MEDIOS DIGITALES Y ESTADO DE DERECHO

HARTMUT RANK* Y MIGUEL BARBOZA LÓPEZ**

KONRAD ADENAUER STIFTUNG
ESTADO DE DERECHO · LATINOAMÉRICA

El Estado de derecho (en adelante "EdD"), en términos generales, busca garantizar la igual aplicación de la ley y el respeto de los derechos humanos bajo un marco jurídico establecido por Estados democráticos [1]. En Latinoamérica no existe un consenso amplio de lo que se entiende por EdD – sea conforme a la teoría *thin o thick* – sin embargo, es ampliamente válido el reconocimiento de ciertos elementos que son esenciales para su configuración[2]. Entre estos elementos se destacan la accesibilidad de la ley (inteligente, clara y predecible); el sometimiento a la ley y la no discrecionalidad en la toma de decisiones; la igualdad ante la ley; el ejercicio del poder de forma legal, justa y razonable; la protección de los derechos humanos; la existencia de medios gratuitos para resolver disputas sin dilación; los juicios justos; y el cumplimiento de las obligaciones de derecho internacional como nacional[3].

Las sociedades han avanzado y con ella el uso de la tecnología, el internet y la digitalización masiva de contenidos y procedimientos [4] en adelante "medios digitales") por lo que la garantía del EdD en el campo digital resulta indispensable y a la vez un desafío para los Estados. En este punto es esencial comprender el concepto de "ecosistema digital", que abarca el conjunto de fenómenos industriales y de impacto económico asociados con el despliegue de tecnologías de información y comunicación y más específicamente con Internet. Es decir, el ecosistema digital nos lleva a estudiar la cadena de valor que está detrás de la producción de estos servicios digitales [5], así como la interacción que genera la tecnología entre personas, estados y actores económicos, como las empresas.

Tomando en cuenta dicho concepto existen tres elementos al hablar de medios digitales. El primero es el "medio digital propiamente dicho" que no es más que la tecnología a través de la cual se canaliza, crea o transforma la información, como radios, drones, grabadoras, filmadoras, etc. El segundo es la "producción digital" materializada a través de informaciones plasmadas en publicaciones o productos derivados de los medios digitales; y la tercera, es la "subjetividad digital" que es la intención detrás de la producción digital cuya legalidad puede ser controvertida.

El ecosistema digital y la interacción de los elementos mencionados que forman parte de este generaron diversos desafíos para los Estados a fin de consolidar el EdD y con ella la democracia y el respeto de los derechos humanos. Seis son los puntos que la Fundación Konrad Adenauer (KAS) resaltó como principales problemas que trae consigo la digitalización y que guarda íntima relación con el EdD: el desarrollo de monopolios empresariales en el área de comunicaciones, es decir el poder de innovación está en pocas manos (*Facebook, Google, Amazon, Apple, Alibaba, Baidu*); las restricciones estatales al uso de los medios digitales y su uso para ejercer una vigilancia masiva hacia diversos actores; la recolección de información; la inequidad social y económica en el acceso; la ausencia de normas globales coordinadas entre los Estados para regular el tema; y la capacidad estatal para adaptarse a los nuevos cambios digitales y resolver conflictos relacionados con esta interacción [6].

Importante tener en cuenta que frente a estos desafíos los medios digitales de mayor interacción ya no son aquellos en donde se requiere tener un computador, sino un "teléfono móvil" u otro medio digital, y los operadores principales para el intercambio de información ya no son en mayor medida la televisión o la radiodifusión, sino aplicaciones web en donde cada persona puede recibir información, intercambiar información en tiempo real, y puede ser objeto de control directo sin un gran intermediario digital [7]. Situación que complejiza aún más el garantizar el EdD.

Conforme a lo hasta aquí señalado, la garantía del EdD en el marco de las diferentes dinámicas de interacción digital puede analizarse a través de dos ejes centrales: la política democrática de los estados; y la garantía de los derechos humanos a través de los medios digitales que ha cobrado especial relevancia con la actual situación de pandemia por la Covid-19 [8].

LA POLÍTICA DEMOCRÁTICA DE LOS ESTADOS

El cimiento para el EdD es sin duda un gobierno democrático, sujeto a la ley y que respete la plena garantía y disfrute de los derechos humanos. La voluntad política y la materialización de esta son dos elementos indispensables. Este primer elemento busca que diversos temas de actualidad, como la digitalización sean debidamente abordados y que no exista silencio frente a los desafíos en el uso de la tecnología que se puedan presentar. El segundo elemento, requiere que una política pública- que posteriormente se puede traducir en una ley - no quede en letra muerta, sino que se aplique de forma efectiva en igualdad de condiciones y sin discriminación.

Los gobiernos de los países de América Latina han emitido diversas leyes en materia de gobierno digital y la digitalización en procesos judiciales. Entre estas, la aprobación del Decreto Legislativo No. 1412, por el cual el gobierno peruano aprobó la Ley de Gobierno Digital [9]; la Ley No. 1564 a través de la cual el gobierno de Colombia aprobó el Código General de Proceso que incluye un capítulo sobre el "Plan de Justicia Digital [10]; la Ley No. 20.886 en donde el gobierno de Chile regula la tramitación digital de los procedimientos judiciales [11]; y la aprobación en Ecuador de la "Política Ecuador Digital", que busca, entre uno de sus tantos objetivos, disminuir la brecha digital [12] . En este punto la alerta sobre el cumplimiento del EdD tiene que estar encendida, pues regularmente las nuevas regulaciones en materia digital no guardan coherencia normativa con el resto del paquete de normas sobre transparencia de la información; los códigos de procesos penales, civiles, laborales; y las normas sustantivas de tratamiento de algunos tipos penales, solo por mencionar algunos casos.

Asimismo, se tiene que considerar que la aplicación efectiva de una ley o política demanda diversos esfuerzos, particularmente relevantes en el tema de la digitalización, como la capacitación de funcionarios públicos en temas digitales, la sensibilización en el uso de las tecnologías, la creación de una unidad de supervisión de los servicios digitales, y el acercamiento de la ciudadanía hacia estos medios.

La democracia también demanda el uso correcto de la tecnología a través de la digitalización en asuntos políticos - bilaterales o multilaterales- con diversos Estados. El espionaje a través del uso de drones y de manera virtual, o el jaqueo de repositorios de datos, el chuponeo de llamadas telefónicas, etc., pueden constituirse elementos que pongan en riesgo la soberanía estatal o creen conflictos, incluso armados. Como fue el caso entre China y Estados Unidos, en donde el ex oficial de inteligencia chino *Xu Yanjun*, fue arrestado en Bélgica y extraditado a los Estados Unidos para ser juzgado por un caso de espionaje económico [13]; por otro lado, también se destacan casos en donde diversos estados latinoamericanos han empleado el uso de medios digitales para espiar a sus ciudadanos, como Ecuador, Honduras, Guatemala, Colombia, Chile, México, Panamá y Brasil; así como otros que si bien no concretaron un contrato de espionaje estuvieron a portas de hacerlo, como Paraguay, Argentina, Uruguay y Perú [14]. Por ello, es indispensable que los Estados puedan también, a través de relaciones diplomáticas, regular el uso de las tecnologías a fin de evitar la comisión de ilícitos.

En el caso del uso de drones se cuenta con un referente internacional como es el Convenio de Aviación Civil Internacional, o más conocido como "Convenio de Chicago" de 1944 que establece que las naves que no tengan piloto no podrán traspasar las fronteras de otro Estado sin autorización. Y ello es particularmente importante, pues no sólo se pone en riesgo la estabilidad económica y política de un país a nivel externo en su relación con los demás estados, sino a nivel interno y con ella también la seguridad de sus nacionales. Por ejemplo, se intentó asesinar al gobernante venezolano *Nicolás Maduro* a través de un dron comercial [15], por su parte en Colombia, se prohibió el uso de drones cerca a la Casa de Nariño en la toma de posesión del presidente *Iván Duque* [16]. En este sentido, el liderazgo estatal para regular el uso de drones es trascendental [17], sin embargo, actualmente en Latinoamérica todavía se necesitan reforzarse las pocas normas que existen al respecto, por ejemplo, abordando más el tema de seguridad en el uso de drones en territorio ajeno a la soberanía de un estado [18].

GARANTÍA DE DERECHOS CON UNA PERSPECTIVA PLURAL

Lo medios digitales también exponen las "brechas" y "riesgos" existentes en cuanto a la garantía de derechos humanos con especial impacto a individuos o grupos en situación de vulnerabilidad. La amplitud o restricción en el acceso a medios o servicios digitales de manera voluntaria o no, ha generado diversas situaciones de vulnerabilidad a los derechos humanos que pueden derivarse de la ciberdelincuencia [19]. Así, la era digital ha transformado los medios por los cuales los derechos humanos son ejercidos, y también como podrían llegar a ser vulnerados [20]. Entonces surge la pregunta ¿cómo controlar estos medios digitales a fin de no evocar vulneraciones a los derechos humanos? La respuesta puede centrarse en tres elementos que analizaremos a continuación: a) analizar la no discriminación e igualdad en los medios digitales; b) determinar cuál es el rol de las empresas en los medios digitales para mejorar su supervisión; y c) conocer las actuales vulneraciones a los derechos humanos para identificar los vacíos y ejercer una adecuada acción; esta será la manera de garantizar el EdD.

- La no discriminación y la igualdad en los medios digitales

Las bases de toda protección a los derechos humanos en la era digital son el respeto del derecho a la no discriminación y a la igualdad, ejes que conducen a la garantía de la dignidad humana [21]. Puede desprenderse entonces que el empleo de los medios digitales tiene como principales prioridades el máximo respeto de los derechos humanos, el acceso igualitario a ellos, y el uso justo de estos por parte de funcionarios y/o agencias estatales, así como de actores privados.

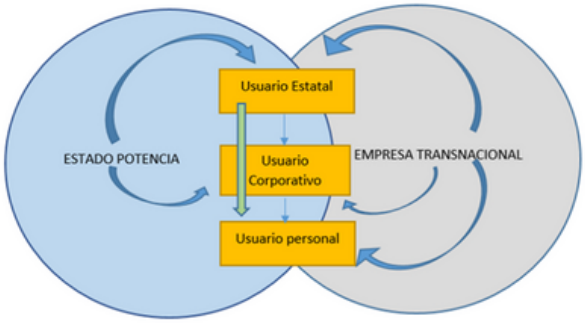
Al hablar de discriminación, podemos destacar las "categorías sospechosas de discriminación" entendidas como aquellas que:

> "(i) se fundan en rasgos permanentes de las personas, de las cuales estas no pueden prescindir por voluntad propia a riesgo de perder su identidad; ii) han estado sometidas, históricamente, a patrones de valoración cultural que tienden a menospreciarlas; y (iii) no constituyen, per se, criterios con base en los cuales sea posible efectuar una distribución o reparto racional y equitativo de bienes, derechos o cargas sociales"[22].

Estas categorías sospechosas implican un deber reforzado por parte de los Estados para supervisar, controlar y erradicar políticas, leyes o prácticas no escritas tendientes a hacer un uso inadecuado de los medios digitales con el fin de fomentar violaciones a los derechos humanos, para lo cual es esencial tener una lectura de las *"vulnerabilidades digitales sospechosas"*. Criterio que incorpora la "discriminación múltiple" y "discriminación interseccional". La primera dirigida a la convergencia de múltiples factores que motivaron la violación, como la pobreza, ser indígena, entre otros; y el segundo factor se refiere a la intersección de estos factores [23].

Al realizar este estudio sobre posibles "vulnerabilidades digitales sospechosas" se puede identificar si una ley o una práctica no fue igualitaria. Ello por considerar superior a un determinado grupo, tratarlo con privilegios o con inferioridad [24]. Las situaciones de desigualdad se pueden analizar considerando el nivel de poder económico y tecnológico con el que cuentan determinados tipos de usuarios digitales, que en este caso puede ser un usuario estatal, un usuario corporativo, o un usuario natural (una persona o grupo de

personas) frente a cualquier usuario afectado que puede ser un usuario personal o incluso una empresa. No obstante, no necesariamente un estado o una empresa nacional (agentes internos) van a estar en una situación de poder pleno con el fin de someter sea a otras empresas nacionales, como a proveedores, o a personas naturales, pues incluso los estados y las empresas pueden llegar a ser sometidos por grandes empresas transnacionales u estados que por su poder dominan en mayor medida ciertos sectores de la económica y de la tecnología (estado potencia). En el caso de las empresas transnacionales incluso los niveles de inferencia frente a sus subsidiarias en un determinado país podrían llegar a tener efectos directos en las personas. La siguiente gráfica ilustra lo señalado.



Fuente: Elaboración propia

- El rol de las empresas y los medios digitales

El EdD también regula la relación entre particulares, como aquellas desarrolladas por compañías de comunicación tales como Facebook, Twitter, Google o Weibo, quienes a través de diversos algoritmos o términos de servicios juegan un rol importante sobre temas vinculados a derechos humanos: medio ambiente, salud, educación, sólo por mencionar algunos ejemplos [25]. Los estados, conforme lo señalan los estándares internacionales, tiene obligaciones respecto a las actividades realizadas por particulares, como las empresas u otro actor económico (nacional o transnacional) debiendo ejercer una adecuada supervisión, control y fiscalización referente al manejo de información, almacenamiento de datos, resolución de casos, entre otros [26]. Democracias débiles traducidas en leyes laxas, poco equitativas y que no se aplican en la práctica podrían ser elementos decisivos para que a través de la digitalización se quiebre el EdD.

En el caso de las empresas, públicas o privadas o de capital mixto, estas también tienen obligaciones que pueden llegar a adoptarse a nivel interno, como mejores prácticas corporativas, incluso si la legislación nacional es menos garantista: abarcado dentro del II Pilar de los Principios Rectores sobre Empresas y Derechos Humanos de Naciones Unidas (en adelante “Principios Rectores”) que versa sobre el deber de respeto.

En el marco de este deber de respeto, las empresas en un contexto digital pueden evaluar y abordar determinados riesgos en su actuar, tal como lo ha señalado el Alto Comisionado de las Naciones Unidas para los Derechos Humanos a través del grupo *B-Tech* [27], entre las que destacamos: compartir largos volúmenes de información; vender productos o asociarse a los gobiernos que buscan emplear nuevas tecnologías para funciones estatales o prestar servicios públicos que podrían poner en riesgo a poblaciones vulnerables; decisiones de marketing que podrían conducir a situaciones de discriminación; usar “jefes algorítmicos” para mediar relaciones laborales entre trabajadores y empresas; proveer tecnología que pueda conducir a violaciones a los derechos humanos; e informar sobre cuestiones personales sin consentimiento previo [28]. Temas a considerar que no configuran una lista cerrada.

Sobre algunos de estos problemas, las personas afectadas tienen el derecho a saber qué información de carácter personal tiene una empresa sobre ellas y de dónde procede o se recibió esa información personal; exigir la eliminación de la información personal que una empresa haya recopilado sobre ellas; optar por no consentir que se venda información personal; y recibir el mismo servicio y precio de una empresa aunque ejerzan sus derechos de privacidad [29].

A fin de evitar cualquiera de estas posibles controversias con personas afectadas e incluso instituciones, las empresas deben desarrollar un proceso de debida diligencia. *Humberto Cantú*, tomando en consideración a los Principios Rectores, señaló cinco fases que se deben seguir en este proceso de debida diligencia: la evaluación de impactos, la integración de resultados, la comunicación con actores interesados, el monitoreo de medidas adoptadas y la participación en procesos de reparación [30]. Leer estos elementos desde una perspectiva digital implica un desarrollo mayor, pues generalmente el análisis de estos elementos puede resultar ambiguo por lo complejo que puede ser el ecosistema digital – antes explicado – destacando también la importancia de la cadena de valor y la cadena de suministro que hay detrás de los productos o servicios digitales.

Las empresas que forman parte del ecosistema digital deben asumir la debida diligencia como un proceso que busque cumplir los derechos humanos por encima de los intereses corporativos, y ver estas normas como obligaciones y no como "ejercicios voluntarios", punto por donde se ha tratado de introducir el tema de *compliance* corporativo [31].

El asegurar un adecuado marco de debida diligencia en los medios digitales ayudaría a promover que estos no sean usados, por ejemplo, para violentar a la mujer, promover el sexismo y los estereotipos de género [32] y otras vulnerabilidades asociadas a otros grupos en situación de vulnerabilidad particularmente relacionados a la limitación al derecho a la libertad de expresión. Pues generalmente no son conocidas las acciones que toman las plataformas web para ejercer una debida diligencia. No obstante, observamos algunos avances por parte de iniciativas corporativas como la adoptada por Facebook a través del "*Oversight Board*" o Consejo Asesor de Contenido el cual se creó para analizar situaciones en donde puede verse vulnerado el derecho a la libertad de expresión en relación al contenido de *Facebook e Instagram* [33].

¿Múltiples desafíos? Sí, mas es esencial considerar que las empresas son agentes primordialmente importantes para asegurar el EdD en los medios digitales.

- Algunos derechos vulnerados a través del actuar estatal y empresarial

A medida que avanza la tecnología cada vez se evidencian más situaciones de vulnerabilidad en el espacio digital. En el caso del derecho a la libertad de expresión, los diversos medios de comunicación y servicios digitales han tenido un poder amplio para censurar ciertos contenidos (*Twitter, TikTok, Facebook,* ahora *Meta*) sin un previo análisis de proporcionalidad (legalidad, necesidad, idoneidad y proporcionalidad en sentido estricto) y una perspectiva sistémica digital, que implica evaluar una restricción no sólo desde una perspectiva particular del impacto, sino de la perspectiva del impacto en el funcionamiento de la red y del conjunto de usuarios [34].

Asimismo, amparado bajo la libertad de expresión, encontramos también el derecho a buscar, recibir y difundir información [35], a través de medios digitales. Este derecho se ha visto restringido al ser muchas veces usado para transmitir información de manera engañosa induciendo en error a la población [36]. A esto se suman tendencias globales a limitar el uso de redes sociales como *Twitter y Youtbe* [37], o el control absoluto de internet [38], situaciones que no podemos dejar de analizar al poder también presentarse en América Latina.

La protesta social ha sido una de ellas, por ejemplo, en las últimas manifestaciones ocurridas en Colombia en 2021, la Fundación para la Libertad de Prensa (FLIP) denunció que los medios de comunicación no recibían información importante y de coyuntura por parte de instituciones estatales respecto a lo ocurrido en pleno estallido nacional [39]. Sin cuya información no era posible fomentar la democracia en los estados a través del análisis libre de la data, sino que por el contrario con la limitada información muchas veces se ha estigmatizado y criminalizado a los ciudadanos que ejercen su derecho a la protesta pacífica. Misma situación de limitación que

puede poner en riesgo otro cúmulo de derechos.

También, se observa que diversos agentes estatales han reprimido el derecho de las personas a informar libremente sobre algún acontecimiento, como las diversas protestas o manifestaciones a través de la transmisión en vivo de los acontecimientos o la publicación de fotos en sus redes sociales. Esto a través del *Ciberpatrullaje* en denominas circunstancias que han sido calificadas como *Ciberterrorismo* [40]. Esto sin dejar de lado el derecho de las personas a recibir información en un lenguaje sencillo y a través de medios digitales que sean amigables tanto en procesos judiciales, en procedimientos administrativos, como en cualquier información que el Estado o las empresas les proporcionen.

Por otro lado, los procesos electorales también se vieron gravemente impactados por el avance tecnológico. La utilización de inteligencia artificial en el lenguaje de datos ha sido cuestionada en cuanto a su esfera de "legalidad" e "idoneidad" al denunciarse fraude y al no tener un control adecuado por parte de organismos estatales [41]. Por ejemplo, *Smartic*, la empresa que estuvo a cargo del sistema de votación de Venezuela por muchos años [42], denunció a través de su director ejecutivo, Antonio Mugia, fraude en los comicios de la constituyente. Señaló que *"Nuestro sistema automatizado está diseñado para evidenciar cualquier manipulación, pero deben existir personas observando el sistema y esperando por esas evidencias: los auditores"* [43]. Entonces es indispensable que los sistemas de inteligencia artificial no sean usados sin una supervisión directa por parte de personas humanas [44]. Por otro lado, en las comisiones electorales, es muy importante ejercer un parámetro de "valoración-acción" respecto a si todos electores cuentan con sistemas digitales de votación, de no hacerlo es esencial que se aseguren los medios para hacerlo y se respeten las particularidades de cada grupo.

El derecho a la privacidad, guarda estrecha relación con el derecho a la libertad de expresión e información. La *International Federation of Library Associations and Institutions* señaló que "el derecho a la privacidad en la era digital es amenazado agresivamente por la automatización de la información [45]. Cobra especial relevancia entonces que las empresas de comunicaciones y los Estados cuenten previamente con la autorización de las personas o colectivos para poder almacenar, procesar y difundir su información. Por ejemplo, en el caso de los proveedores de servicios de comunicaciones, el *Tribunal de Justicia de la Unión Europea* señaló que no deben conservar información de sus usuarios sin previo consentimiento. Del mismo modo enfatizó que no se justifica que exista una ley general que establezca la conservación generalizada e indiferenciada de los datos de tráfico y localización [46]. En estos casos debe existir un riguroso test de proporcionalidad garantizándose la máxima divulgación [47]. Este aspecto hoy en día está fuera de control, pues en diversas aplicaciones digitales es común observar mensajes que requieren aceptar los términos y condiciones que por lo general no se leen o cuya advertencia no es clara respecto a la autorización de datos. Por otro lado, pareciera que viviéramos en un "ambiente digital intrusivo", pues los historiales de búsqueda rastrean información que puede ser de nuestro interés cuando buscamos algún contenido o permanecemos largo tiempo en un determinado producto o servicio digital, en donde, a diferencia de los teléfonos electrónicos, suelen tener salvaguardas menos estrictas [48].

Ligado a lo anteriormente abordado sobre el derecho a la protesta o manifestaciones pacíficas, el derecho a la privacidad en estos contextos es particularmente invadido, como por ejemplo el rastreo de celulares [49] y/o el chuponeo de las comunicaciones, sumado también al discurso de odio que pueden emplearse en redes sociales [50]. Fuera del ámbito de la protesta, no puede dejarse de lado la consideración a los grupos en especial situación de vulnerabilidad, quienes por lo general sufren desde dos frentes y se desenvuelven en dos escenarios, uno "ataques físicos" y otro "ataques digitales" o violencia digital [51].

Entre estos grupos podemos destacar a quienes son discriminados o marginados por motivos de género [52], personas con discapacidad [53], niños, niñas y adolescentes [54], personas adulto mayores, personas privadas de libertad, pueblos indígenas, entre

otros. En todos estos casos las vulneraciones cometidas por medios digitales son diferenciadas y responden a escenarios distintos. Por ejemplo, no será lo mismo analizar un ataque digital en un contexto de paz que en un contexto de conflicto, misma postura que se presenta en estados bajo un régimen dictatorial. En este escenario el barómetro del EdD en el caso de grupos en situación de vulnerabilidad en contextos digitales tiene que medirse tomando en cuenta los siguientes elementos: a) la coherencia normativa y política relacionada al grupo en situación de vulnerabilidad y el desarrollo tecnológico; b) la efectividad de las políticas y normas en la materia, medida a través de los roles de supervisión y fiscalización de las autoridades estatales; c) la posibilidad de acudir a un proceso judicial independiente, imparcial, e idóneo en temas sobre medios digitales; d) la especialización de la normativa y sus protocolos para internalizar las situaciones particulares de los grupos en situación de vulnerabilidad a los entornos digitales; y e) la receptividad y respuesta de los grupos ante el desarrollo tecnológico.

Citando particularmente la situación de los pueblos indígenas, resaltamos que es esencial reconocer la soberanía inherente de estos respecto a los datos que les conciernen o que se recaben de ellos, y que guarden relación con sus sistemas de conocimientos, sus costumbres o sus territorios [55]. Generalmente, los datos y la infraestructura de datos existentes no reconocen ni dan prioridad a los conocimientos y las cosmovisiones indígenas, ni satisfacen las necesidades actuales y futuras de los pueblos indígenas en materia de datos [56].

En cuanto al derecho a la educación, las escuelas se han vuelto un medio para conducir la gran revolución digital en materia educativa. La información ahora puede llegar a ser más accesible y amplia, no obstante, también se necesita un mayor control sobre información errada o imprecisa. La educación a través de medios digitales también pone de manifiesto el reto de "igualar desigualdades digitales". Particularmente en casos de personas en situación de discapacidad y en el caso de pueblos indígenas, último caso en donde no sólo hay que tomar criterios de acceso a servicios básicos como la electricidad, o el uso de medios electrónicos, sino también el tomar en cuenta "la interculturalidad" en la forma de transmitir el conocimiento. Para *Juana Sales*, indígena guatemalteca *Maya Man*, en relación al contexto del Covid-19, "los Estados habrían obligado indirectamente a los pueblos a comprar nueva tecnología que con anterioridad no utilizaban" [57].

En materia de salud, los datos producidos se consignan y usan de infinitas formas, con o sin el consentimiento del interesado [58], no respetando la información personal de los pacientes en todos los casos [59]. Resulta interesante que los algoritmos médicos que a través de programas o medios informáticos se utilizan para facilitar la adopción de decisiones sobre la salud o el análisis de la información sobre la salud puedan requerir la intervención humana o carecer de ella [60]. Este último aspecto tiene que ser analizado cuidadosamente dado que la manipulación de información médica sin el control humano podría llevar a cabo determinadas imprecisiones y generar la responsabilidad estatal por omisión u acción. En otro aspecto, no menos importante, el rastreo y seguimiento de ciudadanos a través de medios tecnológicos para la gestión de las emergencias de salud pública, como la Covid-19 resulta ser un factor interesante, sin embargo, preocupa el uso de la tecnología y el grado de intromisión y control al que se pueden someter las personas en casos de escaso efecto en la salud pública [61].

Por su parte, el trabajo en la era digital también ha sido y continúa siendo un desafío, especialmente en tiempos de Covid. En espacios completamente digitales se observa un mayor número de horas dedicadas por los empleados, así como una alta demanda de teletrabajo a través de medios digitales distintos al computador, como celulares, tabletas electrónicas, relojes inteligentes, solo por mencionar algunos ejemplos. Esto ha demandado que en la actualidad países como Chile [62] y Perú [63] hayan regulado el trabajo a distancia y el teletrabajo, y que Colombia recientemente haya aprobada una ley para la desconexión laboral [64]. Un aspecto fundamental que ha sido advertido por la Organización Internacional de Trabajo es que, en el contexto del Covid-19, menos mujeres que hombres recuperarían su empleo [65], sumado al acoso laboral y de género que muchos trabajadores y trabajadoras han sufrido [66].

Habiendo hecho una pequeña reseña de aquellas vulnerabilidades que se podrían generar con los medios digitales, no se debe dejar de lado aquel derecho que es el canalizador de las problemáticas digitales por parte de las personas hacia las autoridades estatales: el derecho al acceso a la justicia. Este derecho en un escenario donde versan asuntos digitales debe cumplir con todas las garantías judiciales y el adecuado acceso a recursos judiciales establecidos convencionalmente [67]. Es decir, los recursos judiciales deben realizarse en un tiempo razonable, asegurar el derecho de las víctimas y familiares a conocer la verdad, e investigar, juzgar y en su caso sancionar a los eventuales responsables [68]. Adicionalmente a estas garantías se debe promover el uso de tecnologías de información a distancia, por ejemplo, video conferencias; facilitar la interconexión de las bases de datos y los registros nacionales; fomentar el uso de canales de transmisión electrónica segura entre autoridades competentes [69]; capacitar a funcionarios estatales de todos los niveles [70]; y acercar los medios digitales a las personas. Las lecturas de las garantías judiciales frente a la tecnología deberán tener en cuenta las vulnerabilidades de todos los grupos sociales tanto en su esfera personal (pertenencia a un grupo), así como las condiciones sociales y políticas en las que se desarrollan.

Ahora bien, la digitalización hay que verla también teniendo en cuenta los desafíos que aún diversos países de Latinoamérica presentan por la cantidad de expedientes físicos que existen en diversos procesos judiciales y que no se han digitalizado. Del mismo modo debe evaluarse hasta qué punto la tecnología pueda ser empleada para resolver asuntos procesales, como, por ejemplo, el realizar una pericia antropológica o cultural en el caso de los pueblos indígenas, en donde no es posible razonar sobre una realidad que necesita de la intervención humana.

Por otro lado, en cuanto a la justicia penal que se realice en entornos digitales debe evitarse interferencias con los derechos a la defensa, incluidos el derecho a la asistencia del letrado y a examinar también pruebas materiales. Esto implica que lo digital no debe ser tampoco un obstáculo para acceder a la justicia de manera presencial, especialmente cuando no se tiene todo el sistema de justicia debidamente adecuado a un entorno digital.

CONCLUSIÓN

Latinoamérica es una región diversa y plural incluso cuando se habla sobre medios digitales. El presente texto buscó hacer una primera pincelada o aproximación a este tema y vincular el desarrollo de los medios digitales y su aplicación con el EdD.
Como se pude observar existen dos grandes esfuerzos que deben tener en cuenta los Estados para hacer compatible los medios digitales con el EdD como es regular su política democrática y garantizar los derechos vinculados desde una perspectiva plural. Último punto que a su vez tiene que tomar en cuenta el respeto a la igualdad y a la no discriminación, el rol importante de las empresas inmersas en los medios digitales, y los diversos escenarios de vulnerabilidad que los entornos digitales pueden generar a los derechos humanos.

Los retos para garantizar los medios digitales en conformidad con el EdD son múltiples, esto nos conduce a ponerse diversas gafas para asegurarlo. Unas primeras gafas son relacionadas a lo digital, que permita revelar lo ya complejo que es este; unas segundas gafas jurídicas, que permitan analizar los actuales desarrollos nacionales e internacionales desde una perspectiva interseccional para garantizar los derechos humanos de todos los usuarios digitales; y unas gafas técnicas, basado en la asesoría técnica de ingenieros, y expertos en las áreas de las ciencias digitales a fin de entender mejor las problemáticas y avanzar en el tema.

Finalmente, resaltamos que el rol de la academia, la sociedad civil, las empresas y los Estados es esencial. Mencionamos en este punto a las empresas y a los Estados pues también estos actores pueden realizar buenas prácticas corporativas o iniciativas que coadyuven a mejorar una situación de conflicto en los medios digitales. Por su parte la sociedad civil y la academia, pueden ejercer presión para avanzar con las discusiones y asegurar la no impunidad en ciertos casos, fortaleciendo así la democracia desde diversos y múltiples frentes.

REFERENCIAS:

* Director del Programa Estado de Derecho para Latinoamérica de la Fundación Konrad Adenauer

** Coordinador de Proyectos del Programa Estado de Derecho para Latinoamérica de la Fundación Konrad Adenauer

[1] Puede verse el concepto de Tom Bingham sobre Estado de derecho en Bingham, Tom (2010). *El Estado de Derecho*, Ed. Tirant Lo Blanch.

[2] Algunos países de la región entienden el Estado de derecho de diferente manera en sus constituciones políticas. Brasil lo denomina "Estado de derecho Democrático" (artículo 1); Perú, "Estado Democrático de Derecho" (artículo 3); Colombia, "Estado Social de Derecho" (artículo 1); Paraguay, "Estado Social de Derecho (artículo 1); Venezuela "Estado Democrático y Social de Derecho" (artículo 2); República Dominicana, "Estado Social y Democrático de Derecho" (artículo 7); Ecuador, "Estado Constitucional de Derechos y Justicia Social (artículo 1); y Bolivia, "Estado Unitario Social de Derecho Plurinacional Comunitario (artículo 1). Países como Honduras, Guatemala, El Salvador, Costa Rica y Nicaragua no mención Estado de derecho en sus constituciones.

[3] Comisión Europea para la Democracia a través del Derecho. (2011). *Reporte sobre el Estado de Derecho*. Adoptado por la Comisión de Venecia en su 86ª sesión plenaria, Venecia, pp. 25-26 de marzo de 2011, párr. 37. Disponible en: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2011)003rev-spa.

[4] La Relatoría Especial para la Libertad de Expresión de la CIDH ha señalado que la digitalización "permite la convergencia de contenidos y plataformas a través de múltiples tipos de redes, sean el espectro radioeléctrico, cables ópticos o emisiones satelitales. Ver. Comisión Interamericana de Derechos Humanos (CIDH). Comunicado de Prensa. *Libertad de Expresión, diversidad, pluralismo e inclusión de nuevas voces en la televisión digital*. 21 de mayo de 2015.

[5] Comisión Económica para América Latina y el Caribe & Banco de Desarrollo de América Latina. (2020). *El Ecosistema y la Economía Digital en América Latina*, 2015, pp. 5 y 6. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/38916/1/ecosistema_digital_AL.pdf. También ver: Comisión Económica para América Latina y el Caribe. (2020). *Las oportunidades de la digitalización en América Latina frente al Covid-19,* 2020, p. 2. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/45360/4/OportDigitalizaCovid-19_es.pdf.

[6] Ver: Fundación Konrad Adenauer & Lee Kuan Yew. (2019). *The Future of Digitalisation. Workshop Report,* Phnom Penh, March 4 -6, 2019.

[7] Fundación para la Libertad de Prensa. (2021). *En vivo: de la calle a la pantalla. Medios Digitales, redes sociales y protesta social,* p. 7. Disponible en: https://www.flip.org.co/images/FLIP_C.E._Medios_paro_2021-V.2.pdf

[8] Por ejemplo, a nivel de la Unión Europea se ha reconocido la importancia de la transformación digital para un mejor acceso a la justicia, lo cual recobró especial importancia durante la COVID-19. Ver. Comisión Europea (2020). L*a digitalización de la justicia en la UE: Un abanico de oportunidades.* Disponible en: https://op.europa.eu/en/publication-detail/-/publication/b94fc82c-3588-11eb-b27b-01aa75ed71a1/language-es/format-PDF/source-search

[9] Perú (2012). Decreto Legislativo 1412 "Ley de Gobierno Digital", 2018. Disponible en: https://www.gob.pe/institucion/pcm/normas-legales/289706-1412

[10] Colombia. Ley No, 1564 "Código General del Proceso", 2012. Disponible en: https://riu.austral.edu.ar/bitstream/handle/123456789/1574/Justicia%20digital%20en%20Colombia.pdf?sequence=1

[11] Chile. Ley No. 20.886 "Tramitación Digital de Procedimientos Judiciales", 2016. Disponible en: http://tramitacionelectronica.pjud.cl/2016/04/25/ley-de-tramitacion/

[12] Ecuador. (2019). Política Ecuador Digital, 2019. Disponible en: http://www.pge.gob.ec/images/documentos/LeyTransparencia/2019/octubre/a2/politica_ecuador_digital.pdf

[13] Deutsche Welle. (2021). *Tribunal EE.UU. condena a agente chino por espionaje económico,* 6 de noviembre de 2021. Disponible en: https://www.dw.com/es/tribunal-eeuu-condena-a-agente-chino-por-espionaje-econ%C3%B3mico/a-59738981

[14] Deutsche Welle. (2016). *Espionaje digital: una práctica común en América Latina*, 04 de mayo de 2016. Disponible en: https://www.dw.com/es/espionaje-digital-una-pr%C3%A1ctica-com%C3%BAn-en-am%C3%A9rica-latina/a-19237204

[15] Ver: El Comercio Perú. *Maduro fue blanco de un intento de asesinato con drones, denuncia el presidente del Parlamento de Venezuela*, 13 de julio de 2021. Disponible en: https://bit.ly/3GcN0Qf

[16] Ver: Deutsche Welle. *Prohiben drones durante acto de posesión de Duque en Colombia*, 2018, Disponible en: https://www.dw.com/es/proh%C3%ADben-drones-durante-acto-de-posesi%C3%B3n-de-duque-en-colombia/a-44978109

[17] Ver: O´Connell & Marie Ellen O´Connell. (2015). *Game of Drones*. 109 American Journal of International Law 889.

[18] Pocos países de Latinoamérica cuentan con legislación que regula el uso de drones, enfocándose más a las autorizaciones que ha situaciones de violaciones de derechos. Ver: México. NOM-107-SCT3-2019. *Que establece los requerimientos para operar un sistema de aeronave piloteada a distancia (RPAS) en el espacio aéreo mexicano.* Disponible en: https://www.sct.gob.mx/transporte-y-medicina-preventiva/aeronautica-civil/3-servicios/35-rpas-drones/; Venezuela. *Enmienda a las Regulaciones Aeronáuticas Venezolanas (RAV)* 5, 21, 39, 45, 47, 60, 67, 91, 130, 141, 273 y 281. Disponible en: http://www.inac.gob.ve/wp-content/uploads/2017/09/Informe-RPA-FINAL.pdf; Colombia. Circular Reglamentaria No. 002. *Requisitos Generales de Aeronavegación y operaciones para RPAS* (Numeral 4,25,8,2). Versión 1. 27 de julio de 2015. Disponible en: https://www.aerocivil.gov.co/servicios-a-la-navegacion/sistema-%20de-aeronaves-pilotadas-a-distancia-rpas-drones/Documents/CR%20Requisitos%20grales.%20de%20Aeronavegabilidad%20y%20Operaciones%20RPAS.pdf; Argentina. Resolución 880/2019. *Reglamento de Vehículos Aéreos No Tripulados (VANT) y Sistemas de Vehículos Aéreos No Tripulados (SVANT).* Disponible en: https://www.marval.com/publicacion/nuevo-reglamento-sobre-el-uso-de-drones-13511; Chile. Ley 18,916 de la Dirección General de Aeronáutica Civil (DGAC). Perú. NTC 001-2015, *sobre la regulación de los drones emitida por la Dirección General de Aeronáutica Civil del Ministerio de Transportes y Comunicaciones.*

[19] Ver: Consejo de Europa (2001). *Convenio sobre la Ciberdelincuencia, Budapest*, 23 de noviembre de 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[20] Human Rights Watch (2016). *So Software Has Eaten the World: What Does it Mean for Human Rights, Security & Governance?* Disponible en: So Software Has Eaten the World: What Does It Mean for Human Rights, Security & Governance? | Human Rights Watch (hrw.org)

[21] La Corte IDH se ha referido a que "La no discriminación, junto con la igualdad ante la ley y la igual protección de la ley a favor de todas las personas, son elementos constitutivos de un principio básico y general relacionado con la protección de los derechos humanos. El elemento de la igualdad es difícil de desligar de la no discriminación". Ver: Corte IDH. *Condición jurídica y derechos de los migrantes indocumentados*. Opinión Consultiva OC-18/03 del 17 de septiembre de 2003. Serie A No. 18, párr. 83.

[22] Corte Constitucional de Colombia. (1998), Sentencia C-481 de 1998, M.P. Alejandro Martínez Caballero.

[23] Ver: Corte Interamericana de Derechos Humanos (2015). *Caso Gonzales Lluy y otros vs. Ecuador*, Sentencia de 1 de septiembre de 2015. Excepciones Preliminares, Fondo, Reparaciones y Costas. Serie C, núm. 298, párr. 290.

[24] Corte Interamericana de Derechos Humanos (1984). *Propuesta de modificación a la Constitución Política de Costa Rica relacionada con la naturalización*. Opinión Consultiva OC4/84 de 19 de enero de 1984. Serie A No. 4, párr. 55.

[25] *Op.Cit*. 18

[26] Pilar I de los Principios Rectores sobre Empresas y Derechos Humanos de Naciones Unidas.

[27] El Grupo B-Tech "proporciona orientación de referencia y recursos para aplicar los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos en la esfera de la tecnología". Ver: https://www.ohchr.org/SP/Issues/Business/Pages/B-TechProject.aspx

[28] Oficinal del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2019). *UN Human Rights Business and Human Rights in Tecnology Project (B-Tech). Applying the UN Guiding Principles on Business and Human Rights to digital tecnologies*. November 2019, p. 5. Disponible en: https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Project_revised_scoping_final.pdf

[29]Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2018). Informe del Relator Especial sobre el derecho a la privacidad. Big Data and Open Data. A/73/439, 17 de octubre de 2018, párr. 83

[30] Cantú Rivera, Humberto. (2018). *Responsabilidad Social, Empresas y Derechos Humanos*. Publicación de la Coordinación para la Atención de los Derechos Humanos del Gobierno del Estado de Oaxaca, 2018, pág. 20.
Disponible en: https://www.oaxaca.gob.mx/cadh/wp-content/uploads/sites/18/2019/02/Responsabilidad_social_empresas_derechos_humanos.pdf

[31] Addo, Michael. (2010). *Is Business and Human Rights Suitable for the Compliance Function?* University of Chicago Law REVIEW Online, 2020. Disponible en: https://lawreviewblog.uchicago.edu/2020/01/07/is-business-and-human-rights-suitable-for-the-compliance-function-by-michael-k-addo/

[32] Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos. (2019). *Informe del Relator Especial sobre el derecho a la privacidad. Privacidad y tecnología desde una perspectiva de género*. A/HRC/40/63, 16 de octubre de 2019, párr. 91.

[33] Para mayor información visitar: https://oversightboard.com/

[34] Comisión Interamericana de Derechos Humanos. (2013). *Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet).* OEA/Ser.L/V/II.149. Doc. 50, 30 de diciembre de 2013, párr. 53.

[35] Comisión Interamericana de Derechos Humanos. (2020). I*nforme Derecho a la información y seguridad nacional.* OEA/Ser.L/V/II, julio 2020, párr. 2.
Disponible en: https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

[36] Ver: Deutscher Bundestag (2018). *Los derechos humanos en la era digital: Estado actual de la investigación y el debate. Tensión fundamental sobe la situación de los derechos humanos en la era digital. Ventajas y Oportunidades.* Disponible en:
https://www.bundestag.de/resource/blob/568306/39edaff23c4b48b1bee67944a169df27/wd-2-107-18-pdf-data.pdf

[37]El gobierno Turco en 2020 aprobó una nueva Ley para regular el uso de redes sociales que cuenten con más de un millón de usuarios diarios en el país. Ver. TRECEBITS. *Turquía amenaza con prohibir Facebook, Twitter y Youtube*, 05 de noviembre de 2020. Disponible en: https://www.trecebits.com/2020/11/05/turquia-amenaza-con-prohibir-facebook-twitter-y-youtube/

[38] En China la oficina de Administración del Cuberespacio obliga a blogeros e influencer a solicitar una credencial al gobierno a fin de poder expresarse sobre una amplia gama de temas. Ver: INFOBAE. *China endurece el control sobre internet: el régimen de Xi Jinpig otorgará credenciales a quienes quieran tener una web*, 17 de febrero de 2021. Disponible en: https://www.infobae.com/america/mundo/2021/02/17/china-endurece-el-control-sobre-internet-el-regimen-de-xi-jinping-otorgara-credenciales-a-quienes-quieran-tener-una-web/

[39] *Op.Cit*. 7

[40] *Ibid*. Por Ciberpatrullaje se entiende el monitoreo de cuentas en redes sociales por parte de la Policía. Por su parte, por Ciberterrorismo, el Ministerio de Defensa de Colombia entiende a este como al "uso de medios de tecnología de información, comunicación y/o informática, con el objetivo de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas"

[41] El País. (2017). *La empresa de gestión electoral de Venezuela denuncia manipulación en los comicios a la constituyente*, 03 de agosto de 2017. Ver: https://elpais.com/internacional/2017/08/02/actualidad/1501678213_523507.html

[42] El País. *La empresa de gestión electoral de Venezuela denuncia manipulación en los comicios a la constituyente,* 03 de agosto de 2017. Ver: https://elpais.com/internacional/2017/08/02/actualidad/1501678213_523507.html

[43] BBC. *Smarti, la empresa a cargo del sistema de votación en Venezuela, denuncia "manipulación" en la elección de la Constituyente y el CNE lo niega*, 02 de agosto de 2017. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-40804551

[44] Consejo de la Unión Europea: *Conclusiones del Consejo "Acceso a la justicia: aprovechar las oportunidades de la digitalización"*. 2020/C 342 I/1. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/836f8ddc-0de5-11eb-bc07-01aa75ed71a1/language-es/format-PDF/source-234222964C

[45] International Federation of Library Associations and Institutions, *The right to privacy in the digital age,* S. 1, Disponible en: https://www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf.

[46] Tribunal de Justicia de la Unión Europea, Tele2 Sverige AB c. *la autoridad sueca de control de los servicios de correos y telecomunicaciones*, sentencia de 21 de diciembre de 2016.

[47] Corte Interamericana de Derechos Humanos. (2006). *Caso Claude Reyes y otros.* Sentencia de 19 de septiembre de 2006. Serie C No. 151. Párr. 92. En el mismo sentido, en la Declaración Conjunta de 2004, los relatores para la libertad de expresión de la ONU, la OEA y la OSCE han explicado que, este principio "establece la presunción de que toda la información es accesible, sujeto solamente a un sistema restringido de excepciones". Disponible en: http://www.cidh.org/relatoria/showarticle.asp?artID=319&lID=2

[48] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2017). Informe del Relator Especial sobre el derecho a la privacidad. *Actividades de Vigilancia Gubernamental*, 06 de septiembre de 2017, Res. A/HRC/34/60, párr. 27

[49] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2019). Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación. Informe sobre *"El Espacio de la sociedad civil, la pobreza, la política nacional y el ejercicio de los derechos a la libertad de reunión pacífica y de asociación"*, 11 de septiembre de 2019, párr. 22

[50] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2017). Informe del Relator Especial sobre el derecho a la privacidad. *Actividades de Vigilancia Gubernamental*, 06 de septiembre de 2017, Res. A/HRC/34/60, párr. 27.

[51] Oficina del Alto Comisionado de Naciones Unidas. (2020). Informe del Relator Especial sobre el Derecho a la Privacidad. *Security and Surveillance, health data, and business enterprises use of personal data*. A/HRC/45/52, 24 de marzo de 2020, párr. 43

[52] *Ibíd*., párr. 55

[53] *Ibíd*. párr. 32

[54] *Ibíd*., párr. 33

[55] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2018). Informe del Relator Especial sobre el derecho a la privacidad. *Big Data and Open Data*. A/73/439, 17 de octubre de 2018, párr. 52

[56] *Ibíd.*, párr. 72

[57] Intervención de Juana Sales, Maya Man y Licenciada en Historia de Guatemala durante el Panel "Pueblos Indígenas, Empresas y Covid 19: retos y oportunidades, 25 de noviembre de 2021, organizado por el Programa Estado de Derecho para Latinoamérica de la KAS y la Universidad de San Carlos de Guatemala, sede de Quetzaltenango.

[58] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2019). Informe del Relator Especial sobre el derecho a la privacidad. *The Protection and Use of Health-Related Data*. A/74/277, 05 de agosto de 2019, párr. 3

[59] El artículo 8 de la *Carta de Derechos Fundamentales de la Unión Europea*, así como el artículo 16 del *"Treaty on the Functioning of the European Union"* han precisa la importancia de la protección de la información personal en cualquier esfera social.

[60] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2019). Informe del Relator Especial sobre el derecho a la privacidad. *The Protection and Use of Health-Related Data*. A/74/277, 05 de agosto de 2019, p. 5

[61] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2020). Informe del Relator Especial sobre el derecho a la privacidad. *Preliminary Evaluation of the privacy dimensions of the coronavirus disease (Covid-19)*, A/75/147. 27 de julio de 2020, párr. 5

[62] Chile. (2020). *Ley No. 21.220 sobre trabajo a Distancia y Teletrabajo* a regir a partir del 1 de abril de 2020, regula el teletrabajo y trabajo a distancia.

[63] Perú. (2020). *Decreto de Urgencia No. 026-2020*, por medio del cual se dispuso el trabajo remoto.

[64] Colombia. (2021). *Ley de Desconexión Laboral*. Disponible en: https://www.eltiempo.com/politica/congreso/aprueban-proyecto-de-ley-que-defiende-derecho-a-la-desconexion-laboral-632729

[65] Organización Internacional del Trabajo. (2021). Menos mujeres que hombres recuperarán el empleo durante la etapa post COVID-19, según la OIT. Disponible en: https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_813643/lang--es/index.htm

[66] Ver: Organización de los Estados Americanos. (2019). *Combatir la violencia en línea contra las mujeres. Un llamado a la protección. White paper series.* Edición 7, 2019. Disponible en: https://www.oas.org/es/sms/cicte/docs/20191125-ESP-White-Paper-7-VIOLENCE-AGAINST-WOMEN.pdf

[67] El artículo 8 y 25 de la Convención Americana sobre Derechos Humanos regula el derecho a las garantías judiciales y a la protección judicial.

[68] Corte Interamericana de Derechos Humanos. (2016). *Caso Tenorio Roca y otros Vs. Perú. Excepciones Preliminares, Fondo, Reparaciones y Costas*. Sentencia de 22 de junio de 2016. Serie C No. 314, párr. 237.

[69] Comisión Europea (2020). *La digitalización de la justicia en la UE: Un abanico de oportunidades.* Disponible en: https://op.europa.eu/en/publication-detail/-/publication/b94fc82c-3588-11eb-b27b-01aa75ed71a1/language-es/format-PDF/source-search

[70] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2017). Informe del Relator Especial sobre el derecho a la privacidad *Actividades de Vigilancia gubernamental*, 06 de septiembre de 2017, Res. A/HRC/34/60, 6 de septiembre de 2017, párr. 28