de manifiesto, en las minas de estos materiales no se garantiza a las personas trabajadoras unas condiciones de trabajo dignas, lo que puede derivar en esclavitud[28].

No hay duda alguna de que en todos estos ejemplos el uso, más que la tecnología en sí misma, hacen que su impacto sea negativo. Pero si es así, parecería que, entonces, el llamado debería ir en el sentido de sancionar esos usos inadecuados y claramente flagrantes de derechos humanos.

24 Véase para más información: https://www.thorn.org/

25 Véase iniciativas como: https://www.terredeshommes.org/ y https://www.netclean.com/

26 Véase para más información: https://www.tdh.ch/en/projects/sweetie-how-stop-webcam-child-sex-tourism

27 Véase para más información: https://gulfnews.com/world/mena/child-brides-now-being-auctioned-off-on-social-media-1.1542798382754 y https://edition.cnn.com/2018/11/20/africa/south-sudan-child-bride-facebook-auction-intl/index.html

28 Véase para más información: https://www.abc.net.au/news/2020-03-01/tech-companies-rely-child-labour-abuse-to-mine-coltan-in-congo/11855258 y https://www.amnesty.org/en/latest/news/2016/01/child-labour-behind-smart-phone-and-electric-car-batteries/

Artículo 5: derecho a ser libre de la tortura

> Nadie será sometido a **torturas ni a penas o tratos crueles**, inhumanos o degradantes.

Con este derecho ocurre algo similar que con el anterior en cuanto a los malos usos, además de que se relaciona con muchas de las situaciones descritas en los artículos antes analizados por afectar la integridad del ser humano.

Así, existe el riesgo de que se usen **armas autónomas**, es decir, armas con la capacidad de usar IA para replicar el razonamiento cognitivo humano, tomando decisiones de forma autónoma, con fines contrarios a los derechos humanos. El arma autónoma es aquella que funciona de manera independiente, al identificar un determinado tipo de objetivo[29] (diferente a las armas automáticas que conocemos, que son aquellas armas de fuego que disparan continuamente manteniendo apretado el gatillo).

Actualmente se utilizan **robots** en situación de conflicto, con el objetivo de recopilar información, vigilar, etc. Ejemplo de ello es el robot Samsung SGR-A1: un robot de vigilancia en la frontera entre Corea del Sur y Corea del Norte que es capaz de seleccionar objetivos y emplear fuerza letal sin la intervención de un operario, un humano (en relación también con el artículo 3 DUDH).

Además, existe un peligro real de que se utilicen robots e IA para interrogar a sospechosos. No es una teoría utópica, en el sentido de que actualmente ya se usan polígrafos y escáneres para realizar interrogatorios. Esta tecnología podría usarse con el objetivo de detectar engaños y mentiras y de manipular conversaciones. Si bien podría crearse con la intención de mejorar los interrogatorios, suponiendo que una máquina lo haría mejor que un humano, no se sabe hasta qué punto podría afectar al sospechoso. Es posible que esta tecnología causase angustia al interrogado. A día de hoy la tecnología es usada para interrogar a personas sospechosas.

Además de esto, no podemos perder de vista los ataques armados con drones; los cinturones paralizantes que administran descargas de alto voltaje a través de electrodos situados en los riñones, activándose en muchos casos por control remoto; porras paralizantes que administran potentes descargas eléctricas y no dejan señales físicas duraderas; tortura psicológica con ayuda de IA, entre muchas más que se dirigen a afectar la integridad física o psicológica de las personas.

Evidentemente, muchas de esas tecnologías también podrían utilizarse con fines protectores de derechos y, por tanto, los impactos serían positivos. Así por ejemplo, se podría ayudar a prevenir la tortura al instalarse sistemas de video vigilancia o monitoreo eficaz de las instalaciones donde se llevan a cabo los interrogatorios, detenciones o privaciones de libertad de cualquier tipo. Aunque esto ya se hace y se siguen dando casos de tortura.

29 Véase para más información: https://files.sld.cu/derinthumanitario/files/2016/03/las-armas-autonomas-y-el-dih-dr-c-leonel-gorrin-merida.pdf

Pero en general, drones, satélites, GPS y otras tecnologías podrían y deberían ser utilizados no solo para obtener datos e información, sino también y prioritariamente para detectar vulneraciones de derechos humanos, para rastrear personas, para identificar afectaciones de la integridad personal y, en general, para garantizar que efectivamente la prohibición de la tortura sea un derecho absoluto en todo el mundo.

Artículo 6: derecho a ser reconocido como persona ante la ley

> Todo ser humano tiene derecho, en todas partes, al **reconocimiento de su personalidad jurídica**.

Este es uno de esos derechos en los que las TIC tienen un importante ámbito de influencia. Especialmente, porque se observa cómo en los últimos tiempos se ha producido una digitalización de procesos burocráticos, obligando a las personas usuarias a llevar a cabo trámites de forma telemática. Es el caso del registro de una persona para el reconocimiento de su personalidad jurídica.

El primer problema de esto, en el que insistimos, es que no todo el mundo tiene acceso a internet. Existe un "privilegio digital" en algunas zonas del mundo por las grandes desigualdades existentes en lo que se refiere al acceso a internet (en relación al artículo 2 DUDH). Así, un número importante de impactos positivos de las TIC son materializables solo en algunos países o incluso en algunas regiones de algunos países.

Con motivo de la pandemia Covid19 se ha visto un incremento notable de la creación y establecimiento de procedimientos electrónicos en prácticamente todos los ámbitos. En la práctica eso ha dejado fuera del ejercicio de derechos o limitado ese ejercicio, no solo a personas que no tienen acceso a tecnologías digitales, sino también a personas que, teniendo acceso a estas, son "analfabetas digitales".

Por otra parte, el uso de tecnologías biométricas en el marco de este derecho también presenta aspectos positivos y negativos. En los positivos supone una mayor seguridad para el usuario. El uso de información como la huella dactilar, el reconocimiento facial o de voz, o la lectura del iris facilitan que solo la persona interesada pueda acceder, modificar y hacer uso de esa información, permitiendo así una identificación más segura. Pero tienen también puntos negativos, especialmente en todo lo relativo con el uso que se pueda dar a la información (datos biométricos) y cómo esto podría afectar a la privacidad de las personas usuarias.

Respecto al uso de tecnologías de reconocimiento facial, el Comité contra la Discriminación Racial de la ONU ha expresado su preocupación en cuanto a su uso para rastrear y controlar a determinados grupos demográficos. Expone que resulta inquietante en relación a muchos derechos humanos como el derecho a la intimidad, la libertad de reunión pacífica y de asociación, la libertad de expresión y la libertad de circulación. Estas tecnologías están diseñadas para identificar de forma automática a personas sobre la base de motivos de discriminación como raza, color, origen nacional, étnico o de género,

lo cual permite a los gobiernos mantener registro de los movimientos de las personas sobre objetos de seguimiento basados en discriminación[30].

Como un ejemplo concreto de los impactos de las tecnologías en el ejercicio del derecho a la personalidad jurídica en sí mismo, pero también para el ejercicio de otros derechos, prestaciones y servicios, se puede mencionar el programa que lanzó en 2009 India: *Aadhaar*. Se trata de un sistema que, mediante la cesión de datos biométricos (principalmente la huella dactilar y el escáner del iris), proporciona un ID. El objetivo de este sistema es simplificar el sistema público, pero las críticas apuntan a nuevas barreras (en relación también con el artículo 12).

Este ID se requiere para poder acceder a ayudas económicas estatales, a la seguridad social y, en general, a los servicios públicos. Incluso las empresas privadas empezaron a requerir este ID para contratar un servicio de telefonía o para abrir una cuenta bancaria, por ejemplo. No obstante, la Corte Suprema de la India declaró que las empresas privadas no pueden solicitar el ID como condición para ofrecer sus servicios.

Por lo que se refiere a los servicios públicos, se han observado casos en los que a menores de edad de zonas rurales, que nunca recibieron un certificado de nacimiento, se les ha denegado la solicitud de acceso a escuelas públicas por no poder probar su identidad con el sistema *Aadhaar*. Incluso se han encontrado casos en los que personas enfermas de la lepra no pueden acceder a los servicios públicos porque el escáner de la huella dactilar y del iris son requisitos obligatorios para obtener el ID, que al mismo tiempo es necesario para acceder a los servicios públicos.

Otros de los impactos negativos que pueden tener las tecnologías digitales en el reconocimiento de la personalidad jurídica se vincula con las posibilidades de *hackeo* de firmas electrónicas; de expedientes electrónicos y en el acceso a documentación personal y confidencial; la usurpación de la personalidad, etc.

Sin olvidar por supuesto los impactos positivos como son la disponibilidad de acceso de 24 horas, la firma electrónica que acredita identidad, el acceso desde muchos puntos, incluso desde el domicilio; la facilidad de acreditar la personalidad jurídica en todo tipo de procedimientos frente a las administraciones públicas o prestadores de servicios, etc.

Artículo 7: derecho a la igualdad ante la ley

> Todos son **iguales ante la ley** y tienen, sin distinción, derecho a igual protección de la ley. Todos tienen derecho a igual protección contra toda discriminación que infrinja esta Declaración y contra toda provocación a tal discriminación.

30 Véase: Recomendación General No. 36 (2020), relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden, Comité contra la Discriminación Racial, párr. 35.

Artículo 10: derecho a un juicio justo

> Toda persona tiene derecho, en condiciones de plena igualdad, a **ser oída públicamente y con justicia por un tribunal independiente e imparcial**, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación contra ella en materia penal.

Artículo 8: derecho de acceso a la justicia y a la reparación

> Toda persona tiene derecho a un **recurso efectivo ante los tribunales nacionales**, competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la constitución o por la ley.

Artículo 11: derecho a la presunción de inocencia

> **1.** Toda persona acusada de delito tiene derecho a que se **presuma su inocencia** mientras no se pruebe su culpabilidad, conforme a la ley y en juicio público en el que se le hayan asegurado todas las garantías necesarias para su defensa.
>
> **2. Nadie será condenado por actos u omisiones que en el momento de cometerse no fueron delictivos** según el Derecho nacional o internacional. Tampoco se impondrá pena más grave que la aplicable en el momento de la comisión del delito.

Por la estrecha relación que hay entre todos los artículos antes citados, preferimos desarrollarlos de manera conjunta por ahora. Esto no significa que no requieran un análisis pormenorizado cada uno, sino tan solo que nos parece que en este momento es más fácil y mejor mostrar cómo algunas tecnologías impactan en positivo y negativo en todos estos derechos.

El uso de la IA en los sistemas judiciales está siendo explorado por los poderes judiciales, los servicios de fiscalía y otros órganos judiciales de dominios específicos en todo el mundo. Por ejemplo, en el campo de la justicia penal, el uso de sistemas de la IA para brindar asistencia en los procesos de investigación y automatizar los procesos de toma de decisiones ya está implementado en muchos sistemas judiciales a nivel global.

Así, un aspecto transversal que se presenta como riesgo a la igual protección de la ley, al acceso a la justicia, a la presunción de inocencia y del acceso a un recurso efectivo tiene que ver con la "**automatización de decisiones**", o en este caso, la asistencia en la toma de decisiones de los tribunales mediante el

uso de IA. Esta herramienta consiste en el uso de **algoritmos** que asisten a los jueces para, por ejemplo, determinar el fallo de una sentencia. Una de estas es la que recibe el nombre de *risk assessment tool*.

Esta herramienta se nutre de datos que provienen de historiales policiales, del perfil del acusado, etc., y le atribuyen a este un número, el cual estima la probabilidad de reincidencia de ese individuo. Conforme el número es más elevado, debe entenderse que hay un mayor riesgo de reincidencia. Los jueces tienen en cuenta estas puntuaciones en el momento de tomar decisiones que se refieren a, por ejemplo: qué servicios en forma de rehabilitación deben recibir; si es necesario que permanezcan en régimen de prisión preventiva a la espera del juicio; y qué tan severa es la condena (refiriéndose, mayoritariamente, a los años de condena).

Podría entenderse, en un primer plano, que esta herramienta permite objetivizar el proceso. Sin embargo, se trata de una falacia, puesto que la información en la que se basa y mediante la cual establece probabilidades estadísticas presenta dos problemas:

- La información que se introduce ha sido elaborada por una persona. Por tanto, está contaminada de sus sesgos y puede resultar discriminatoria. Esto es, se estaría "educando" a una máquina con unas bases discriminatorias que derivarían en decisiones discriminatorias.

- Además, teniendo en cuenta que los algoritmos usan estadísticas para encontrar patrones en los datos, se estarían obteniendo correlaciones, que no causalidades. Por lo que las conclusiones a las que llegaría el algoritmo pueden ser erróneas. Por ejemplo, si el algoritmo observa que bajos ingresos se correlaciona con una alta reincidencia, ello no significa que sea una causalidad[31]. Para ponerlo de forma simple y ejemplificarlo: cuando las personas que compran bebidas azucaradas tienden a tener malos hábitos alimenticios (correlación), pero ello no significa que comprar bebidas azucaradas provoque malos hábitos alimenticios (causalidad)[32].

Hay docenas de estos algoritmos de evaluación de riesgos en uso. Desde una organización llamada ProPublica[33], por ejemplo, analizaron una herramienta de la empresa Northpointe, llamada COMPAS (que significa Perfiles de Gestión de Delincuentes Correccionales para Sanciones Alternativas), y encontraron que los acusados negros eran mucho más propensos que los acusados blancos a ser juzgados incorrectamente como "en mayor riesgo de reincidencia", mientras que los acusados blancos tenían más probabilidad que los acusados negros de ser marcados incorrectamente como "de bajo riesgo".

En Cataluña se aplica actualmente un sistema similar, llamado *Riscanvi*. Este mide el riesgo de reincidencia de los internos y se ha observado que tiene un importante peso en las decisiones judiciales. En los últimos tiempos han surgido dudas respecto su "fiabilidad" por su alta tasa de "falsos positivos"[34].

31 Véase para más información: https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/

32 Véase: Soriano Arnanz, Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos, *Revista de Derecho Público: Teoría y Método*, Vol. 3 (2021), pp. 85-127.

33 Véase para más información: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

34 Véase, para más información: https://www.lavanguardia.com/encatala/20211206/7911583/algoritme-imprecis-condiciona-llibertat-dels-presos.html

Los sistemas de decisión automatizados, que pueden basarse en la correlación entre conjuntos de datos y consideraciones de eficiencia, pueden depender de estas variables para generar resultados que perpetúan o exacerban los patrones de sesgo y discriminación. Este tipo de discriminación puede ser difícil de corregir, o incluso de detectar, si solo se valora el resultado algorítmico[35].

Como se observa, el uso de la IA plantea una amplia gama de desafíos que deben abordarse: desde el reconocimiento de patrones hasta la ética, las decisiones sesgadas tomadas por algoritmos basados en la IA, la transparencia y la rendición de cuentas. Los algoritmos de autoaprendizaje, como vemos, pueden ser entrenados por ciertos conjuntos de datos (decisiones previas, imágenes faciales o bases de datos de videos, etc.) que podrían contener datos sesgados con el potencial de ser utilizados por aplicaciones con fines criminales o de seguridad pública, lo que lleva a decisiones sesgadas.

El Comité para la Eliminación de la Discriminación Racial de la ONU se ha pronunciado en reiteradas ocasiones acerca de la **elaboración de perfiles raciales** por parte de los Estados, utilizados a fin de reforzar la seguridad o los sistemas judiciales. En su Recomendación General número 30 (2004), sobre la discriminación contra las personas no ciudadanas, recomienda que los Estados velen por que las medidas que se tomen en la lucha contra el terrorismo no discriminen, por sus fines o efectos, por motivos de raza, color, ascendencia u origen nacional o étnico, y que las personas no ciudadanas no se vieran sometidos a las caracterizaciones o estereotipos raciales o étnicos (párr. 10).

En su Recomendación General número 31 (2005), sobre la prevención de la discriminación racial en la administración y el funcionamiento de la justicia penal, recomienda a los Estados partes que adopten las medidas necesarias para impedir los interrogatorios, las detenciones y los cacheos basados de facto exclusivamente en el aspecto físico del individuo, su color, sus rasgos faciales, su pertenencia a un grupo racial o étnico, o cualquier otra categorización que pudiera hacerle particularmente sospechoso (párr. 20).

En este orden, dicho Comité en su recomendación número 36 (2020) analiza particularmente la elaboración algorítmica de perfiles raciales, reconociendo que debido al desarrollo tecnológico, las actividades de los agentes del orden están cada vez más determinadas por la elaboración algorítmica de perfiles. Aunque estos avances pueden aumentar la eficiencia de estos agentes, el Comité reconoce el grave riesgo de que reproduzcan y refuercen prejuicios y prácticas discriminatorias. Entiende que, al emplear métodos de IA, los resultados discriminatorios pueden ser más difíciles de detectar que en aquellos casos en que se derivan de decisiones humanas (párrafos 31 y 32).

El Comité menciona el ejemplo del uso de algoritmos para detectar la probabilidad de que se produzcan ciertas actividades delictivas en determinadas localidades. Por ejemplo, los datos históricos de detenciones en un barrio pueden reflejar prácticas policiales con sesgo racial. El uso de estos datos puede provocar que las predicciones futuras vayan en la misma dirección sesgada, provocando mayor vigilancia en determinada zona y hasta más detenciones. De igual manera, pone el ejemplo de mecanismos similares utilizados en sistemas judiciales. Es así que se recurre cada vez más a estos sistemas predictivos a los fines de prever si un individuo cometerá uno o varios delitos en el futuro. Para ello,

35 Véase para más información: https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf

se recopila información sobre el historial delictivo del individuo, su familia y amigos, sus condiciones sociales, su historial laboral y académico, etc. y se evalúa su "grado de peligrosidad" (párrafos 33 y 34).

Finalmente, por ahora, no podemos olvidar el problema que se repite en la mayoría de derechos con la falta de acceso a las tecnologías digitales y de la información por toda persona, solo algunas gozan del "privilegio digital". No todos tenemos el mismo acceso a internet ni disponemos de dispositivos tecnológicos. En el caso de que las fases de un proceso en cualquier materia (interponer una demanda, aportar pruebas, celebrar una audiencia, etc.), si estos se deben desarrollar de forma telemática, la falta de acceso estaría repercutiendo en aquellas personas que no tienen acceso a estas tecnologías, por lo que se estaría afectando a un sector de población que muy probablemente ya es previamente vulnerable o que no tenía acceso efectivo a la justicia.

Artículo 9: derecho a ser libre de detención arbitraria

> Nadie podrá ser **arbitrariamente detenido**, preso ni desterrado.

Estrechamente relacionado con todo lo anterior, encontramos también el uso de **IA, *machine learning, data*, algoritmos** con el objetivo de analizar los datos introducidos para prevenir la comisión de delitos. Esta tecnología recibe el nombre de *predictive policing*, y se basa en la localización o ubicación (*location-based*) y en las personas (*person-based*).

Mientras que en el caso de *location-based*, el algoritmo identifica los lugares donde se repite la comisión de delitos para predecir dónde se van a cometer en un futuro, la *person-based* tiene como objetivo identificar quién podría cometer un delito. En ambos casos, la información introducida proviene de historiales policiales, información sobre créditos, historiales médicos, etc. Se ha demostrado que estos sistemas codifican **racismo sistémico**, afectando negativamente a comunidades ya marginalizadas o en situación de vulnerabilidad[36].

Esta tecnología, la *predictive policing*, utiliza sistemas informáticos para analizar grandes conjuntos de datos con el objetivo de decidir dónde se deben realizar las patrullas o para identificar a las personas que presuntamente son propensas a cometer o ser víctimas de un delito.

La *predictive policing* presenta unos cuantos problemas[37]. El primero hace referencia a la poca transparencia y a la necesidad de establecer un sistema para la rendición de cuentas. La falta de transparencia se refiere tanto al tipo de datos que se analizan como a la forma en que los departamentos (policiales) usan las predicciones elaboradas por esta tecnología. Además, también hay escasez de información respecto a cómo se utilizan en última instancia estas predicciones. Para intentar solucionar este pro-

36 Véase para más información: https://epic.org/ai/criminal-justice/index.html

37 Véase para más información: https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

blema sería interesante elaborar un registro de autoría sobre quiénes crean o quiénes acceden a las predicciones y, por otra parte, un sistema de auditoría que permita verificar el sistema y buscar, si existen, sesgos para poder eliminarlos. Del mismo modo, sería interesante determinar cómo proceder, en términos de responsabilidad, cuando se usan estos sistemas y se pone en evidencia que perjudican a determinadas personas por motivos discriminatorios.

El segundo problema afectaría a la "sospecha razonable". Se trata de una norma cuyo objetivo es proteger a las personas contra posibles registros e incautaciones irrazonables y/o arbitrarias. Las herramientas de análisis predictivo pueden facilitar a la policía la afirmación de que se cumplen los estándares de sospecha razonable. La cuestión es qué tanto objetivas son las predicciones si se basan en información (datos policiales históricos) que presenta sesgos y discriminaciones raciales.

Además de lo anterior, en este derecho se repiten los mismos problemas que en el artículo 5 *supra*, por lo que se refiere a la instalación de sistema de video vigilancia para realizar un control; y al uso de nuevas tecnologías en la detención o encarcelamiento. Al igual que el uso de tecnologías biométricas para identificar a las personas y justificar con ello su detención, a pesar de los márgenes de error y sesgos que dichas tecnologías presentan.

Evidentemente, vinculado con este derecho también se podrían dar impactos negativos cuando la IA es utilizada para patrullar determinadas zonas geográficas, reforzar presencia policial, perseguir a determinados grupos sociales, etc., sin que exista sospecha razonable, sino simplemente información obtenida a partir de la recolección de datos e información que ha sido procesada por algoritmos.

No hay duda de que todo lo que se ha señalado como ejemplo en este artículo y respecto a los derechos analizados en el bloque anterior podría ser usado también en sentido positivo para reducir arbitrariedades, sumar a la imparcialidad e independencia de jueces, reducir los márgenes de discrecionalidad en las actuaciones policiales, evitar actos discriminatorios en la aplicación de la ley y, por qué no, permitir un mayor y más eficiente acceso a la justicia. Sin embargo, todo parece indicar que eso solo será posible en la medida en que no se deje toda la decisión a la IA, sino que sea tan solo un auxiliar que ayude a agilizar procedimientos e información, dejando la decisión final a las personas que, igualmente pueden tener sesgos, pero también tienen la oportunidad de valorar más aspectos que una máquina difícilmente podrá considerar.

Artículo 12: derecho a la privacidad y a la vida privada

> Nadie será objeto de **injerencias arbitrarias en su vida privada**, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Uno de los derechos que está en el centro del uso de las tecnologías de la información y, especialmente, de la IA y sus algoritmos, es la vida privada. Como ya se ha estableciendo antes, es uno de los derechos que, incluso sin darnos cuenta, podría recibir impactos negativos. Por ejemplo, cuando aceptamos o autorizamos sin leer que se acceda a datos e información privada.

De igual forma, en los últimos meses, con tanta videoconferencia desde casa, hemos abierto nuestro domicilio, como antes ya lo estaba parte importante de nuestra correspondencia electrónica y otra información personalísima que tenemos almacenada, compartimos o introducimos en aplicaciones, correos electrónicos, formularios, etc.

Pero no solo eso, como también se ha visto antes, el acoso y los ataques a la honra y la reputación de las personas, de todas las edades, también se han hecho de mayor alcance con el uso de tecnologías de la información como las redes sociales.

Ejemplos de esto hay muchos. Es más, ante la falta de transparencia con la que funcionan actualmente muchas aplicaciones de IA, casi se puede afirmar que la mayoría están incidiendo en nuestra vida privada, sin darnos cuenta, con simplemente tener la capacidad de conocer nuestros gustos musicales, los lugares en donde nos conectamos a internet, nuestras preferencias sexuales e identidad de género, el lugar al que iremos en nuestras próximas vacaciones, las personas con las que nos relacionamos, etc.

Así, un ejemplo interesante ha ocurrido en Países Bajos, donde desde 2014, se venía utilizando un algoritmo, llamado *System Risk Indication* o **SyRI**, por sus siglas en inglés[38]. Esta tecnología se creó con la voluntad de detectar casos de fraude. Para ello, se utilizan bases de datos que se crearon con referencias cruzadas de datos personales de la ciudadanía. Si alguna agencia gubernamental sospecha de fraude en algún barrio en concreto, se puede acceder al programa y este, con base en la información de que dispone, señalará a las personas de ese barrio que necesitan ser investigadas con mayor detalle.

La información de que dispone este algoritmo es amplia y diversa: datos laborales, penales, tributarios, información sobre propiedades, educación, jubilación, deudas, beneficios, subsidios, permisos de que se dispone o han sido solicitados, exenciones, etc.

Tienen acceso a este algoritmo funcionarios de la seguridad social, inspectores del Ministerio de Asuntos Sociales y Empleo, autoridades tributarias, etc. Evidentemente, ha recibido cuestionamientos debido a que no existe transparencia. Las personas no saben qué sucede con sus datos. También, porque los vecindarios a los que se les aplica esta tecnología no son avisados en la mayoría de casos. Además, organizaciones de la sociedad civil alegan que SyRI se emplea, mayoritariamente, para investigar barrios humildes y con bajos ingresos[39]. Este hecho agrava los sesgos, prejuicios y discriminaciones preexistentes. Si esta tecnología solo se usa para analizar barrios de este perfil, obviamente va a encontrar allí más ciudadanos de "riesgo".

Diferentes organizaciones presentaron una demanda en contra de SyRI. El 5 de febrero de 2020, un tribunal holandés de La Haya ordenó el cese inmediato de SyRI porque en su consideración viola el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH), que protege el derecho al respeto de

38 Véase para más información: https://algorithmwatch.org/en/syri-netherlands-algorithm/, así como: https://www.privacyfirst.eu/court-cases/tag/System%20Risk%20Indication.html y https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf

39 Véase para más información: https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html

la vida privada y familiar. Para ello argumentó que la legislación no es lo suficientemente transparente y verificable, y que no hay suficientes salvaguardias contra las intrusiones a la privacidad[40].

Este ejemplo es muestra clara de dos cosas: la primera, que hay muchas aplicaciones de la IA que están incidiendo en nuestra vida privada, que además tienen el mismo problema que SyRI, no son transparentes ni verificables. La segunda, que los tribunales sí cuentan con herramientas jurídicas para actuar y poner freno a este tipo de aplicaciones, pues el CEDH es de 1950, no es una norma nueva que muchas veces se pide para actuar en casos como este.

Otro ejemplo respecto al cual se debe poner atención por los impactos que puede tener en la vida privada, lo tenemos con **Clearview**, una aplicación [de reconocimiento facial] que, facilitándole una imagen de cualquier persona, muestra todas las fotografías e información publicada en internet de esa misma persona. Incluso se habla de vincular esta tecnología con gafas de realidad aumentada, de modo que cualquier persona que las esté utilizando, al ir por la calle, pueda identificar a todas las personas con las que se cruce[41].

Uno más es el ***Metaverse*** o **Metaverso**: esto es, entornos digitales donde los humanos interactúan social y económicamente como avatares. Funcionan como una metáfora del mundo real, pero sin las limitaciones físicas o económicas allí impuestas. Existe hace ya varios años pero, recientemente, Mark Zuckerberg, CEO de Facebook, ha anunciado que su empresa comenzará a desarrollar la tecnología *metaverse*, con el fin de que en un futuro cercano las personas puedan encontrarse masivamente en un mundo virtual inmersivo. Es evidente que esta realidad virtual potenciará todos los aspectos conflictivos que caracterizan a las redes sociales: la manipulación de los datos personales de las personas usuarias, la seguridad e integridad de los mismos (especialmente cuando se trata de niños, niñas y adolescentes) y la cuestión de la discriminación impregnada en el diseño y origen mismo de estos sistemas.

En relación a la **niñez y la protección de la privacidad**, el Comité de Derechos del Niño de Naciones Unidas ha resaltado que el entorno digital puede plantear problemas particulares a los padres y cuidadores a la hora de respetar el derecho a la privacidad de niñas y niños. Las tecnologías que controlan las actividades en línea con fines de seguridad, como los dispositivos y servicios de rastreo, si no se aplican con cuidado, pueden impedir que un niño acceda a una línea de asistencia digital o busque información delicada.

Además, niños y niñas suelen utilizar avatares o seudónimos en línea para proteger su identidad, prácticas que el Comité considera importantes para proteger su privacidad. El Comité aconseja a los Estados delinear la vigilancia de la actividad digital de niñas y niños, la cual debe ser proporcionada y acorde con la evolución de las facultades de niños y niñas. A su vez, debe garantizar la debida seguridad a fin de evitar que las prácticas anónimas sean utilizadas como medio para ocultar comportamientos nocivos o ilegales, como la ciberagresión, el discurso de odio o la explotación y los abusos sexuales[42].

40 Véase para más información: https://algorithmwatch.org/en/syri-netherlands-algorithm/

41 Véase para más información: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

42 Véase: Observación General No. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital, Comité de los Derechos del Niño, 02/03/2021.

Si miramos a nuestro alrededor, especialmente en una ciudad, en una oficina, incluso en nuestro bolsillo, nuestra mano o las aplicaciones que hemos descargado en nuestro teléfono móvil, podemos tener un poco de conciencia respecto a qué tanto estamos abriendo nuestra privacidad a "alguien" o a "algo".

Es un hecho que la inteligencia artificial está invadiendo nuestras vidas en todas sus facetas: **wearables** (ropa con tecnología incorporada para conectarse al móvil, controlar la temperatura corporal, medir nuestra frecuencia cardiaca, etc); **smartwatchs** (relojes inteligentes que sirven como teléfono, reproductor de música, controlador de constantes vitales, videojuegos, monederos, etc); ***chatbots*** (*software* capaz de mantener una conversación con una persona para hacer una reserva, realizar trámites, pagar multas, recibir quejas o instrucciones, etc.); **sensores** y **cámaras** que permiten el reconocimiento de matrículas de vehículos en gasolineras y aparcamientos, pero también de personas en espacios públicos (calles, plazas, estaciones de metro, aeropuertos, etc.) o privados (centros de trabajo, gimnasios, clubes sociales, bancos, etc.); **aplicaciones de teléfono** o **tableta** (para reservar en un restaurant, para conocer personas, para encontrar pareja, para vender cosas, para subir fotografías, para expresar ideas, para subir vídeos, para seguir rutinas de ejercicio o alimentación, etc.); entre otras tantas más. Parece claro que mucha de nuestra información personal que, en ocasiones, no conoce ni siquiera nuestra familia o personas cercanas o incluso nosotras mismas, está a disposición de quienes han desarrollado los algoritmos por los que funcionan todas esas aplicaciones de IA.

Si vemos, muchas de esas aplicaciones sirven a su vez para el ejercicio de muchos otros derechos y libertades que aquí se analizan, pero como ya lo decíamos desde el estudio introductorio, no solo impactan en aquellos derechos y libertades, sino también en la privacidad, por la forma en la que se nos obliga a seguir para poder hacer uso de todo lo antes señalado como ejemplo.

Es evidente que toda esa tecnología podría tener un impacto positivo en la vida privada, en tanto que nos permite en muchos casos conocer y sistematizar información personal que de otra forma no podríamos tener. Pero, mientras no haya transparencia total respecto al diseño, destino, almacenamiento, uso y características específicas de los datos e información que se recoge de nosotras, aunque demos autorización, los impactos negativos siempre serán lo primero que se observará por el simple hecho de la incertidumbre que genera el no saber quién está detrás y para qué quiere no solo saber tanto de nosotras, sino tener registro detallado de todo eso que conoce.

Artículo 13: derecho a la libertad de movimiento, residencia y circulación

1. Toda persona tiene derecho a **circular libremente** y a elegir su residencia en el territorio de un Estado.

2. Toda persona tiene derecho a salir de cualquier país, incluso del propio, y a regresar a su país.

Artículo 14: derecho a buscar asilo

> **1.** En caso de persecución, toda persona tiene derecho a **buscar asilo**, y a disfrutar de él, en cualquier país.
>
> **2.** Este derecho no podrá ser invocado contra una acción judicial realmente originada por delitos comunes o por actos opuestos a los propósitos y principios de las Naciones Unidas.

Si se piensa en que por medio de procedimientos telemáticos o digitales se podría facilitar, agilizar o automatizar la solicitud de protección internacional, asilo o refugio, así como de visados o autorizaciones para ingresar en los países o registrarse en los censos de población del país en el que se reside, sin duda que eso podría ser un impacto positivo en muchos casos, especialmente porque podría agilizar procedimientos o permitir que toda persona pudiese presentar esas solicitudes.

Sin embargo, el primer punto en contra que se puede tener y en el que hay que pensar siempre, es si efectivamente las personas a las que se dirige esa posibilidad tendrán acceso a internet, computadoras o dispositivos con los requerimientos técnicos necesarios que les permitan presentar la solicitud. De lo contrario, muy posiblemente solo volverán a tener acceso las personas que desde antes ya tenían la posibilidad de hacerlo al contar con recursos para trasladarse físicamente a los lugares en los que se deben presentar o pagar los servicios de quien se los gestione. Tampoco podemos olvidar la importancia que deberá ponerse en la forma en la cual se diseñan esos procedimientos, a fin de evitar que sean discriminatorios a partir de la información que recogen.

Un ejemplo claro de esto se puede observar en Canadá, donde desde 2014, se ha ido introduciendo la tecnología de automatización de toma de decisiones en el marco de los mecanismos de migración, sobre todo por lo que se refiere a funciones llevadas a cabo por administrativos y para dar soporte a la evaluación y decisión de concesión de permisos. Estas funciones se refieren, por ejemplo, a observar si una solicitud está completa, si un matrimonio es "genuino" y no de conveniencia, si una persona en particular debería ser considerada "de riesgo", etc.[43].

Muy vinculada con lo anterior, también tienen la aplicación *Pre-Removal Risk Assessment*, la cual "permite" obtener los riesgos (de tortura y demás dificultades y riesgos) que una persona corre en caso de ser expulsada de Canadá[44].

En Nueva Zelanda, está en funcionamiento también el uso de tecnología que se basa en la edad, sexo y etnia para identificar a personas que puedan suponer un riesgo. Se usa para identificar aquellas personas que pueden suponer un elevado coste hospitalario, que sean más propensas a cometer delitos,

43 Véase para más información: https://citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/

44 Véase para más información: https://www.cbc.ca/radio/sunday/november-18-2018-the-sunday-edition-1.4907270/how-artificial-intelligence-could-change-canada-s-immigration-and-refugee-system-1.4908587

etc., de forma que la institución encargada de migración puede actuar con mayor eficacia, deportando a estas personas, negándose a concederles el visado o no permitiéndoles volver a solicitar visas. Por lo que se estaría actuando en base a estadísticas formuladas por un algoritmo[45].

Un ejemplo más es el *iBorderCtrl* o *Intelligent Portable Control System*. Se trata de un sistema de seguridad de fronteras automatizado (se encontraba en fase de prueba en 2020). Está diseñado para que las personas que no son nacionales de ningún país de la UE, antes de salir del país de origen, se registren y proporcionen información sobre su viaje. Con ello "se acepta" ceder información detallada (por ejemplo, de las redes sociales). Además, los agentes de frontera podrían solicitar a los viajeros que, mediante un dispositivo tecnológico y con la cámara encendida, se sometan a un "interrogatorio", realizado por un avatar (inteligencia artificial), en la que no solo recogerá la información que se facilite sino que, además, hará un estudio de los gestos con el objetivo de detectar si le están mintiendo y si esa persona supone o no un riesgo. Lo que puede interpretarse como un método intrusivo. Por último, una vez se llega al país de destino, se recogerían un conjunto de datos biométricos.

Este proyecto, que no había entrado en funcionamiento en 2021, es sin duda un ejemplo de "desarrollos" tecnológicos para el control migratorio que deben ser observados, transparentados y seguidos muy a detalle. Especialmente porque como está planteado, parecería no solo una injerencia arbitraria en la vida privada, sino que también implicaría una restricción a la libertad de circulación (artículo 13 de la DUDH) puesto que, de negarse a ceder esta información, la persona no se encontrará habilitada ya no solo a cruzar la frontera, sino ni siquiera a iniciar su viaje.

Además de eso, también se está dando el uso de tecnologías biométricas por parte de Estados para elaborar bases de datos biométricos de los no nacionales. Esta información les ayuda a elegir si conceden o no permisos y, además, pueden usarla con el objetivo de crear nuevas leyes en materia de inmigración, refugio y asilo. Por tanto, el uso que se dé a esta tecnología y a la información recopilada mediante esta, depende de la voluntad de los Estados[46].

Es el caso, por ejemplo, de Canadá, que usa el reconocimiento de voz para identificar a aquellas personas que pretenden entrar en el país y que, manifiestamente, pueden suponer un potencial riesgo para la seguridad de este[47].

También Alemania[48] emplea el uso de tecnologías biométricas. Es el caso del reconocimiento de voz con el objetivo de identificar el origen de migrantes que no lleven documentación y (caso muy concreto) de evitar que se alegue ser de algún país o lugar para pedir asilo cuando realmente no se es de ahí[49].

45 Véase para más información: https://www.nzherald.co.nz/nz/immigration-nzs-data-profiling-illegal-critics-say/P5QDBGVDGFSI6I3NV4UHPOSBRA/ y https://www.zdnet.com/article/nz-to-perform-urgent-algorithm-stocktake-fearing-data-misuse-within-government/

46 Véase para más información: https://iow.eui.eu/wp-content/uploads/sites/18/2013/04/07-Rijpma-Background4-Refugees-and-Biometrics.pdf

47 Véase para más información: https://findbiometrics.com/canadian-authorities-refugees-voice-recognition-507261/

48 Véase para más información: https://www.bbc.com/news/world-europe-39307155

49 Véase para más información: https://www.dw.com/en/german-refugee-agency-unveils-new-asylum-identity-technology/a-39857345

Quienes justifican el uso de estas tecnologías alegan que permiten tomar decisiones relativas al asilo con mayor celeridad.

El problema que estas tecnologías plantean gira en torno a lo que en el artículo anterior señalábamos: la privacidad, el uso que se da a los datos biométricos recogidos (*data*), a la confidencialidad, el tiempo que esta información se mantiene disponible en el sistema. Otra cuestión es qué tan fiable y de qué calidad son los *softwares* que se usan para estas tecnologías.

Además, también preocupa la divulgación que pueda hacerse de la información biométrica obtenida, el riesgo de robo o uso indebido de esta. Y, también, el margen de error de estas tecnologías y el riesgo que ello puede suponer para las personas afectadas, esto es, migrantes en busca de asilo y refugiadas.

También supone un problema que los migrantes se vean obligados a ceder esta información o ser sometidos a estas tecnologías. Esto es, que no se les presente ninguna alternativa, por lo que si no la ceden no pueden solicitar asilo o refugio. Ello pone en duda el consentimiento de los afectados (hasta qué punto es un consentimiento pleno, libre e informado).

Como se está viendo hasta ahora, estas tecnologías pueden contener sesgos e información discriminatoria[50]. Los críticos con estas tecnologías y su uso en las fronteras y sistemas de inmigración, refugio y asilo comentan que ello puede derivar en una menor movilidad. Además, podría estar facilitando una mayor vigilancia por parte de los gobiernos. Finalmente, si las "fronteras digitales" se intensifican y refuerzan cada vez más, haciendo más difícil cruzarlas, ello puede derivar en que los viajes sean más costosos y peligrosos.

Pero estos sistemas no solo están siendo aplicados y desarrollados por los Estados. ACNUR ofrece un carnet de refugiado (ID UNCHCR[51]), mediante el cual se puede acceder a distintas ayudas. Los problemas que ello plantea giran en torno a la privacidad y el consentimiento[52]. Para que se conceda este carnet es necesario ceder cierta información y someterse a determinadas tecnologías biométricas (escaneo de iris, huella dactilar, historiales personales y familiares, de salud, documentación legal, etc.).

Uno de los problemas que plantea es si las personas refugiadas pueden prestar consentimiento para la recopilación y uso de sus datos biométricos de forma plena, libre e informada. Si bien es cierto que, teóricamente, pueden negarse a un escaneo biométrico, ello les niega la concesión del carnet y el acceso a las ayudas. Además, estudios han demostrado que los interesados no están suficiente ni correctamente informados, en el sentido de que no se les explica detalladamente cómo, a quién y con qué propósito se comparten sus datos biométricos.

50 Véase para más información: http://aei.pitt.edu/103233/1/IB_MSG_AI_Digital_Identities_Biometrics_Blockchain_2020.pdf

51 https://hir.harvard.edu/new-technologies-that-monitor-displaced-persons/

52 https://iow.eui.eu/wp-content/uploads/sites/18/2013/04/07-Rijpma-Background4-Refugees-and-Biometrics.pdf, https://www.cigionline.org/sites/default/files/documents/WRC%20Research%20Paper%20no.12.pdf (en este se recoge qué información y qué datos biométricos deben cederse). https://assets.publishing.service.gov.uk/media/5cecedd6ed915d2475aca8c5/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf y https://digitalid.theengineroom.org/assets/pdfs/200128_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive_Edit1.pdf

Del mismo modo, las tecnologías empleadas para obtener los datos biométricos son, en determinados casos, discriminatorias. Por ejemplo, el escáner de la huella dactilar tiene más dificultad en leer aquellas de personas negras o que se dedican a trabajos manuales, lo que les hace más propensos a tener problemas con falsos negativos, entradas dobles, impidiéndoles recibir asistencia.

Se observa, pues, que el uso de tecnologías como las que se acaban de mencionar puede servir para agilizar procedimientos, pero también para fortificar las fronteras o establecer nuevas fronteras digitales mucho más allá de las fronteras territoriales. Con lo que el uso de estas puede suponer limitaciones a la libre circulación y a la búsqueda de asilo o refugio.

Finalmente, para mostrar algunos impactos positivos en estos derechos, al menos en cuanto a los usos de las tecnologías, sin entrar en sus detalles de diseño, se puede mencionar en este ámbitos el proyecto *Karim the Chatbot X2AI* que ofrece psicoterapia virtual a personas refugiadas que se encuentran en el denominado campo de refugiados situado en Zaatri; el *Free Robot Lawyers* que ofrece asistencia legal a personas migrantes y refugiadas; el REFUNITE que ayuda a las personas refugiadas a buscar familiares desparecidos o de los que no tienen noticias o la aplicación *PareuDePararme* que ha desarrollado SOS Racismo Cataluña para registrar los casos y lugares en los que se presentan identificaciones por perfil racial en la ciudad de Barcelona. Con lo que, usos en beneficio de las personas migrantes extranjeras sí que se les pueden dar a las tecnologías, aunque por desgracia la tendencia más general, organizada y desarrollada va en el sentido de limitar o impedir el ejercicio del derecho de libre circulación, residencia y asilo.

Artículo 15: derecho a la nacionalidad

> **1.** Toda persona tiene **derecho a una nacionalidad**.
>
> **2.** A nadie se privará arbitrariamente de su nacionalidad ni del derecho a cambiar de nacionalidad.

En este derecho se observan muchas situaciones similares a las desarrolladas en el análisis anterior, en la medida de que muchos procedimientos migratorios y de la obtención de la nacionalidad siguen vías similares, incluso cuando se ha nacido en el país del que se pide el reconocimiento de nacionalidad.

Esto se observa especialmente porque en los últimos tiempos se ha producido una digitalización de procesos burocráticos, obligando a las personas usuarias a llevar a cabo trámites de forma telemática. Es el caso del registro de nacionalidad y todas las demás gestiones que deseen hacerse en relación a esta. El problema es que no todo el mundo tiene acceso a internet. Existe una brecha digital, una realidad de desigualdades por lo que se refiere al acceso a internet (en relación al artículo 2 DUDH).

Un impacto negativo adicional está en procesos de automatización en los que la persona solicitante no tiene contacto nunca con una persona funcionaria, sino que todo se desarrolla por medios electrónicos y con interacción con estos.

Eso se vuelve problemático por dos razones. La primera es que en procedimientos en los que se exige la demostración de algún tipo de conocimientos o dominio de un idioma, si la aplicación de los exámenes es de igual forma telemática, se pueden recoger datos de la persona que vayan más allá del examen mismo, como lo hemos visto con los procedimientos migratorios desarrollados en el artículo anterior. La segunda es que no siempre son claros los requisitos que se solicitan, por lo que en caso de duda solo queda esperar a que la aplicación tenga por admitida la documentación e información que se solicite, generando que todo el procedimiento se desarrolle sin tener certeza de que se está haciendo de manera correcta. Además de que, en general, en estos procedimientos el único medio de comunicación con una persona humana es por medio de correos electrónicos o formularios previstos en las mismas aplicaciones, con lo que la respuesta ante las dudas, quejas o inconformidades, difícilmente será atendida de manera breve y eficaz.

Así, en estos procedimientos como en otros que antes se han analizado, parece importante señalar que la IA solo debe ser utilizada para simplificar procedimientos, facilitar el ejercicio de derechos y libertades o agilizar la toma de decisiones, pero la decisión final debe ser tomada siempre por un ser humano y, en todo caso, debe hacerlo sin discriminación o sin considerar información que discrimine a las personas solicitantes.

Artículo 16: derecho al matrimonio y a fundar una familia

> **1.** Los hombres y las mujeres, a partir de la edad núbil, tienen derecho, sin restricción alguna por motivos de raza, nacionalidad o religión, a **casarse y fundar una familia**, y disfrutarán de iguales derechos en cuanto al matrimonio, durante el matrimonio y en caso de disolución del matrimonio.
>
> **2.** Solo mediante libre y pleno consentimiento de los futuros esposos podrá contraerse el matrimonio.
>
> **3.** La familia es el elemento natural y fundamental de la sociedad y tiene derecho a la protección de la sociedad y del Estado.

En este derecho volvemos a ver un importante impacto de las **TIC**, concretamente de las **redes sociales**. Más allá de las cuestiones relativas a la privacidad y al consentimiento pleno, libre e informado, tienen mucho que ver aquí con la forma en la que las personas estamos relacionándonos, conociéndonos e interactuando. Si bien es cierto que, en muchos aspectos, ha permitido la conexión de personas que se encuentran en lugares del mundo distantes entre sí, también está la posibilidad de que algunas aplicaciones solo nos estén dando la posibilidad de interactuar con personas que tienen un perfil determinado, ya no solo por nuestras preferencias, sino por lo que un algoritmo considera, de acuerdo a como fue programado, que es lo que estamos buscando para cualquier tipo de relación familiar.

Pero no solo eso, también hay situaciones que nos deben alarmar, como la ocurrida en 2018, a la que hicimos referencia antes, en la que un padre hizo una publicación en Facebook poniendo a subasta a su

hija menor de edad, de 17 años, para que contrajese matrimonio con el mejor postor (matrimonio forzado). El post no fue retirado hasta días después de su publicación, cuando la menor ya había sido "vendida"[53].

Con estos ejemplos, parece mostrarse de manera clara que el mayor impacto negativo en el ejercicio de este derecho está en la posibilidad de que no en todos los casos haya un libre y pleno consentimiento, y ya no por el hecho de aceptar una relación personal, sino desde antes por las posibilidades que un algoritmo nos dé para conocer personas, con lo que ya se estaría limitando esa libertad indirecta o inconscientemente.

Si preferimos quedarnos con la parte positiva, sin duda se debe valorar la posibilidad que dan las tecnologías de acortar distancias, de mejorar las comunicaciones y de desarrollar proyectos familiares.

Artículo 17: derecho a la propiedad (individual y colectiva)

> **1.** Toda persona tiene derecho a la **propiedad, individual y colectivamente**.
>
> **2.** Nadie será privado arbitrariamente de su propiedad.

Tal vez uno de los ejemplos más disruptivos para el ejercicio de este derecho, en positivo y negativo, tiene que ver con las **criptomonedas** (Bitcoin, Ethereum, Dogecoin, Cardano o Solana, por ejemplo, como algunas de las más famosas hasta 2021). Las criptomonedas, en esencia, son monedas digitales que utilizan métodos de criptografía para asegurar las transacciones. Esto significa que es un sistema descentralizado en el que mediante la tecnología ***blockchain***, también conocida como cadena de bloques, cada agente de la red garantiza la seguridad y el equilibrio de las transacciones, alejando el modelo de los bancos centrales tradicionales y de las monedas de curso legal que existen actualmente en todos los países[54].

Los impactos positivos que estas criptomonedas ofrecen, si lo vinculamos con el derecho de propiedad, es que podrían hacer pensar que es posible la "democratización" de la riqueza, al menos en apariencia. Y esto, porque no dependen de una institución estatal, sino que su base es la descentralización, los bajos costes, la confidencialidad de las operaciones y la rapidez con que se ejecutan las transacciones. Aunque al mismo tiempo, uno de sus mayores impactos negativos está en el hecho de que el mercado de criptomonedas tiene una alta volatilidad, lo que podría provocar pérdidas significativas.

La ONU desarrolla otro aspecto negativo de la criptomoneda que se refiere a su uso para la compra y venta ilegal de drogas. En este sentido, ha expresado en su Informe Mundial sobre Drogas 2021 que la

53 Véase para más información: https://www.globalvillagespace.com/father-auctions-17-year-old-daughter-on-facebook/ y https://www.dailymail.co.uk/news/article-6384311/Facebook-auction-South-Sudan-child-bride-inspire-families-activists.html

54 Véase para más información: https://www.nationalgeographic.com.es/mundo-ng/que-son-criptomonedas-y-como-funcionan_16981

venta de drogas ha aumentado considerablemente, en parte por el desarrollo de nuevas tecnologías y la posibilidad de pago en criptomonedas. Es por eso que indica que para combatir las ganancias y los flujos financieros ilícitos que rigen el tráfico de drogas es preciso regular y supervisar a nivel internacional y nacional los mercados de criptomonedas y vigilar los pagos electrónicos para detectar operaciones sospechosas y denunciarlas[55].

Además de eso, se observa cómo en los últimos tiempos se ha producido una digitalización de procesos burocráticos, obligando a las personas usuarias a llevar a cabo trámites de forma telemática. Es el caso del registro de una propiedad y demás gestiones que deseen hacerse en relación a esta, el problema recurrente que podemos identificar es que no todo el mundo tiene acceso a internet. Existe una brecha digital, una realidad de desigualdades por lo que se refiere al acceso a internet (en relación al artículo 2 DUDH).

Y para evitar repeticiones innecesarias, se podrían añadir aquí los impactos positivos y negativos en el ejercicio y la privación de este derecho mencionados en el artículo 6, relativos al uso de tecnologías biométricas.

Sin olvidar también que el *Metaverse* o **Metaverso**, como entornos digitales donde los humanos interactúan social y económicamente como avatares, es y será un ámbito en el que habrá que poner atención para el ejercicio del derecho a la propiedad, individual y colectiva.

Artículo 18: libertad de pensamiento, de conciencia y de religión

> Toda persona tiene derecho a la **libertad de pensamiento, de conciencia y de religión**; este derecho incluye la libertad de cambiar de religión y de creencia, así como la libertad de manifestar su religión o su creencia, individual o colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia.

Artículo 19: libertad de opinión y expresión

> Todo individuo tiene derecho a la **libertad de opinión y de expresión**; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

55 Véase: World Drug Report 2021, https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html

Artículo 20: libertad de reunión y asociación pacífica

1. Toda persona tiene derecho a la libertad de **reunión y de asociación pacíficas**.

2. Nadie podrá ser obligado a pertenecer a una asociación.

Por la estrecha relación que existe entre estos derechos y su ejercicio, preferimos desarrollarlos de manera conjunta a fin de evitar repeticiones que pudieran resultar innecesarias, pero también porque en muchos casos, el ejercicio de uno de estos derechos no se puede separar del ejercicio de otro de ellos, por lo que nos parece necesario vincularlos en este primer análisis. Como se ha establecido en otros derechos, no significa que en desarrollos posteriores que se hagan a partir de este documento de trabajo, se pueda hacer un análisis individualizado.

En cuanto a la libertad de pensamiento, de conciencia y de religión y a la libertad de opinión y expresión, las TIC, junto con otras tecnologías (por ejemplo, los algoritmos) pueden utilizarse con el objetivo de manipular a las personas usuarias. Mediante el uso de *Big data* e IA (*machine learning*), las plataformas personalizan la información y el contenido al que tienen acceso y visualizan sus usuarias. Las redes sociales han establecido un nuevo modo de comunicación y un foro de opiniones, de las cuales se puede hacer un seguimiento gracias a la tecnología.

Esta información se utiliza para determinar qué contenido se recomienda y cuál no, restringiendo así, o dificultando, el acceso a determinados contenidos (limitando, por tanto, la información mediante la cual uno se crea sus propias opiniones). Se personaliza, por tanto, el contenido que se muestra, lo que puede conllevar a una manipulación masiva y a una polarización de la sociedad, lo que pone en duda hasta qué punto la opinión y los pensamientos son realmente libres. Este problema puede derivar en la radicalización de la sociedad (*rabbit hole*), facilitar un nuevo medio mediante el cual se expresen discursos de odio. Esto se consigue, por ejemplo, gracias a las *cookies*.

Además, este seguimiento de contenido consumido y compartido, podría afectar a los derechos recogidos en los artículos 18, 19 y 20, en el sentido de que el contenido que una persona publica y consume queda registrado y ello se puede usar en su contra, creando así una atmósfera de censura y modificando, consecuentemente, el comportamiento de los individuos.

Centrándose en el artículo 18, este se puede dividir en varias dimensiones. Por ejemplo, en el derecho a no revelar los pensamientos propios, a no ser penalizado o sancionado por estos y el derecho a no ser manipulado.

En cuanto a la primera dimensión, se ha demostrado que mediante *deep learning*, las redes podrían llegar a detectar la orientación sexual de las personas usuarias, sin que sea la persona afectada la que lo exprese y revele[56]. Por lo que se refiere a la segunda dimensión, como ya se ha dicho, la información

56 Véase para más información: https://psycnet.apa.org/record/2018-03783-002 y https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph

que se comparte y se consume en línea puede ser usada en contra del usuario. Además, también podría hablarse de la peligrosidad de las *fake news* y su capacidad de polarizar a la sociedad. Por último, en cuanto al derecho a no ser manipulado, se observa que a través de algoritmos y *machine learning* se estudia el comportamiento de las personas usuarias (mediante información como las preferencias musicales, las visitas a páginas web, el vocabulario empleado en las redes sociales, el número y tipo de reacciones en redes sociales, etc.) y ello sirve para personalizar el contenido que se muestra a las personas usuarias[57].

Además, tanto por lo que se refiere al artículo 18 como al 19, se presenta un dilema relativo a la censura. ¿Quién determina qué contenido se censura y cuál no? Estas decisiones pueden resultar discriminatorias unas veces, pero otras necesarias (a modo de ejemplo, la influencia de Facebook en la limpieza étnica de la minoría rohinyá en Myanmar).

En cuanto a la censura, hay quienes han propuesto la tecnología del *blockchain* como una solución debido a su descentralización, que supondría mayor dificultad y probabilidad de que se censuren contenidos. Sin embargo, hay quienes son más críticos con esta posición y no consideran que el *blockchain*[58] sea una solución[59], ya que las cadenas de bloques aún conservan funciones centralizadas, es decir, siempre habrá un censor.

En el marco de la ONU se ha desarrollado la cuestión del discurso de odio en línea, en un informe[60] presentado ante la Asamblea General en 2019. En dicho informe, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión interpreta los Principios Rectores sobre las Empresas y los Derechos Humanos[61] en relación al discurso de odio, y pone en cabeza de las empresas la obligación de disponer de procesos continuos para determinar cómo el discurso de odio afecta a los derechos humanos en sus plataformas, en particular mediante los algoritmos propios de dichas plataformas. Además, indica que no solo deberían valerse de personas expertas sino también de consultas con los grupos potencialmente afectados y las partes interesadas. Remarca que el Estado es responsable de controlar el accionar contrario a los derechos humanos de las empresas que se encuentran bajo su jurisdicción.

En cuanto a la expresión de género, la navegación anónima en redes ha facilitado el acceso a la esfera pública de mujeres que, de lo contrario, podrían haber sufrido represalias o ser objeto de violencia. Es

57 Véase para más información: https://www.frontiersin.org/articles/10.3389/frai.2019.00019/full

58 Las cadenas de bloques autorizadas tienden a ser, por diseño, más "cerradas" en cuanto a quién puede acceder en ese momento y el creador puede incluso designar quién ejecuta los nodos responsables de autenticar las transacciones. En el caso de las cadenas de bloques públicas, la mayoría de las personas usuarias aún requieren servicios y software intermediarios para conectarse e interactuar con las cadenas de bloques. La presencia de estos terceros para acceder a los servicios de blockchain, ya sean software, sitios web o extensiones de navegador, significa que los usuarios están depositando su confianza en entidades que pueden o no ser confiables.

59 Véase para más información: https://www.article19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf

60 Véase: Informe A/74/486 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión David Kaye, 09/10/2019.

61 Véase: "Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para 'proteger, respetar y remediar'", elaborados por el Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas. El Consejo de Derechos Humanos los adoptó en resolución 17/4, de 16/06/2011; véase: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

el caso de las activistas feministas y LGTBQ+, defensoras de derechos humanos y hasta víctimas de violencia doméstica. Pero, tal como resalta la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de la ONU, si esos espacios no son seguros, los grupos vulnerabilizados corren un mayor riesgo de ser víctima de violencia, censura o vigilancia[62]. Por esta razón es fundamental el papel de los Estados en la protección de los derechos humanos tanto en línea como fuera de línea.

Por otra parte, los Estados han restringido el uso de internet y de las redes sociales, afectando gravemente la libertad de expresión y de participación política de sus la ciudadanía. Tal es el caso de Venezuela en donde, durante protestas llevadas a cabo contra el gobierno de Nicolás Maduro, se interrumpió masivamente el servicio de internet y se bloquearon Twitter, Facebook, Instagram y YouTube[63].

Sobre la injerencia del Estado en la libertad de expresión –ya sea por sí o a través de empresas privadas– se ha expedido el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión diciendo que "las exigencias, solicitudes y otras medidas encaminadas a retirar contenido digital o acceder a la información de los clientes deben basarse en leyes promulgadas de forma válida, estar sujetas a supervisión externa e independiente, y demostrar que son medidas necesarios y proporcionales para alcanzar uno o más objetivos en virtud del artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos"[64]. Ello a fin de evitar restricciones desmesuradas de la libertad de expresión.

Esta situación fue reconocida en el ámbito de las Naciones Unidas por la Alta Comisionada de las Naciones Unidas, quien explica que los cierres de Internet, también llamados "cierres de la Red", "cortes" o "apagones", son una forma particularmente perniciosa de injerencia en las TIC y, por lo tanto, en el derecho a la reunión pacífica. Además, surten graves efectos en la efectividad de los derechos económicos y sociales, dado el número de actividades y servicios básicos afectados, incluido el acceso a los servicios de urgencia, información médica, banca móvil, transportes y material educativo. Esta interrupción deliberada al acceso a internet o a la divulgación de información no solo supone una vulneración del derecho internacional de los derechos humanos, sino también un perjuicio en el ámbito económico, habiéndose comprobado que provoca graves pérdidas económicas[65].

En cuanto a la libertad de asociación, el Comité de Derechos Humanos de ONU indica en su Observación General No. 37: "La manera en que se llevan a cabo las reuniones y su contexto cambian con el tiempo. Por ejemplo, como las nuevas tecnologías de la comunicación ofrecen la oportunidad de reunirse total o parcialmente en línea y a menudo desempeñan un papel fundamental en la organización,

62 Véase: Informe A/76/258 de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan, 30/07/2021.

63 Véase para más información: https://espaciopublico.ong/internet-amurallado-acceso-restringido-en-venezuela/ y https://www.infobae.com/america/venezuela/2019/11/16/a-horas-del-comienzo-de-la-jornada-de-protestas-contra-maduro-en-venezuela-ya-se-registran-interrupciones-masivas-en-internet/

64 Véase: Informe A/HRC/32/38 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, 11/05/2016.

65 Véase: "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 24/06/2020, párrafos 16-20.

la participación y la vigilancia de las reuniones físicas, la injerencia en esas comunicaciones puede impedir las reuniones. Si bien las tecnologías de vigilancia se pueden utilizar para detectar amenazas de violencia y, por consiguiente, proteger a la población, también pueden atentar contra el derecho a la intimidad y otros derechos de los participantes y los transeúntes y tener un efecto disuasorio".

"Muchas de las actividades conexas (al derecho de asociación y reunión pacífica) se realizan en línea o se basan en servicios digitales. La DUDH también protege esas actividades. Los Estados partes no deben, por ejemplo, bloquear o dificultar la conexión a Internet en relación a las reuniones pacíficas. Lo mismo se aplica a las interferencias georreferenciadas o específicas de una tecnología en la conectividad o el acceso al contenido. Los Estados deberían velar por que las actividades de los proveedores y los intermediarios de servicios de Internet no restrinjan indebidamente las reuniones o la intimidad de los participantes en ellas. Toda restricción del funcionamiento de los sistemas de difusión de información debe estar en conformidad con las pruebas de las restricciones de la libertad de expresión".

"El hecho de que los participantes en una reunión se cubran la cara o se disfracen de otra manera (...) o tomen otras medidas para participar anónimamente puede formar parte del elemento expresivo de una reunión pacífica o servir para contrarrestar las represalias o proteger la intimidad, en particular en el contexto de las nuevas tecnologías de vigilancia. Se debería permitir el anonimato de los participantes, a menos que su conducta ofrezca motivos razonables para su detención (...)"[66].

En línea con lo expresado en esa Observación, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos expresa preocupación en torno al uso de armas y municiones menos letales por parte de las fuerzas policiales a la hora de reprimir a manifestantes durante el ejercicio de su derecho de reunión y asociación. Explica que elementos como las armas de energía dirigida (como las pistolas *Taser*), los proyectiles avanzados de impacto cinético (como proyectiles de energía atenuada), los drones y los sistemas autónomos que emplean gases lacrimógenos y otras municiones menos letales, las bolas de pimienta y lanzadores de bolas de pimienta, las armas de aturdimiento, armas acústicas y sustancias malolientes, son utilizadas por las fuerzas de seguridad en aquellos casos en que es necesario cierto grado de fuerza pero donde utilizar armas de fuego sería ilícito. Sin embargo, no hay que perder de vista que estos elementos tecnológicos de los que se vale la policía son alternativas de fuerza letal, que pueden infligir daños realmente graves. Agrega que algunas armas menos letales utilizan la fuerza de forma autónoma o por control remoto, lo que plantea cuestiones complejas en cuanto a la determinación de la responsabilidad por las posibles vulneraciones de los derechos humanos, en particular el derecho a la vida[67].

Para el ejercicio de estos derechos se debería pensar más en aquellas tecnologías que generen un impacto positivo, como podría ser el acceso de todas las personas a la información, más formas de expresar y difundir opiniones, ejercer convicciones religiosas o de pensamiento sin discriminación desde cualquier lugar adecuado para ese fin, desarrollar reuniones y manifestaciones por medio de entornos digitales, entre muchas otras más.

66 Véase para más información: https://www.hchr.org.co/files/observacion-general-37.pdf

67 Véase: "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 24/06/2020, párrafos 41-45.

Esos impactos positivos sin duda los puede tener toda tecnología, pero como en todos los derechos y tecnologías, lo primero que se debe garantizar para poder pensar en impactos positivos es en la accesibilidad a toda persona. Pero también, en evitar que a partir del ejercicio de estos derechos se obtenga información personal que no solo invada el derecho a la privacidad, sino también aquella que puede poner en riesgo la vida o integridad de las personas que ejercen sus derechos.

Pero también es importante no establecer a las tecnologías digitales y de la información como las únicas y principales vías que se tengan para el ejercicio de estos derechos y libertades, pues con el simple hecho de que "nos apaguen" los servidores, las redes o las aplicaciones, nos dejarían sin posibilidad de ejercer parte importante de estos derechos.

Artículo 21: derecho a la participación política y elección de gobierno

> **1.** Toda persona tiene derecho a **participar en el gobierno de su país**, directamente o por medio de representantes libremente escogidos.
>
> **2.** Toda persona tiene el derecho de acceso, en condiciones de igualdad, a las funciones públicas de su país.
>
> **3.** La voluntad del pueblo es la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por **sufragio** universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto.

Todos los derechos analizados en el apartado anterior son herramientas de participación política por parte de la sociedad. Pero el derecho que permite acceder a muchas de las posiciones de decisión en los países, es el derecho al voto, pasivo y activo.

El voto electrónico se ha desarrollado como una herramienta que puede facilitar el proceso del voto a la ciudadanía, ya sea porque se encuentren en lugares de difícil acceso, porque se encuentran en el extranjero o, simplemente, porque al ser en apariencia de más fácil acceso desde el domicilio, se podría aumentar la participación ciudadana. El voto electrónico no se diferencia mucho del voto físico. La ciudadanía se identifica y registra a partir de unos documentos y ejerce su derecho de votación pero de manera telemática, a través de un dispositivo con conexión a internet.

El primer problema que se debe señalar, como en otros derechos, es que no toda persona tiene el "privilegio digital", con lo que la pretendida facilidad e incremento de participación, no siempre está garantizado.

Además de eso, también representan problemas en el sentido de que actualmente el *hardware* y *software* necesarios para su implementación son elevados en sus costos, contemplando el costo total de propiedad, a lo que se debe añadir mantenimiento, licencias, soportes y capacitación.

Aunque el elemento más importante es el hecho de que en muchas regiones del mundo el electorado desconfía del uso de los medios electrónicos en ejercicios democráticos. No solo en relación a aspectos de seguridad y privacidad de los votantes (recordemos que el voto se considera privado o secreto), sino también en cuanto a que efectivamente el voto emitido sea contado en la opción política en la que originalmente se emitió y solo voten quienes efectivamente tienen derecho.

No son muchos los países que han incorporado esta vía de votación en sus procesos electorales. Se podrían destacar entre los que lo han implementado y ejercido de esa forma, al menos en parte, los siguientes países: Australia (2011), Bélgica (2014), Brasil (2000), Bulgaria (2021), Canadá (2008), Estonia (2005), Estados Unidos de América (2000), Filipinas (2007), India (2003), México (2020 solo elección de diputación migrante de la Ciudad de México), Suiza (2005) y Venezuela (2004).

Con el aparente fin de brindar más seguridad en estos procesos, aquí también se podría incluir el uso de tecnologías biométricas, con todos los aspectos positivos y negativos en el ejercicio y la privación de este derecho mencionados en los artículos 6 y 17.

Vinculado con el proceso electoral y lo señalado en el apartado anterior, el uso de las redes sociales en las campañas políticas ha adquirido una gran importancia. Aportando cosas positivas como el llegar a públicos que de otra forma no se llegaría, pero también aspectos negativos como campañas de odio, *fake news*, manipulación de campañas, etc.

Otra situación no menor para el ejercicio de las funciones públicas es el hecho de que muchas oposiciones a cargos públicos se están desarrollando desde sus primeras etapas por medios telemáticos, con lo que nuevamente se puede poner en duda la efectiva posibilidad de que acceda cualquier persona, el uso de algoritmos para seleccionar o rechazar determinados perfiles, así como selecciones basadas en criterios poco transparentes aunque públicamente se establezcan otros.

Una correcta implementación de las tecnologías para garantizar la participación política requieren de base una confianza plena en las instituciones que las ponen en marcha. Sin eso, es difícil que, por confiables que sean, brinden seguridad a las personas. Pero no hay duda alguna de que si se cuidan los aspectos que se han reiterado en otros derechos respecto a la transparencia, protección de datos y privacidad, podrían ser una herramienta importante para fomentar la democracia y el buen gobierno.

Artículo 22: derecho a la seguridad social

> Toda persona, como miembro de la sociedad, tiene **derecho a la seguridad social**, y a obtener, mediante el esfuerzo nacional y la cooperación internacional, habida cuenta de la organización y los recursos de cada Estado, la satisfacción de los derechos económicos, sociales y culturales, indispensables a su dignidad y al libre desarrollo de su personalidad.

El derecho a la seguridad social puede verse afectado de distintas formas por la tecnología. El mayor problema se presenta cuando la tramitación de las gestiones necesarias para tener acceso a ella se rea-

liza de forma telemática, ya que, como se viene diciendo, no todas las personas tienen acceso a internet ni a dispositivos tecnológicos que les permitan llevar a cabo estas gestiones.

Por otra parte, se observa que en algunos países se está utilizando el ***big data***, el ***machine learning*** y la toma de decisiones automatizada mediante algoritmos para conceder o denegar las prestaciones de la seguridad social. Es el caso del Crédito Universal de Reino Unido. Se trata de un tipo de prestación de la seguridad social que pretende asistir y conceder ayudas económicas a aquellas personas que se encuentran en situación de riesgo o vulnerabilidad. Mediante este sistema se concede una asignación a quien la solicite y cumpla con los requisitos establecidos para ello.

Para decidir la cantidad o suma de dinero que se atribuye a cada solicitante se utiliza un sistema de algoritmo basado en datos de las personas solicitantes que se refieren a su situación financiera y personal. Por ejemplo, se valora cuánto dinero ganan las personas solicitantes, datos que se extraen a partir de la información contenida en las nóminas de aquellos. Dicha información era introducida de forma manual por funcionarios y el sistema administrativo de impuestos. Se puso de manifiesto que dicha información no se estaba introduciendo (o, al menos, no correctamente) y que, por tanto, el algoritmo no tenía en cuenta la frecuencia con la que las personas solicitantes cobraban sus nóminas o demás prestaciones. Por tanto, el cálculo puede resultar erróneo. Si el sistema entiende, de forma equivocada, que a una persona se le ha pagado con mayor frecuencia y, por tanto, que ha ganado más dinero de lo que realmente ha cobrado, la asignación que le va a conceder el algoritmo es menor a la que tiene derecho. Concluyendo, nos encontramos ante un sistema que puede afectar de forma negativa a aquellas personas que ya se encuentran en situación de vulnerabilidad o riesgo[68].

Otro ejemplo, si bien no se limita a afectar únicamente al derecho a la seguridad social, es el Sistema de Crédito Social establecido en China[69]. Se trata de un sistema, con base en un marco regulatorio, que persigue el objetivo de informar al Estado sobre la "confianza" de los individuos, corporaciones y entidades. Se trata de un sistema que si bien no es definitivo y todavía se encuentra en desarrollo, ya se han llevado a cabo algunas pruebas piloto. Mediante este sistema se incluye a la ciudadanía en una *blacklist* si llevan a cabo acciones que el Estado considera incorrectas. Ejemplos de "actuaciones no deseables" serían: comprar bebidas alcohólicas con frecuencia; escuchar música a un volumen elevado; comer en el transporte público; hacer una reserva en un hotel o en un restaurante y no asistir, etc. Estas acciones "negativas" conllevan la atribución de puntos negativos al individuo.

También cabe la posibilidad de ganar puntos. Por ejemplo donando sangre, haciendo servicios voluntarios para la comunidad, donando a la caridad, etc. Estar incluido en la *blacklist* conlleva consecuencias negativas. Una de ellas podría ser la denegación del acceso a prestaciones de la seguridad social. Otras consecuencias serían la prohibición para poder viajar en avión o en trenes de alta velocidad; la negativa a poder asistir a escuelas o universidades privadas, etc. Por el contrario, las personas con puntos positivos reciben beneficios. Por ejemplo, un menor tiempo de espera en los hospitales, mayor probabilidad de recibir una oferta de trabajo (en relación con el artículo 23 *infra*), etc.

68 Véase para más información: https://www.hrw.org/report/2020/09/29/automated-hardship/how-tech-driven-overhaul-uks-social-security-system-worsens

69 Véase para más información: https://nhglobalpartners.com/china-social-credit-system-explained/, así como: https://www.wired.co.uk/article/china-social-credit-system-explained y https://journals.sagepub.com/doi/full/10.1177/2059436419856090

Además, más allá de la incidencia negativa que ello puede suponer para el derecho a la seguridad social, se evidencia un problema de discriminación (en relación con los artículos 1 y 2).

Artículo 23: derecho al trabajo

> **1.** Toda persona tiene **derecho al trabajo**, a la libre elección de su trabajo, a condiciones equitativas y satisfactorias de trabajo y a la protección contra el desempleo.
>
> **2.** Toda persona tiene derecho, sin discriminación alguna, a igual salario por trabajo igual.
>
> **3.** Toda persona que trabaja tiene derecho a una remuneración equitativa y satisfactoria, que le asegure, así como a su familia, una existencia conforme a la dignidad humana y que será completada, en caso necesario, por cualquiera otros modos medios de protección social.
>
> **4.** Toda persona tiene derecho a fundar **sindicatos** y a sindicarse para la defensa de sus intereses.

Las nuevas tecnologías pueden poner en riesgo el derecho al trabajo[70]. Algunos de los problemas existentes ya se han expuesto anteriormente con la explotación laboral que se lleva a cabo en determinados países en la extracción de materias primas para la elaboración de dispositivos tecnológicos. Las condiciones laborales de las personas que se dedican a ello son, generalmente, precarias y atentan contra los derechos humanos (en relación con los artículos 3 y 4). Otro problema ya planteado es aquel relacionado con el uso de *darkwebs* con fines de explotación laboral. En muchos casos se trata de explotación sexual que afecta, mayoritariamente, a menores de edad[71].

Por otra parte, se ha observado que en los últimos años las empresas están empezando a utilizar tecnologías para tomar decisiones automatizadas en relación a los procesos de selección o promoción de personal[72]. El uso de **algoritmos** influye en diferentes momentos de estos procesos. Por ejemplo, y como se expondrá a continuación, en la decisión respecto a qué personas se dirigen determinadas ofertas de trabajo. Estas **herramientas predictivas** también analizan y puntúan los currículos vitae, asistiendo a los departamentos de recursos humanos para valorar las competencias y aptitudes de los candidatos y seleccionar al "mejor".

Sin embargo, estos algoritmos se alimentan de información introducida y valorada previamente por un individuo, por tanto, el algoritmo está contaminado de los sesgos, estereotipos y prejuicios de la persona que introduce la información. El algoritmo aprende, desarrolla y toma decisiones en base a unos patrones que pueden resultar discriminatorios. Que ello se perpetúe en el tiempo dificulta poner en duda o cuestionar las

70 Véase para más información: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/614539/EPRS_STU(2018)614539_EN.pdf

71 Véase para más información: https://www.diginex-solutions.com/insights/the-human-cost-of-the-dark-web

72 Véase para más información: https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias

decisiones tomadas por el algoritmo e incluso puede resultar que quien creó o quien introdujo la información en este no entienda cómo hace sus predicciones el algoritmo por ser demasiado complicado y autónomo.

Para ejemplificarlo, se evidenció que el algoritmo que Amazon usaba para seleccionar los candidatos, discriminaba a las mujeres. La empresa llevaba usando el algoritmo más de diez años, período durante el cual este aprendió (por la información introducida hasta el momento relativa a los currículos) que los candidatos hombres tenían preferencia por encima de las candidatas mujeres[73]. El algoritmo entendió que a la empresa no le gustaban los CV que contenían la palabra "mujer" en él.

Otro problema que se presenta, concretamente con el ***big data***, **IA** y ***machine learning***, se refiere al anuncio de ofertas de trabajo personalizado[74]. Las empresas usan algoritmos de aprendizaje automático (*machine learning algorithms*) para publicitar las ofertas de trabajo a personas concretas por considerarlas candidatas más relevantes y evitar publicitar a personas que no cumplen con el perfil deseado por la empresa.

Lo mismo sucede con la selección y/o promoción de personal mediante algoritmos de aprendizaje automático. La decisión de publicitar una oferta de trabajo a unos candidatos por tener estos rasgos comunes y no a otros, o el hecho de "ocultar" dichas ofertas a otros colectivos puede resultar discriminatoria. Primero (y se repite siempre que nos encontramos ante este tipo de tecnología) porque se introduce información e historiales que pueden contener sesgos, prejuicios y estereotipos y, segundo, que el algoritmo aprende de ellos y crea patrones y toma decisiones que pueden ser discriminatorias. Se ha evidenciado que existen empresas o plataformas (como Google, LinkedIn o Facebook) cuyo algoritmo ha decidido ocultar sus ofertas de trabajo a colectivos por razón de raza, edad o género o, incluso, que discrimina a las personas con discapacidad.

Por otra parte, en los últimos años también se ha empezado a debatir sobre el uso de **tecnologías de reconocimiento y análisis facial** durante los procesos de selección de personal, esto es, durante las entrevistas. El uso de este tipo de *software* permite analizar las expresiones faciales del entrevistado y las conclusiones que de ellas saque van a asistir al responsable en la decisión de contratar. Ello presenta dos problemas principales. El primero hace referencia a la privacidad. Esto es, quién tendrá acceso a esas grabaciones, durante cuánto tiempo se tendrá acceso a ellas y qué usos se les va a dar. Por otra parte, la cuestión relativa al consentimiento y qué tan pleno, libre e informado es. Además, surge la duda de si aceptar que se le aplique a uno esta tecnología durante una entrevista es una condición necesaria e ineludible para tener la oportunidad de postular para el puesto de trabajo de que se trate (qué tan libre es el consentimiento y no condicionado). A modo de ejemplo, *HireVue* y *Unilever* son empresas que llevan tiempo empleando esta tecnología para la selección de personal[75].

La Alta Comisionada de las Naciones Unidas para los Derechos Humanos ha expresado preocupación en relación al uso de algoritmos en la contratación, monitoreo y despido de personas trabajadoras, en

73 Véase para más información: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN-1MK08G

74 Véase para más información: https://ant.isi.edu/datasets/addelivery/Discrimination-Job-Ad-Delivery.pdf y https://link.springer.com/article/10.1007/s40685-020-00134-w

75 Véase para más información: https://skillroads.com/blog/ai-and-facial-recognition-are-game-changers-for-recruitment

un informe presentado ante el Consejo de Derechos Humanos en 2021[76]. Explica, entre otras cuestiones, que el monitoreo del comportamiento durante las horas laborales se ha extendido al estudio del comportamiento general de las personas empleadas. Esto se ha visto exacerbado con la pandemia de dos formas. Primero, algunas empresas que proporcionan a las personas trabajadoras planes de salud preventiva recopilan cada vez más datos relacionados con la salud. En segundo lugar, a medida que se ejecutan más procesos digitalmente mientras las personas trabajan desde casa, la supervisión del lugar de trabajo mediante sistemas de inteligencia artificial se lleva a los hogares de los las personas trabajadoras. Ambas tendencias aumentan el riesgo de fusionar los datos de la supervisión del lugar de trabajo con entradas de datos no relacionadas con el trabajo. Esta recopilación de datos conlleva la ya mencionada introducción de sesgos y posterior discriminación en el uso de aquellos datos.

Otra crítica que pueden recibir las nuevas tecnologías, especialmente la **IA**, es que si bien permite la creación de nuevos puestos de trabajo, también desfavorece a aquellos empleos que no requieren una elevada calificación y que resultan mecánicos y rutinarios (por ejemplo, el trabajo de operarios de fábricas). Porque este tipo de trabajos pueden automatizarse y ello conlleva la desaparición de puestos de trabajo y/o la reducción de horarios laborales.

Por tanto, el principal problema radica en la posibilidad de que determinadas tecnologías puedan llevar a cabo empleos por un coste menor y, consecuentemente, reemplazar a las personas, provocando así una falta de ingresos para estas[77].

Hasta ahora, y como consecuencia de la segunda revolución industrial, se ha evidenciado que la automatización industrial de los procesos de producción a gran escala reemplaza la mano de obra humana. Pero ¿podría, hoy en día, esta tecnología, afectar a otros perfiles de trabajo? Es un ejemplo de ello los cada vez más aceptados ***delivery drones***. Si bien esta tecnología puede resultar muy beneficiosa para la ayuda humanitaria, quizás también esté reemplazando, o lo haga en un futuro muy cercano, puestos de trabajo.

Además, estas tecnologías que venimos mencionando incluso han sido empleadas para evaluar el trabajo de las personas, con consecuencias, en algunos casos, negativas. Es el ejemplo de IMPACT[78], un sistema desarrollado en Estados Unidos. Se trata de un algoritmo creado con el objetivo de "optimizar el sistema escolar y garantizar mejores resultados para los alumnos" mediante la evaluación de los profesores, para, a final de curso, dejar de contar con aquellos que hubieran obtenido los resultados menos favorables. Ya de entrada, cabe objetar que, pretender evaluar el impacto que una persona puede tener sobre otra a lo largo de un curso escolar resulta un proceso muy complejo, y, desde luego, muy difícil de medir con un algoritmo[79].

Dicho algoritmo se aplicó y no resultó posible revocar las decisiones que ofreció y que luego un equipo de personas evaluó y afirmó. Las autoridades competentes argumentaron que "aunque fuera posible

76 Véase: Informe A/HRC/48/31 "The right to privacy in the digital age", Alta Comisionada de Naciones Unidas para los Derechos Humanos, 13/09/2021.

77 Véase para más información: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237.pdf

78 S. Sawchuck, "Rhee to Dismiss Hundreds of Teachers for Poor Performance", *Education Week Blog* (2010).

79 J. Gillum, M. Bello, "When standardized test scores soared in D.C., were the gains real?", *The Hechinger Report* (2011).

que hubiera errores en las puntuaciones, las pruebas aportadas no eran concluyentes". Ello pone de manifiesto que, aun cuando existan argumentos razonables para cuestionar los datos que se suministran a los algoritmos de aprendizaje automático, es difícil poder recurrir sus decisiones[80]. Por eso insistimos en la necesidad de desarrollar sistemas de auditoría y de rendición de cuentas.

En lo que refiere a **empleo y discapacidad**, las personas con discapacidad están expuestas al desempleo, a las condiciones de trabajo vulnerables y a una amplia brecha salarial. La revolución tecnológica influye tanto positiva como negativamente en las oportunidades de empleo de las personas con discapacidad. En este escenario, las herramientas digitales les permiten acceder a plataformas de contratación en línea, a empleos con modalidad de teletrabajo, y hasta ayudarlos en sus tareas diarias. Sin embargo, si no poseen las competencias necesarias, si las TIC se encuentran fuera de su alcance o si las herramientas digitales no son accesibles, las personas con discapacidad no se beneficiarán de estas oportunidades y, por tanto, correrán el riesgo de quedarse atrás.

La IA puede asistirlos en sus tareas laborales diarias. El *software* está aprendiendo a reconocer y a reaccionar frente a imágenes, sonidos y expresiones lingüísticas, lo que permite que se hagan valer de herramientas como el subtitulado automático con IA, vehículos autónomos y el reconocimiento facial y de imágenes que hacen posible la interacción con el entorno. Sin embargo, estas herramientas solo tienen impacto positivo si se diseñan para una inclusión plena. Existen riesgos, ya mencionados, como son los datos sesgados que reproducen discriminación, que los datos de formación no representen suficientemente a los grupos minoritarios y que la recopilación de datos no incluya a las personas con discapacidad[81].

Además de lo anterior, también se puede señalar que las nuevas tecnologías pueden tener un impacto negativo en el derecho al trabajo cuando se usan e instala *software* en los ordenadores de empleados y empleadas que teletrabajan, a fin de monitorear su actividad, emitiendo informes y capturas de pantalla constantes que además pueden identificar contraseñas, correos electrónicos, transferencia de archivos, aplicaciones que usan, etc. (empresas como ActiveTrak, Hivedesk, Teramind, Time Doctor y WorkExaminer se dedican a desarrollar estos *software*).

De igual manera, las tarjetas de entrada y tecnologías biométricas para controlar la entrada y salida del trabajo que recogen más información que la estricta de entrada y salida del trabajo; o la video vigilancia en todos los ámbitos de trabajo y el monitoreo mediante GPS.

Aunque estas mismas se podrían usar para generar un impacto positivo si por ejemplo, la video vigilancia en el lugar de trabajo se usa solo para dar seguridad a las personas empleadas, sistemas privados de seguridad que los vigilan constantemente y acuden de inmediato en caso de peligro; los sistemas para controlar que si trabajan más horas quede constancia de ello y se pueda exigir su pago, o bien soluciones tecnológicas destinadas al respeto del derecho a la desconexión: definir un horario en que la red WIFI corporativa estará disponible (horario fuera de cual las personas empleadas no podrán acceder a la red corporativa), *software* de registro de la jornada laboral, *software* que bloquea envío de correos a determinada hora, etc.

80 C. O'Neil, "Armas de destrucción matemática: cómo el *Big data* aumenta la desigualdad y amenaza la democracia", *Capitán Swing Libros* (2017).

81 Véase: "Una economía digital inclusiva para las personas con discapacidad", Publicación de la Fundación ONCE y la Red Mundial de Empresas y Discapacidad de la OIT, desarrollada en el marco de Disability Hub Europe, un proyecto liderado por la Fundación ONCE y cofinanciado por el Fondo Social Europeo, febrero 2021.

El trabajo ha ido cambiando en todas las épocas de la historia humana y, evidentemente, con la existencia de nuevas tecnologías no podía quedar ajeno a esos cambios. En todo caso, lo importante seguirá siendo no perder de vista el contenido de los principios básicos del derecho al trabajo, pues independientemente de las nuevas tecnologías que se apliquen, los mínimos y sus desarrollos establecidos desde siglos atrás permanecen y deben ser observados, aun cuando lo que ponga en riesgo al trabajo se trate de la más reciente tecnología disponible.

Artículo 24: derecho al descanso y al tiempo libre

> Toda persona tiene derecho al **descanso**, al disfrute del tiempo libre, a una limitación razonable de la duración del trabajo y a vacaciones periódicas pagadas.

Muy vinculado con el derecho anterior, está el derecho al descanso. En este encontramos ahora dos problemas principales en relación con la limitación razonable de la duración del trabajo. El primero quizás más técnico y tangible, y el segundo más abstracto.

El primero hace referencia al uso de tecnologías como el GPS (*Global Positioning System*) o de vigilancia masiva, cuando estas suponen un control constante de la localización y actividad de los individuos. El segundo, estrechamente relacionado con el primero, es el impacto que estas tecnologías pueden causar al bienestar de los individuos, en el sentido de sentirse continuamente vigilados y forzados u obligados a trabajar y ser productivos.

Además, desde un punto de vista todavía más abstracto, podríamos cuestionarnos si debería existir y si es posible un derecho al descanso de las tecnologías, ya que nos encontramos influenciados por ellas constantemente y una desintoxicación parece, de momento, no ser muy viable.

Así, parecería que en la actualidad algunos de los impactos negativos más claros en el derecho al descanso están en el uso excesivo de móviles, tablets y dispositivos similares, pues eso puede provocar:

- Síndrome de FOMO (*Fear of missing out*): sensación de malestar que aqueja a un individuo al conocer que otras personas están disfrutando distintas actividades agradables o placenteras, no siendo parte activa de ello.
- Síndrome de la vibración fantasma (*Phantom Vibration Syndrome*): percepción de que el móvil está vibrando o sonando, cuando no lo está.
- Lapso de atención acortado, debido a la exposición constante a noticias y videos cortos.
- "*Popcorn brain*": navegar muchas horas provoca el síndrome de "*popcorn brain*" que implica que el cerebro esté acostumbrado a la constante estimulación electrónica, por lo que la interacción real resulta aburrida o provoca ansiedad.

La hiperconectividad ha generado en este ámbito que ya se hable del **derecho a la desconexión**, que en principio está pensado solo para ámbitos laborales, pero que bien se podría extender a otros ámbitos personales que permitan que las personas puedan interactuar entre ellas, que se desarrollen actividades lúdicas o recreativas más allá de los dispositivos electrónicos y, en general, que toda persona pueda y sea capaz de no tener un contacto constante ni dependencia a tecnologías digitales.

En este derecho también se tiene que decir que, aquí, el "privilegio digital" en realidad parece más una carga, pues el hecho de no tener acceso a estas tecnologías es sin duda una de las mejores garantías para evitar el apego, control, dependencia y adicción a aparatos electrónicos, así como a las muy diversas aplicaciones y usos que se les puede dar en perjuicio del derecho al descanso.

Artículo 25: derecho a un nivel de vida adecuado

> **1.** Toda persona tiene derecho a un **nivel de vida adecuado** que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios; tiene asimismo derecho a los seguros en caso de desempleo, enfermedad, invalidez, viudez, vejez u otros casos de pérdida de sus medios de subsistencia por circunstancias independientes de su voluntad.
>
> **2.** La maternidad y la infancia tienen derecho a cuidados y asistencia especiales. Todos los niños, nacidos de matrimonio o fuera de matrimonio, tienen derecho a igual protección social.

En este derecho convergen muchos otros que ya se han analizado antes, por lo que solo señalaremos algunos aspectos que pueden impactar en el derecho a un nivel de vida adecuado que no se han desarrollado.

Así, añadimos dos nuevos posibles problemas. Por una parte, y exclusivamente vinculado con el derecho a la asistencia médica, se plantean las siguientes cuestiones. Primero, relativo a los datos. Actualmente se utilizan **IA** y ***big data*** para asistir en el diagnóstico, pronóstico, tratamiento, etc., de los pacientes. Toda esta información que se recopila provoca que el conocimiento de esta ya no se limite a una relación entre paciente y médico exclusivamente. Además, debemos de preguntarnos hasta qué punto el paciente presta su consentimiento y si este es libre, pleno e informado y, por otra parte, si se informa sobre dónde queda almacenada esta información, qué uso va a dársele, durante cuánto tiempo va a estar disponible, etc.

Pero, además, con el auge del uso de tecnologías como la videollamada, acrecentado tras la pandemia de covid-19, nos encontramos ante un nuevo concepto: la "telemedicina". Como en todos los casos que hacen referencia a tecnologías que requieren el uso de un dispositivo tecnológico y el acceso a internet, se repite el problema de la brecha digital.

Asimismo[82], podría mencionarse el uso de **tecnologías de asistencia** (robots, herramientas como Alexa, Siri…) en relación a las personas de avanzada edad. Si bien es cierto que, generalmente, esta tecnología se percibe como algo positivo que puede ayudar a este colectivo, por ejemplo, en el sentido de hacerles compañía, no deben olvidarse ciertos aspectos negativos. Primero, por lo que se refiere a las cuestiones de privacidad que ya se vienen mencionando, así como el riesgo de que estas tecnologías sean *hackeadas* y se usen para perjudicar física o mentalmente a sus usuarias.

Además, qué tanto conocemos y, concretamente, sus usuarias, el funcionamiento de estas herramientas. No entenderlas puede perjudicarnos en relación al uso que se les da o la voluntad de utilizarlas o no. Hay quienes afirman que estas tecnologías pueden contribuir a la infantilización y edadismo de las personas de edad avanzada, tipos de discriminación por razón de edad[83].

En el marco de la Observación General No. 25 (2020) elaborada por el Comité de Derechos Económicos, Sociales y Culturales, el Comité se encarga de interpretar el artículo 15, párrafo 1 b del Pacto Internacional de Derechos Económicos, Sociales y Culturales que consagra el derecho a "*gozar de los beneficios del progreso científico y de sus aplicaciones*". Es así que delinea la **estrecha relación entre el goce del progreso científico y el pleno desarrollo de otros derechos íntimamente relacionados a las nuevas tecnologías como son el derecho a la alimentación y a la salud.**

Respecto al derecho a la salud y el desarrollo de tecnologías emergentes, delinea beneficios y perjuicios de estas últimas. Por una parte, podrían mejorar el disfrute de los derechos económicos, sociales y culturales. Por ejemplo, las aplicaciones de la IA en la industria o los servicios pueden dar lugar a enormes aumentos de la productividad y la eficiencia, y la biotecnología puede permitir la cura o el tratamiento de muchas enfermedades.

Por otra parte, estos cambios podrían intensificar la desigualdad social al aumentar el desempleo y la segregación en el mercado laboral, y los algoritmos incorporados en la inteligencia artificial pueden reforzar la discriminación, etc.

El Comité entiende que esta problemática debe ser abordada desde tres frentes: (i) cooperación internacional, (ii) adopción de decisiones relativas a las nuevas tecnologías en clave de derechos humanos y desde una perspectiva holística e integradora, y (iii) abordaje especial de ciertas aspectos que impiden el pleno disfrute de derechos económicos, sociales y culturales (por ejemplo, acceso de personas con discapacidad a las nuevas tecnologías para su desarrollo personal y laboral).

Como se ha insistido en muchos derechos, las tecnologías pueden sumar mucho al efectivo ejercicio de todos los derechos y libertades, por lo que un uso adecuado, universal y sin discriminación de las tecnologías, sin duda alguna, podría asegurar un nivel de vida adecuado para toda persona.

82 Véase para más información: https://www.researchgate.net/publication/230884254_Assistive_technology_use_and_human_rights_enjoyment_A_cross-sectional_study_in_Bangladesh, así como: http://www.powertopersuade.org.au/blog/is-assistive-technology-a-human-rights-issue-for-dementia/5/4/2017 y https://digital.csic.es/bitstream/10261/212028/1/Personal%20autonomy%20in%20elderly%20and%20disabled.pdf

83 Véase para más información: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.684012/full

Artículo 26: derecho a la educación

> **1.** Toda persona tiene derecho a la **educación**. La educación debe ser gratuita, al menos en lo concerniente a la instrucción elemental y fundamental. La instrucción elemental será obligatoria. La instrucción técnica y profesional habrá de ser generalizada; el acceso a los estudios superiores será igual para todos, en función de los méritos respectivos.
>
> **2.** La educación tendrá por objeto el pleno desarrollo de la personalidad humana y el fortalecimiento del respeto a los derechos humanos y a las libertades fundamentales, favorecerá la comprensión, la tolerancia y la amistad entre todas las naciones y todos los grupos étnicos o religiosos, y promoverá el desarrollo de las actividades de las Naciones Unidas para el mantenimiento de la paz.
>
> **3.** Los padres tendrán derecho preferente a escoger el tipo de educación que habrá de darse a sus hijos.

Si bien es cierto que el ***big data*** y la **IA** pueden facilitar el acceso a la educación, ello depende del acceso que se tenga a internet y de la disponibilidad de un dispositivo tecnológico que nos permita este acceso[84]. Por lo que un primer reto sería asegurar el acceso a internet y a dispositivos tecnológicos de forma igualitaria y sin discriminaciones (en relación a los artículos 1 y 2).

Además, el acceso a las herramientas educativas digitales personalizadas depende del acceso a los datos del usuario. Por lo que se repiten los problemas de privacidad y de consentimiento. En relación al consentimiento, sobre todo, porque aceptar que se tenga acceso a los datos es un requisito imprescindible y obligatorio para poder beneficiarse de estas herramientas educativas digitales. El acceso al entorno digital de niños y niñas implica, entonces, el procesamiento de sus datos por parte de empresas que manipulan los contenidos para su propio beneficio (por ejemplo: características de diseño publicitario que anticipan las acciones del niño y lo guían hacia la búsqueda de contenidos más extremos, o uso de la información personal o la ubicación de un niño para transmitir contenidos potencialmente nocivos con fines comerciales)[85].

Esta nueva posibilidad, la de hacer más accesible la educación (teniendo en cuenta lo que ya se ha dicho, brecha digital y datos), en ningún caso debe entenderse como una herramienta sustitutiva a la forma convencional educativa. La formación online o *e-learning* debe entenderse como complementaria y no como sustitutiva.

Asimismo, estas plataformas o herramientas educativas digitales pertenecen a una empresa, a la cual se le va a ceder información. Existe el riesgo de que se utilice esta información de forma perjudicial (manipulación). Por último, no será el usuario o el beneficiario (en este caso los alumnos o sus progeni-

84 Véase para más información: https://www.unicef.es/educa/blog/covid-19-brecha-educativa

85 Observación General No. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital, Comité de los Derechos del Niño, 02/03/2021.

tores) quienes escojan el programa educativo digital, sino que será la escuela, por lo que la posibilidad de elegir el programa sería reducida.

Un ejemplo concreto de estos impactos está en un **algoritmo** desarrollado en Australia que, basándose en información que el Estado dispone, puede recomendar a adolescentes nacidos en clases socioeconómicas bajas cursar o no estudios universitarios, y qué tan bien o mal les puede ir. Volvemos a la cuestión de la estadística, el resultado que da la máquina no es seguro y no asegura que sea tal como lo predice, intervienen otros muchos factores. Además está la cuestión de la privacidad de los datos. Y, por último, esta tecnología también puede verse como desmotivadora y discriminatoria[86].

Parece que el impacto más positivo de las tecnologías en el derecho a la educación está en la posibilidad de facilitar su acceso, al dar la posibilidad de generar más alternativas que las tradicionales de un profesor y sus alumnos en un aula, ya sea con el *E-learning*, la enseñanza video asistida, la *gamification* que promueve aprendizaje a través del juego, la enseñanza inmersiva a través de realidad virtual, etc. Con lo que sin duda parecería que si se cuidan los aspectos de impacto negativo, puede ser una gran oportunidad para cambiar muchas realidades actuales y hacer llegar la educación a todos los rincones del mundo.

Artículo 27: derecho a la vida cultural, artística y científica

> **1.** Toda persona tiene derecho a tomar parte libremente en la **vida cultural de la comunidad**, a gozar de las artes y a **participar en el progreso científico** y en los beneficios que de él resulten.
>
> **2.** Toda persona tiene derecho a la **protección de los intereses morales y materiales** que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora.

En este derecho se presentan los mismos problemas que en otros artículos: el privilegio o la brecha digital en cuanto a las posibilidades que tienen las personas de usar las TIC como nuevo medio de ejercicio de los derechos, cuando hay muchas regiones en el mundo, incluidas en países con grandes desarrollos económicos y tecnológicos, en donde el simple acceso a internet no es posible.

La discriminación en el acceso a las TIC y en todo tipo de avance tecnológico, es abordada por la Observación General No. 25 (2020) elaborada por el Comité de Derechos Económicos, Sociales y Culturales. En este sentido, el Comité desarrolla el derecho a **gozar de los beneficios del progreso científico** y pone especial énfasis en la obligación de los Estados de eliminar todas las formas de discriminación contra personas y grupos en el disfrute de dicho progreso, con el fin de fomentar la más amplia participación de las poblaciones que tradicionalmente han quedado excluidas del mismo. Cree que habría que prestar especial atención a los grupos que han experimentado una discriminación sistémica en

86 Véase para más información: https://www.zdnet.com/article/should-big-data-be-used-to-discourage-poor-students-from-university/

el disfrute de los mismos, especialmente mujeres, personas con discapacidad, personas del colectivo LGTBI+, pueblos indígenas y personas que viven en la pobreza.

Con respecto a la **relación entre el acceso a las nuevas tecnologías y la pobreza**, el Comité manifiesta que el aumento de la desigualdad económica dificulta el acceso a la educación científica y a los beneficios del progreso científico por las familias de bajos ingresos y por las personas que viven en la pobreza. Esto refuerza, a su vez, la desigualdad económica, puesto que las familias de más altos ingresos disfrutan de mejor educación científica y de acceso a innovaciones científicas, lo que los hace más productivos tecnológicamente y perpetúa y justifica la desigualdad.

Asimismo, como se mencionó al desarrollar el artículo 25 de la DUDH, la Observación General delinea la importancia del acceso al progreso científico como un derecho amplio, que no solo constituye un valor en sí mismo sino que también es un **instrumento esencial para el goce de otros derechos**, como son el acceso a la alimentación adecuada y a la salud.

Partiendo de los aspectos antes citados, parece evidente que la base y gran deuda para poder hablar de impactos positivos de las tecnologías en todos los derechos humanos parte de la efectividad de el derecho que aquí analizamos. Pues solo de esa manera se podría pensar que efectivamente todas las personas vamos a tener oportunidad de gozar de los beneficios del progreso científico, esto es, de las oportunidades que ofrecen las tecnologías para el ejercicio y goce de los derechos humanos.

Superado eso, podríamos entonces sí ocuparnos de los demás impactos positivos y negativos que cada tecnología genera en los derechos humanos reconocidos en la Declaración Universal de los Derechos Humanos. De otra manera parece que la discusión, debate e interés solo es relevante y parte de considerar lo que está pasando en países o ciudades en donde los desarrollos tecnológicos están muy presentes, dejando nuevamente de lado a todas aquellas personas a las que difícilmente les puede afectar algo o todo lo que aquí se ha desarrollado, ya que son totalmente ajenas. Ajenas no por decisión propia, sino por el hecho de que hasta hoy ni siquiera han podido disfrutar de todos los derechos y libertades aquí enumerados en lo que se ha denominado como el mundo *offline*.

Glosario

Glosario

Algoritmo: un algoritmo permite llevar a cabo una tarea o encontrar la solución a un determinado problema a través de un flujo de instrucciones bien definidas y estructuradas, que además deben estar en orden y ser finitas, es decir, tener una solución o varias soluciones posibles. El algoritmo es una serie ordenada de procesos o pasos que deben llevarse a cabo para alcanzar la solución a un problema específico.

Un tipo de algoritmo es el informático, que es el elemento fundamental de cualquier programa de computación, formado por el conjunto de instrucciones y pasos desarrollados para llevar a cabo la tarea encomendada al software[87].

Big data: conjuntos de datos o combinaciones de conjuntos de datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales, tales como bases de datos relacionales y estadísticas convencionales o paquetes de visualización[88].

Blockchain o **cadena de bloques:** es una estructura de datos cuya información se agrupa en conjuntos (bloques) a los que se les añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal. De esta forma, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores[89]. Algunas de las ventajas que se defienden de esta tecnología son que elimina los intermediarios y descentraliza la gestión. En términos de criptomonedas, mediante el *blockchain*, el control del proceso es de las usuarias, no de los bancos[90].

87 Definición extraída de: https://www.tecnologia-informatica.com/algoritmo-definicion/

88 Definición extraída de: https://www.powerdata.es/big-data

89 Definición extraída de: https://es.wikipedia.org/wiki/Cadena_de_bloques

90 Definición extraída de: https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda

Brecha digital: se refiere a la diferencia en el acceso y conocimiento de uso de las nuevas tecnologías. Se determina en base a criterios económicos, geográficos, de género, edad, etc. Hay distintos tipos de brechas digitales: la brecha de acceso, relacionada con las posibilidades de acceso; la brecha de uso, relacionada con la falta de competencias y habilidades para manejar las tecnologías; y la brecha de calidad de uso, relativa a la carencia de conocimientos para hacer un buen uso de las tecnologías[91].

Cookies: se refiere a una porción de información enviada por un sitio web que se almacena en el navegador con el que se accede a esa página web. Por ejemplo, una cookie permite que una web en la que se requiera introducir una cuenta (con usuario y contraseña) para acceder a su contenido, pueda recordar esa información y así evitar tener que introducir usuario y contraseña cada vez que se abre la página web, siempre que se esté usando el mismo navegador.

***Data*:** es una representación simbólica de información en un formato que las máquinas pueden entender. Se genera mediante la información que se cede y se puede utilizar para tomar decisiones, resolver problemas, impulsar la automatización, ejecutar transacciones, entretener, informar, etc.[92] Se trata de una representación simbólica de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo[93].

***Darkweb*:** fragmento de internet al que solo se puede acceder mediante aplicaciones específicas y que provee anonimato a sus usuarios. Es aquella porción de internet que está intencionalmente oculta a los motores de búsqueda, usa direcciones IP enmascaradas y es accesible solo con un navegador especial[94]. La *darkweb* es el contenido que se puede encontrar en diferentes *darknets*, que son cada una de las redes a las que solo puede accederse con programas específicos. Se suele definir como una zona no indexable por buscadores convencionales, lo que quiere decir que no se puede encontrar sus páginas en Google, Yahoo y demás buscadores[95].

91 Definición extraída de: https://protecciondatos-lopd.com/empresas/brecha-digital/

92 Definición extraída de: *Cfr.* https://simplicable.com/new/data

93 Definición extraída de: https://es.wikipedia.org/wiki/Dato

94 Definición extraída de: *Cfr.* https://www.xataka.com/servicios/deep-web-dark-web-darknet-diferencias

95 Definición extraída de: *Cfr.* https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella

***Deep learning*:** forma parte del aprendizaje automático. Se trata de un algoritmo automático que imita la percepción humana inspirada en el cerebro humano y la conexión de neuronas. Es la técnica que más se acerca a la forma en la que aprenden los humanos. Tanto el *deep learning* como el *machine learning* imitan la forma de aprender del cerebro humano. Su principal diferencia es el tipo de algoritmos que usan en cada caso, aunque el *deep learning* se parece más al aprendizaje humano por su funcionamiento como neuronas. El *machine learning* acostumbra a usar árboles de decisión y el *deep learning* redes neuronales, que están más evolucionadas[96].

***Deep web*:** es el contenido de internet que no está indexado por los motores de búsqueda convencionales[97]. Es lo contrario al "internet superficial", es decir, aquella porción de internet que es indexada por los motores de búsqueda y que es accesible para todos. El contenido de la *deep web* se oculta tras formularios web (HTML) e incluye usos muy comunes (correo electrónico, perfiles de redes sociales, páginas web que requieren registro para acceder a su contenido, páginas en las que se ofrece un servicio por el que se tiene que pagar, como diarios o revistas, etc.).

Drones kamikaze o ***lotering munition*:** es una categoría de UAV (vehículo aéreo no tripulado) y de arma, en la que la munición merodea por el área buscando el objetivo y ataca una vez lo ha localizado de forma automática.

***Hardware*:** se refiere al total de los elementos materiales, tangibles, que forman al sistema informático de un dispositivo tecnológico (ordenadores, teléfonos móviles, etc.). Esto se refiere a sus componentes de tipo mecánico, electrónico, eléctrico y periférico, sin considerar los programas y otros elementos digitales, que forman parte del software[98].

***Machine learning*:** método de análisis de datos que automatiza la construcción de modelos analíticos. Es una rama de la inteligencia artificial basada en la idea de que los sistemas pueden aprender de datos, identificar patrones y tomar decisiones con la mínima intervención humana[99].

96 Definición etxraída de: *Cfr.* https://blog.bismart.com/es/diferencia-machine-learning-deep-learning y https://www.xataka.com/robotica-e-ia/deep-learning-que-es-y-por-que-va-a-ser-una-tecnologia-clave-en-el-futuro-de-la-inteligencia-artificial

97 Definición extraída de: https://es.wikipedia.org/wiki/Internet_profunda

98 Definición extraída de: *Cfr.* https://concepto.de/hardware/

99 Definición extraída de: *Cfr.* https://www.sas.com/es_es/insights/analytics/machine-learning.html

Social networking service o ***social media*****:** medio social que permite establecer contacto con otras personas por medio de una plataforma web. Está conformado por un conjunto de equipos, servidores, programas, conductores, transmisores y receptores[100].

Software**:** se refiere a todo componente intangible y no físico que forma parte de dispositivos tecnológicos como los ordenadores, teléfonos móviles, etc. Está compuesto por un conjunto de aplicaciones y programas diseñados para cumplir diversas funciones dentro de un sistema. Además, está formado por la información del usuario y los datos procesados. Los programas que forman parte del *software* le indican al *hardware*, por medio de instrucciones, los pasos a seguir[101].

Tecnologías biométricas: pueden dividirse entre las tecnologías biométricas fisiológicas, esto es, aquellas que tienen en cuenta rasgos estrictamente físicos (huella dactilar, reconocimiento facial, escáner de iris y retina, reconocimiento de la geometría de la mano, etc.), y las tecnologías biométricas del comportamiento, es decir, aquellos sistemas que analizan el comportamiento del usuario en tiempo real y que se basan en identificar rasgos derivados de acciones concretas (patrón de escritura, movimientos físicos, patrones de navegación, etc.)[102].

TIC (tecnologías de la información y la comunicación): son las tecnologías que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no solo de forma aislada, sino lo que es más significativo es que lo hacen de manera interactiva e interconexionada (definición de Julio Cabero Almenara[103]).

Se refiere a todas las tecnologías de la comunicación, incluyendo internet, dispositivos sin cable, teléfonos, ordenadores, software, middleware, video conferencias, redes sociales, y otras aplicaciones y servicios que permiten a los usuarios acceder, almacenar, recuperar, transmitir y manipular información de forma digital[104].

100 Definición extraída de: https://es.wikipedia.org/wiki/Servicio_de_red_social

101 Definición extraída de: *Cfr.* https://concepto.de/software/

102 Definición extraída de: *Cfr.* https://www.widefense.com/recursos/ciberseguridad/tecnologia-biometrica/

103 Definición extraída de: *Cfr.* https://www.uv.es/bellochc/pedagogia/EVA1.pdf

104 Definición extraída de: *Cfr.* http://aims.fao.org/es/information-and-communication-technologies-ict