DERECHO Y TECNOLOGÍA: UNA VISIÓN SINÓPTICA

LAW AND TECHNOLOGY: A SYNOPTIC VIEW

Fernanda García Gómez[*]

Resumen: La revolución digital significa un enorme progreso social, pero, a la vez, demanda respuestas jurídicas eficientes que concilien el fomento a la innovación con el debido resguardo de ciertos principios, derechos y libertades fundamentales. Los desafíos jurídicos actuales se presentan en diversas áreas (propiedad intelectual, bioética, digitalización estatal y ciberseguridad). Es en materia de protección de garantías individuales (privacidad, no discriminación, libertades personal y de expresión) donde se demanda mayor regulación, procurando que ella no ahogue la innovación y el progreso técnico. Las tendencias regulatorias local y comparada ensayan fórmulas normativas de equilibrio, a través de leyes específicas de daños, iniciativas de cooperación público-privada multinacional e interdisciplinaria para la elaboración de principios de conducta, y fórmulas de prueba regulatoria tipo "sandboxes financieros".

Palabras clave: Derecho y tecnología, privacidad, inteligencia artificial, sandboxes.

Abstract: The digital revolution implies an enormous social progress, but at the same time, demands efficient legal responses that reconcile the promotion of innovation with the due protection of fundamental principles, rights and freedoms. Current legal challenges arise in various areas (intellectual property, bioethics, state digitization, and cybersecurity). Protection of civil rights (privacy, non-discrimination, personal freedom and freedom of speech) is the area where legal regulation is most required, procuring that it does not stifle innovation and technical progress. Local and comparative regulatory trends test balanced regulatory formulas, through specific damage laws,

[*] Abogada, Licenciada en Ciencias Jurídicas y Sociales Pontificia Universidad Católica de Chile, Master of Laws (LL.M.) Universidad de Londres. Académica Derecho Comercial Universidad del Desarrollo. Correo electrónico: f.garcia01@udd.cl

multinational and interdisciplinary public-private cooperation initiatives for the development of principles of conduct, and regulatory testing formulae such as "financial sandboxes".

Keywords: Law and technology, privacy, artificial intelligence, sandboxes.

Introducción

El presente trabajo tiene por objetivo revisar el contenido actual de la interacción entre derecho y tecnología[1], esto es, examinar cuáles son las áreas de innovación tecnológica que resultan relevantes para el derecho hoy.

El avance tecnológico ha sido un fenómeno consustancial al desarrollo humano mismo. Sin embargo, existen momentos en la historia en que este ha experimentado fuertes aceleraciones, cambiando radical y definitivamente el modo de vida de las personas a escala global, en un periodo relativamente acotado

Esto ha ocurrido, que duda cabe, con las "nuevas tecnologías", también denominadas "tecnologías de la información y comunicación ("TIC")[2], aparecidas a partir del término de la Segunda Guerra Mundial; y, en especial, con la revolución digital, en curso desde la década de 1970, y que ha tenido un desarrollo vertiginoso durante las primeras dos décadas del siglo xxi. Tan rápidas, profundas, generalizadas e irreversibles son las transformaciones, que las denominaciones con que caracterizamos las estructuras organizativas sociales vigentes a partir del siglo xx se suceden las unas a las otras sin tregua: la Sociedad Industrial dio paso a la Sociedad de la Información, y esta última parece ya superada por la denominada Sociedad Red"[3].

[1] Se define 'tecnología' como el "conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico". Real Academia Española (2020).

[2] Las TIC se caracterizan por el uso de equipos de telecomunicaciones y servidores, es decir, computadoras, para la transmisión, el procesamiento y el almacenamiento de datos

[3] La designación para una estructura organizativa social, desde las perspectivas sociológica e historiográfica, busca destacar los elementos que resultan cruciales para caracterizar la fisonomía de una determinada sociedad, a saber, sus caracteres de organización y funcionamiento económico, tecnológico, político y cultural. Así, la Sociedad Industrial, también llamada Sociedad Moderna o Sociedad de Masas, se refiere a las estructuras sociales presentes en los países occidentales a partir de la Revolución industrial, la que, con la incorporación de fábricas, máquinas y otras tecnologías, buscó maximizar la producción mediante la organización eficiente y en serie de los procesos de trabajo, y el reemplazo progresivo de la mano de obra humana. Se superó así, en un periodo corto de tiempo, a la sociedad preindustrial, premoderna o agraria, que había estado vigente en la humanidad durante siglos. La Sociedad de la

El derecho regula las relaciones de los hombres entre sí y con su entorno, mediante normas y principios cuya observancia es garantizada por el Estado. Como ciencia social, mantiene una íntima e indisoluble conexión con la economía, la política y la historia y, en general, con toda actividad y problemática humana donde surja la necesidad de determinar qué es lo justo, de brindar certeza, de imponer el orden o ambos. De esta forma, el derecho evoluciona de manera permanente, al compás de las transformaciones sociales, y de los desafíos que estas conllevan.

Pero esta relación entre demandas sociales y respuestas jurídicas, no consiste en un flujo unilateral desde la sociedad al derecho, sino que se materializa como un flujo recíproco, como una interacción dual, en la que los hechos mueven al derecho, y el derecho, a su vez, condiciona y moldea los hechos, en un patrón continuo y circular. Así como la variopinta actividad humana cuestiona, moviliza y exige respuestas del derecho, el hombre también se sirve del derecho para orientar, encauzar, restringir o fomentar, los procesos y desafíos que le propone el cambio social, de acuerdo con sus convicciones, conveniencias y necesidades en un momento determinado.

La historia del derecho da cuenta de cómo la ciencia jurídica ha ido transformándose al son de los cambios políticos, económicos, y culturales experimentados por las estructuras sociales. No es de extrañar, entonces, que en el presente, y considerando el impacto de la revolución digital en todos los ámbitos de la actividad humana, exista una sustantiva y creciente demanda social por soluciones jurídicas para las más variadas interrogantes y conflictos generados con ocasión del ejercicio científico. Estas dudas y pleitos se generan de manera simultánea con el avance tecnológico, y se encuentran, la gran mayoría de las veces, con vacíos legales que dificultan o impiden definir lo que es justo o procedente en una situación determinada.

Así, existe una necesidad imperiosa del derecho por conocer exhaustivamente, el estado actual de los avances científicos y tecnológicos, para poder contribuir en la toma de decisiones sociales relevantes para la comu-

Información, también denominada Sociedad Posmoderna, por su parte, se caracteriza por el uso intensivo y sistemático de las TIC, a partir de lo cual se expande y globaliza la interacción de las personas, atenuándose e, incluso, eliminándose los límites y divergencias territoriales y culturales que habían primado en el mundo por siglos. Por último, la Sociedad Red es una organización social esencialmente abierta y transversal (no piramidal desde el punto de vista del ejercicio del poder y del control, como sus antecesoras), construida en torno a vinculaciones personales y corporativas, operadas por redes digitales que se comunican a través de Internet. En cada una de estas denominaciones queda de manifiesto que la preeminencia de ciertos elementos tecnológicos modifica y determina la interacción entre las personas y su entorno, de modo tal que ya no es solo la tecnología la que recibe una denominación o apellido, sino que es la sociedad entera la que se tiñe de ese calificativo.

nidad, y orientar la propia actividad científica y tecnológica dentro de un cauce compatible con su identidad cultural y sus convicciones.

Ya sea para la definición de políticas públicas, el ejercicio de la labor legislativa, la administración de justicia, el desarrollo académico-doctrinario o para el adecuado ejercicio privado de la profesión de abogado, el derecho debe conocer y entender, perfectamente, de qué se está hablando cuando se alude a tal o cual tecnología, y cuáles son los desafíos jurídicos que ella propone.

En el caso del estado actual de la llamada Sociedad Red, la transversalidad y autonomía de los agentes tecnológicos impone, además, un desafío sin precedentes para el derecho, otrora habituado a contar con el poder de imperio estatal como garantía de su observancia. Asimismo, el carácter esencialmente dinámico y muy técnico de la innovación tecnológica en la era digital, impone un deber de prudencia a la hora de normar la actividad científica, no solo para no entorpecer su desarrollo, sino, aun más, para no pecar de ingenuidad e ineficiencia frente a avances ingobernables por normas poco inteligentes o apropiadas.

Entonces, ¿cuáles son las áreas de innovación científica y tecnológica que resultan hoy relevantes para el derecho?

II. Áreas de innovación científica y tecnológica que resultan relevantes para el derecho hoy

A continuación, nos referiremos a las áreas de innovación científica y tecnológica relevantes para el derecho en la actualidad, destacando cuáles son los dilemas jurídicos fundamentales que ellas proponen.

1. Propiedad intelectual

El derecho de propiedad intelectual es la rama del derecho que se ocupa de proteger las creaciones producidas por la mente humana en los campos científicos, literarios, artísticos o industriales, comprendiendo, por lo tanto, al derecho de autor y a la propiedad industrial. Su reconocimiento y protección legal tienen larga data en los ordenamientos jurídicos nacional y comparados, pero, la revolución tecnológica ha traído consigo una serie de desafíos para el ejercicio de esta rama del derecho[4].

[4] El estatuto jurídico de la propiedad intelectual en Chile, cuenta con la protección constitucional de los arts. 19 n.° 25 y 20 de la Constitución Política de la República, y está conformado

Por una parte, los avances tecnológico-digitales han provocado la necesidad de extender, diversificar y profundizar creativamente la protección de los regímenes de derechos de autor y propiedad industrial. Estas exigencias tienen relación con el resguardo de la identidad en línea (marcas y nombres de dominio); la defensa del estatuto de propiedad musical y audiovisual frente a los embates de la digitalización de archivos y la proliferación de plataformas de uso compartido en la red;,y la necesidad de conciliar diversos estatutos internacionales en materia de concesión de propiedades industriales en favor de creadores y desarrolladores de contenido.

Pero así como la digitalización social ha exigido un aumento de la protección jurídica de los derechos de autor y de propiedad industrial, al mismo tiempo, y bajo ciertas circunstancias, ha demandado al derecho reconsiderar e, incluso, atenuar, el énfasis de la protección jurídica que brinda para limitar que el poder monopólico de los titulares de derechos consolidados pueda ahogar la libertad de innovación tecnológica emergente.

En este sentido, es ilustrativo revisar la evolución que ha tenido la aplicación en Estados Unidos de la denominada Ley de Derechos de Autor de la Era Digital (en inglés, Digital Millennium Copyright Act o DMCA)[5]. El propósito original de esta norma, vigente desde 1998, era detener la piratería de los derechos de autor, sin embargo, en la práctica, "las disposiciones anti-elusión han sido invocadas no contra piratas, sino contra consumidores, científicos y la legitima competencia"[6]. En efecto,

> "como la DMCA no contempla un umbral de perjuicios, las disposiciones anti-elusión están abiertas a ser mal usadas por compañías inescrupulosas que ambicionan evitar el pago a sus antiguos empleados o contratistas mediante la revocación de la autorización previamente concedida y alegando enseguida elusión"[7].

Finalmente, el derecho de patentes y de propiedad industrial en particular, se ve interpelado por cuestionamientos y desafíos bioéticos, en lo

por abundante legislación, tratados internacionales y disposiciones reglamentarias, destacando la Leyes n.º 17336, sobre Propiedad Intelectual, n.º 19039, sobre Propiedad Industrial, n.º 20169 que regula la Competencia Desleal, n.º 19223, que tipifica Figuras Penales Relativas a la Informática y n.º 20243 sobre Derechos Morales y Patrimoniales de los Intérpretes de las Ejecuciones Artísticas fijadas en Formato Audiovisual.

[5] La Ley de Derechos de Autor de la Era Digital es la legislación estadounidense sobre derechos de autor, que implementa el Tratado de Derecho de Autor y el Tratado de Actuaciones y Fonogramas, ambos de la Organización Mundial de la Propiedad Intelectual (OMPI), del año 1996.

[6] Electronic Frontier Foundation, E. (2004), p. 18.

[7] *Op. cit.*, p. 35.

relativo a la posibilidad de patentar los resultados y aplicaciones de investigaciones clínicas, farmacológicas y alimentarias, particularmente en relación con el desarrollo de la ingeniería genética[8].

2. *Bioinformática y bioética*

La bioinformática, esto es, la aplicación de la informática y, en general, de la tecnología digital, en el campo de la prestación de servicios de salud, de la investigación en medicina y biotecnología, y de las industrias farmacéutica y alimentaria, ha tenido un impacto transformador en estas disciplinas.

En materia de prestación de servicios médicos y de salud en general, la informática tiene influencia en el aspecto administrativo, en la interacción profesional-paciente, y en el desarrollo de tecnologías de diagnóstico y tratamiento médico.

Desde una perspectiva administrativa, la tecnología ha penetrado en todo el sistema de facturaciones, pagos y reclamaciones, en el entramado operativo de las instituciones de salud públicas y privadas. Lo mismo ha ocurrido respecto de la simplificación en la interacción de los profesionales de la salud con sus pacientes, mediante los sistemas automatizados de agendamiento de horas de atención médica, el mantenimiento de registros y la búsqueda de historiales médicos e, incluso, mediante la atención virtual de pacientes por medio de la telemedicina. La injerencia de la tecnología digital se ha hecho presente también en el desarrollo de tecnologías de diagnóstico y tratamiento médico, a través de muchos dispositivos modernos que hacen uso de dicha tecnología[9].

Todo este acervo de información y registro de datos personales, los que por lo general son, además, de carácter sensible para sus titulares, acarrea dilemas éticos y jurídicos en torno al potencial conflicto entre el derecho a la privacidad de pacientes y sujetos de investigación científica, y los propietarios de las bases de datos científicas y médicas.

El intercambio de datos en el ámbito de la salud promete grandes beneficios, considerando que el acceso a dichos datos es clave para el desarrollo de tecnologías sanitarias. En este sentido, hospitales e instituciones académicas de todo el mundo se muestran cada vez más dispuestas a compartir datos con el sector privado, para cooperar al desarrollo de la tecnología médica. De la misma manera, los servicios de salud públicos contienen millones de registros médicos electrónicos sobre la salud de la población, los que,

[8] Véase infra sección II.2.

[9] La tecnología de imágenes médicas por computadora incluye radiografías, resonancias magnéticas, tomografías computarizadas y ecografías.

aprovechados de manera adecuada, pueden ser utilizados para desarrollar tecnologías que mejoren la atención al paciente. Finalmente, los datos de investigación son también un área clave donde se promueve el intercambio público-privado de datos. El financiamiento se destina a determinados proyectos de investigación bajo la condición de que los resultados de estos se difundan y se compartan con el público.

Sin embargo, el intercambio de datos de salud, la mayoría de los cuales son confidenciales, puede generar variadas cuestiones éticas. Se señala, por ejemplo, que una vez que los datos de salud son compartidos con el sector privado, empleadores o compañías de seguros pueden verse inclinados a desfavorecer a individuos respecto de los que exista información sobre condiciones de salud preexistentes, en el contexto de sus procesos selectivos laborales, coberturas, y decisiones de elegibilidad.

El segundo gran tema en que las nuevas tecnologías han impactado a la medicina y la biotecnología, adicionalmente al del intercambio de datos personales de salud, se refiere a los sistemas automatizados de conteo, rastreo y secuenciación de información molecular y celular. Las computadoras permiten conocer y secuenciar el material genético de moléculas, genes, células y virus, a una velocidad muy superior a la que ofrece el trabajo humano manual, lo que ha significado un impulso sin precedentes para la medicina genética y molecular. También la biotecnología[10], y sus aplicaciones en las industrias sanitario-farmacéutica y alimentaria, se han beneficiado con un vertiginoso desarrollo de fármacos y alimentos, respectivamente, a partir de la eficiencia de estos sistemas automatizados de rastreo de moléculas.

La influencia de la bioinformática en el desarrollo de las medicinas molecular y genética, y de la biotecnología, han causado el planteamiento de importantes problemáticas y cuestionamientos en materia de bioética y, en consecuencia, en el campo del derecho. La bioética puede definirse como el "estudio de los problemas éticos originados por la investigación biológica y sus aplicaciones, como en la ingeniería genética o la clonación"[11]. Así, ella comprende el estudio de los aspectos éticos de las ciencias de la vida (medicina y biología), así como de las relaciones del hombre con los restantes seres vivos (ecología).

El derecho es exigido, en estos respectos, para dirimir dudas y conflictos en cuanto a qué está o no permitido. Los campos de la bioética relativos a la bioinformática, y que han resultado relevantes para el derecho, comprenden, entre otros, el aborto eugenésico; el concepto de calidad de vida, trata-

[10] La RAE define la biotecnología se define como el "empleo de células vivas para la obtención y mejora de productos útiles, como los alimentos y los medicamentos". Real Academia Española (2020).

[11] *Op. cit.* (2020).

mientos paliativos admisibles y eutanasia; la ingeniería genética (incluidas la clonación humana, la donación y el trasplante de órganos, los quimerismos y las investigaciones con células madre); la reproducción asistida y reprogenética; el desarrollo sustentable y los derechos de los animales; las investigaciones y ensayos clínicos y farmacológicos; la nanotecnología y la vida artificial.

Por último, y en lo relativo a la investigación clínica, farmacológica y alimentaria, se generan para el derecho cuestionamientos y desafíos allí donde la bioética se entrecruza con el derecho de patentes y de propiedad industrial en general. Las famosas polémicas jurídicas en torno a la posibilidad de científicos para manipular y patentar formas superiores de vida, como ocurrió con investigadores de la Facultad de Medicina de la Universidad de Harvard a propósito del Oncorratón[12] o los peligros de la investigación científica y las disputas sobre la titularidad de la patente sobre la tecnología CRISPR/Cas9[13], son ejemplos concretos de cómo investigaciones científicas sumamente complejas y técnicas, dotadas de una enorme relevancia social y cultural, demandan de manera intempestiva respuestas de justicia y certeza jurídicas informadas y oportunas.

3. *Garantías constitucionales y tecnología*

El derecho a la privacidad y a la igualdad ante la ley, así como las libertades de expresión y de trabajo, son en la actualidad, amenazados por los profundos

[12] La controversia por la solicitud de patente del Oncorratón o Ratón de Harvard, se produjo en Estados Unidos en 1988. Desarrollado por investigadores de la Facultad de Medicina de la Universidad de Harvard, el Oncorratón es un tipo de ratón de laboratorio modificado genéticamente para ser portador de un gen específico que lo hace desarrollar cáncer de forma rápida, siendo así más apto para ser utilizado en investigaciones científicas sobre esta enfermedad. La invención dio pie a intensos debates políticos para determinar si es aceptable que investigadores pudieran manipular formas superiores de vida e, incluso, patentarlas. En 1988, la Oficina de Patentes y Marcas de Estados Unidos se convirtió en la primera oficina en el mundo en conceder una patente sobre una forma de vida superior.

[13] La tecnología CRISPR-Cas9 es una técnica de edición genética de alta precisión: mediante el uso de "tijeras moleculares" (proteínas Cas), se modifican ADN determinados en humanos y otros seres vivos. La "tijeras" cortan un segmento del ADN, para inactivarlo como para lograr que este se regenere por acción de los mecanismos de reparación de la propia célula. Las aplicaciones de esta técnica se encaminan a reparar genes que provocan dolencias o disfuncionalidades, o enfermedades hereditarias, en humanos y animales, con repercusiones extraordinarias en la biotecnología sanitaria, agrícola e industrial. Sin embargo, ella ha generado disputas sobre el registro de su patente, e importantes debates éticos y regulatorios. Las potenciales aplicaciones de esta tecnología van desde la posibilidad de concebir los denominados "bebés de diseño" bajo un pretexto curativo hasta los desconocidos efectos genéticos reales transmisibles a los descendientes de los organismos intervenidos, y que nadie ha previsto al aplicar la técnica.

cambios y desafíos que conlleva la revolución digital. El derecho, por su parte, intenta encontrar la fórmula para proteger de manera adecuada estas garantías constitucionales, sin que el afán regulatorio implique sofocar la innovación científica, la libre iniciativa económica, la libre competencia en la industria tecnológica y la igualdad de acceso de los usuarios a la red.

¿Qué aspectos del desarrollo tecnológico son las que impactan mayormente a las garantías constitucionales en la actualidad?

1) Intercambio de datos[14]

En los últimos años, se ha consolidado un amplio consenso en cuanto a que los datos, personales y no personales, son un activo comercial valioso, cuyo valor aumenta producto de su intercambio, lo cual supone la promoción de la competencia y la innovación. Sin embargo, paralelamente, se ha profundizado la tendencia regulatoria global respecto de la protección de datos personales.

Intercambio de datos personales.

Los cuestionamientos al intercambio de datos personales se fundamentan en la potencial amenaza que dicho intercambio supone para los derechos a la privacidad, a la igualdad ante la ley y la no discriminación, y a la libertad de trabajo de sus titulares.

Lo anterior queda particularmente de manifiesto, como vimos, en el ámbito de la protección de los datos personales de salud, respecto de potenciales discriminaciones en los procesos selectivos de empleadores y compañías de seguro[15]. Así también se manifiesta en numerosas otras áreas, en relación con datos personales de carácter financiero, raciales o étnicos, de preferencias religiosas, políticas o sexuales, entre otras, de cara a los procesos selectivos de índole laboral, financiero, de seguros, de acceso a educación, etcétera.

[14] El estatuto jurídico de protección a la privacidad en Chile, cuenta con la tutela constitucional de los arts. 19 n.os 4 y 5 y 20 de la Constitución Política de la República (CPR), y está integrado por legislación, tratados internacionales y disposiciones reglamentarias. Las principales normas sobre la materia son la Ley n.º 19628 (1999), sobre Protección de la Vida Privada, y la Ley n.º 19223 (1993), que tipifica Figuras Penales Relativas a la Informática. Existen, además, varias disposiciones que abordan el tema de la privacidad de manera fragmentaria en otros cuerpos normativos. El estatuto jurídico señalado, y en particular, la Ley n.º 19628 está en trámite de ser modificada en el Congreso, mediante el *Boletín* n.º 11 144-0, denominado Proyecto de Ley sobre Ley de Protección de Datos Personales, que busca adecuar el ordenamiento nacional a los estándares de protección integral de la privacidad fijados por el Reglamento Europeo de Datos Personales (2016) y por los Principios de la OCDE sobre Inteligencia Artificial (2019). Véase infra sección 3.2.

[15] Véase supra sección II.2.

El dilema jurídico planteado en materia de protección de datos personales, entre la protección de la privacidad y la igualdad ante la ley, por una parte, y el fomento de la competencia y la innovación, por la otra, tiende a ser abordado mediante legislación que restringe el intercambio de datos[16].

La rigidización de las legislaciones de protección de datos, seguramente, aumentará en los próximos años tanto en Chile como en el ámbito comparado[17], mediante la dictación de regulación tendiente a:

a) restringir la venta y otras formas de intercambio de datos personales, lo que favorece la concentración del poder de mercado y la reducción de la competencia;
b) cuestionar los modelos de monetización de datos[18], resultando en menos servicios gratuitos en línea, y ralentizando en consecuencia, la innovación en TIC;
c) aumentar, a escala internacional, los requisitos de localización de datos, y las restricciones al intercambio de datos transfronterizos, socavando el potencial de las tecnologías de computación en la nube y
d) limitar las excepciones existentes a favor de los datos "desidentificados" o "anonimizados"[19], a la luz de las amenazas de reidentificación.

Este endurecimiento normativo aumenta de modo efectivo el resguardo de la privacidad, pero conlleva consecuencias que afectan otras garantías y bienes jurídicos, tales como la libre competencia, la innovación científica y la igualdad de condiciones para el acceso a la red, toda vez que los beneficios comunitarios derivados de los progresos científico-tecnológicos se generan a partir de la recopilación, el uso y, sobre todo, el intercambio de datos entre gobiernos, empresas y otras organizaciones.

---

[16] Otra técnica jurídica propuesta para aumentar el resguardo de los datos personales consiste en constitución de derechos de propiedad sobre los datos personales, o "propietarización" de datos. Sin embargo, este mecanismo no parece eficaz como segunda herramienta jurídica para aumentar la protección de la privacidad, además de apartarse de la naturaleza jurídica real existente entre las personas y sus datos personales. Siendo la facultad de disposición el núcleo de los regímenes de propiedad, resulta evidente que la concesión de derechos de propiedad a individuos (no entidades), respecto de sus datos personales originarios, constituiría una amenaza directa a la privacidad, información y libertad que se pretende resguardar, a partir del momento en que el individuo dispone de sus datos a favor de un tercero.

[17] *Boletín* n.° 11 144-0: Proyecto de Ley sobre Protección de Datos Personales. Véase supra nota 15.

[18] La monetización de datos consiste en el uso de activos de datos para generar y obtener valor para una organización.

[19] La anonimización es una técnica de tratamiento de datos que elimina o modifica los datos personales identificables para obtener datos anónimos que no se pueden asociar con ninguna persona. Las normas de protección de datos contienen excepciones a favor del intercambio de bases de datos anonimizadas, las cuales podrían ser limitadas por legislaciones más estrictas.

A este respecto, se ha planteado que una política pública adecuada, debe sopesar ambos polos jurídicos –privacidad e innovación– logrando un equilibrio mediante la formulación de leyes específicas de daños, que eviten la sobrerregulación del procesamiento de datos y la creación de derechos de propiedad sobre ellos. Así, si existe preocupación respecto de la discriminación por parte de empleadores, compañías de seguros, establecimientos crediticios, educacionales, etc., entonces la legislación debe contemplar normas que prohíban y sancionen dicha discriminación, y no necesariamente centrarse en prohibir o restringir el procesamiento de datos personales.

Intercambio de datos no personales

Comprensiblemente, la protección de datos personales tiende a ocupar gran parte del quehacer jurídico en materia de privacidad, pero, en los últimos años, tanto el sector privado como el público se han centrado también en cómo obtener valor de los conjuntos de datos no personales.

Entre los ejemplos específicos de datos no personales considerados valiosos, se encuentran los conjuntos de datos agregados y anonimizados utilizados para análisis de información a gran escala, los datos sobre agricultura de precisión que pueden ayudar a controlar y optimizar la utilización de plaguicidas y de agua, o los datos sobre las necesidades de mantenimiento de máquinas industriales[20]. Otros ejemplos de datos no personales que resultan de interés para el intercambio transnacional se refieren a informaciones climáticas, oceanográficas, observaciones urbanas y rurales, y otros datos comerciales y gubernamentales.

Existen, respecto del intercambio de datos no personales, preguntas legales en relación con los flujos de datos que trascienden las fronteras jurisdiccionales de los países individuales, la concentración desigual del control de datos entre naciones, y las dificultades de los países en desarrollo para beneficiarse de la digitalización de la economía global.

¿Debieran regularse los flujos transnacionales de datos no personales? Y, de ser así, ¿cómo debería estructurarse el intercambio de tales datos entre los diferentes actores en el ámbito global? Las organizaciones internacionales (Organización de Naciones Unidas, Banco Mundial, Grupo Intergubernamental de Expertos sobre el Cambio Climático, etc.) recopilan y almacenan grandes cantidades de datos, pero afirman ser soberanas respecto de las leyes nacionales y convenios multilaterales. Considerando lo anterior, ¿qué normativas y políticas públicas debieran regir su recopilación y uso de datos? ¿Cuál es el papel de la infraestructura digital transnacional (cables,

[20] Reglamento (UE) 2018/1807, cons. n.º 9.

satélites, centros de datos, computación en la nube, etc.) para habilitar o restringir los flujos de datos? ¿Quién y cómo debe determinarse la normativa destinada a regir ciertas infraestructuras digitales que proyectan efectos regulatorios considerables en el contexto transnacional, como el *software* de código abierto, Internet y la computación en la nube?

Actualmente, y salvo contadas excepciones[21], no existe normativa específica sobre el intercambio de datos no personales. En general, las barreras para el intercambio de este tipo de datos tienden a no ser de carácter regulatorio, sino de índole cultural o, bien, derivados de inquietudes con respecto a la protección de la propiedad intelectual, la ley de competencia o a restricciones técnicas y comerciales.

2) Inteligencia artificial

Podemos definir la Inteligencia artificial (IA), como la

> "disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico"[22].

En otras palabras, y para las ciencias de la computación, es "inteligente" aquella máquina que percibe su entorno y lleva a cabo acciones flexibles y adaptativas, para maximizar las posibilidades de logro de algún objetivo o tarea[23].

El pilar fundamental de la IA, es entonces, el "aprendizaje automático" (en inglés, machine learning), disciplina científica que crea sistemas capaces de identificar patrones complejos en millones de datos. La máquina que en realidad aprende es un algoritmo que revisa una cantidad potencialmente infinita de datos, y es capaz de predecir comportamientos futuros. Automáticamente, también en este contexto, implica que estos sistemas se mejoran de forma autónoma con el tiempo, sin intervención humana.

Las implicaciones sociales de la inteligencia artificial y de sus aplicaciones concretas son profundas, y su capacidad para modificar el modo y calidad de vida de las personas es infinita. Sin embargo, y al mismo tiempo, ellas suponen riesgos para la privacidad, la libertad personal, la libertad de trabajo, la igualdad ante la ley y la seguridad nacional.

---

[21] Reglamento (UE) 2018/1807.

[22] Real Academia Española (2020).

[23] "¿Qué diferencia a la IA respecto de las TIC convencionales? Las TIC se basan en la organización de tareas rutinarias ya definidas para algún proceso o tarea productiva, mientras que la IA se centra en la automatización de tareas complejas que requieren aprendizaje para enfrentar nuevos desafíos.

IA y privacidad, libertad personal y de expresión, y derecho de reunión

Son varias las aplicaciones de IA existentes y proyectadas que pueden llegar a afectar la privacidad y la libertad personal. Ejemplos de estas aplicaciones, que se utilizan para la solución de problemas de alta complejidad sobre la base de mecanismos predictivos de resultado, son las denominadas "ciudades inteligentes" y "vehículos automatizados" (en inglés, Smart Cities y Autonomous Vehicles, respectivamente)[24]. Pero quizá el ejemplo de IA que ha estado más presente en el debate público reciente, ha sido el de la tecnología de reconocimiento facial (TRF), que permite variadas utilizaciones en el ámbito público y privado.

En el sector público, esta tecnología esta siendo empleada a escala mundial por organismos de inteligencia y de justicia para combatir el terrorismo con mayor eficacia. La policía, por su parte, está construyendo bases integrales de datos biométricos faciales contra los cuales contrastar sospechosos. Asimismo, la TRF está siendo utilizada para acelerar autorizaciones de inmigración para viajeros, para identificar de manera eficiente a autores de suplantaciones y de otros fraudes de identidad, y para encontrar personas desaparecidas.

Pero los usos de la TRF no se limitan al ámbito de la administración de justicia y de la labor policial. Los casos de uso privado de la tecnología de reconocimiento facial son múltiples y abarcan la totalidad de los rubros e industrias. Para enumerar algunos, la TRF puede ayudar a identificar trastornos genéticos raros, mejorar la accesibilidad y la comunicación para personas no videntes, monitorear el desplazamiento y asistencia escolar y laboral, controlar el acceso a áreas seguras, mejorar la publicidad comercial individualizada, validar la identidad en cajeros automáticos y desbloquear teléfonos inteligentes.

Si bien son numerosos los beneficios sociales a partir del uso de esta tecnología, ella también es vista como un potencial riesgo para los derechos humanos y las libertades civiles, alimentando un acalorado debate sobre cómo imponer límites para su uso responsable.

Los cuestionamientos al uso de la TRF, tanto en el sector público como en el privado, se presentan en torno a la ética de los perfiles creados a partir esta tecnología y las posiciones al respecto se debaten entre si debiera

[24] La "ciudad inteligente" es aquella capaz de utilizar las TIC con el objetivo de crear mejores infraestructuras para los ciudadanos como, por ejemplo, en materia de transporte público, ahorro energético, sostenibilidad, etc. Los "vehículos autónomos" o "robóticos", son aquellos que se movilizan sin conductor, siendo capaces de percibir el medio que le rodea y navegar en consecuencia.

permitirse en absoluto el uso de la TRF en una sociedad democrática o, por el contrario, permitirse solo con importantes restricciones y salvaguardas a las garantías de las personas. Mientras son muchos los que sostienen que la TRF mejora de forma exponencial la eficacia en el resguardo de la seguridad pública, y constituye una ayuda invaluable en la lucha contra el crimen organizado y el terrorismo; sus opositores destacan que ella conlleva riesgos significativos para las garantías individuales.

Entre dichos riesgos, se señala que la TRF tiene el potencial de posibilitar de manera masiva invisible, e indiscriminada, la vigilancia de personas en espacios públicos, bajo el pretexto de mejorar los estándares de aplicación y cumplimiento de la ley, lo que redunda de manera clara en un impacto en la privacidad de las personas, y eventualmente, en su derecho de reunión. Del mismo modo, las aplicaciones comerciales de TRF permiten a los actores corporativos recopilar grandes cantidades de datos confidenciales de personas que, a su vez, conservan solo un control limitado sobre la forma en cómo se utilizan dichos datos. De modo adicional, se critica que la TRF contiene un riesgo inherente de imprecisión y sesgo, lo cual es corroborado por estudios que demuestran que la TRF puede contribuir a aumentar, en gran medida, prejuicios raciales y de género si la IA subyacente está predominantemente entrenada en imágenes de personas con ciertas características, dejando a parte de la población más vulnerable a ser víctima de identificaciones incorrectas.

Así las cosas,si bien existe consenso sobre la necesidad de normar la TRF, no existe un acuerdo en cuanto a un modelo de regulación adecuado de esta tecnología, que logre conciliar un equilibrio entre los beneficios sociales de la misma y la correcta protección de los derechos humanos y las libertades individuales. Estados Unidos ha regulado la TRF mediante normativa específica, en tanto que la Unión Europea y China, salvo limitadas excepciones, continúan aplicando su normativa general en materia de protección de datos personales para normar el uso de la TRF[25]. Elementos tales

[25] En Estados Unidos, recientemente se ha visto un aumento de la actividad legislativa dirigida a la TRF. En el ámbito federal, en marzo de 2019, el Senado introdujo un proyecto de ley relativo a la "Privacidad del Reconocimiento Facial Comercial" en un intento por fortalecer la protección del consumidor y aumentar la transparencia (S.847-Commercial Facial Recognition Privacy Act of 2019). En virtud de esta norma en trámite, se prohíbe, por regla general a las Entidades Afectas, utilizar las TRF para recopilar datos de reconocimiento facial de usuarios finales, sin darles aviso previo y obtener su consentimiento. Las Entidades Afectas se definen en términos amplios para incluir cualquier entidad no gubernamental que "recolecte, almacene o procese datos de reconocimiento facial". También se prohíbe el uso de la TRF para discriminar a los consumidores, así como la reutilización de datos de tratamientos faciales, o su intercambio con terceros, sin obtener el consentimiento previo de los usuarios finales.

como en qué casos se permite el uso de esta tecnología, la necesidad o no de contar con el consentimiento del individuo para su registro facial, los usos que pueden darse a los datos faciales recolectados, la admisibilidad de intercambio de estos datos con terceros, entre otras materias, son objeto de debate jurídico para compatibilizar el aprovechamiento de los beneficios sociales del uso de la TRF con el respeto por los derechos humanos y las libertades individuales.

IA y libertad de trabajo

En materia de libertad de trabajo, las aplicaciones de IA conllevan procesos de automatización que ya están cambiando la naturaleza del empleo y las condiciones de trabajo en múltiples sectores. Los gobiernos necesitan coordinar sus acciones con científicos sociales, economistas y otros profesionales de distintas disciplinas, para comprender mejor las implicaciones de la IA para el empleo, identificando las partes que resultan beneficiadas, y aquellas que asumen el costo de estos vertiginosos cambios en el mundo laboral.

El temor relativo al efecto perjudicial que la automatización de labores puede tener sobre el empleo y, en particular, sobre ciertas áreas del mismo que serían reemplazadas por las labores de "robots inteligentes", ha sido y seguirá siendo objeto de amplio debate. Con todo, la historia humana demuestra que la incorporación de los avances tecnológicos en el ámbito laboral no es sinónimo de desempleo, sino, más bien, de readaptación y reorientación de la capacidad laboral y creativa del hombre a las nuevas condiciones de su entorno.

IA e igualdad ante la ley

En materia de igualdad ante la ley, discriminación, sesgo e inclusión, los diseñadores de políticas públicas y reguladores deben tener presente que los programas de análisis de datos de la IA reflejan las condiciones sociales, históricas y políticas en las que dicha tecnología de aprendizaje se creó. Los sistemas de inteligencia artificial "aprenden" en función de los datos que reciben. Este condicionamiento, junto a muchos otros factores, puede conducir a procesos de aprendizaje automático con resultados sesgados, inexactos e injustos. Se deben, por lo tanto, investigar las cuestiones de equidad aquí mencionadas, observando atentamente, cómo y quién define la noción de sesgo, y los diferentes impactos de la IA y sus aplicaciones en diversas poblaciones.

IA y Seguridad nacional

En materia de seguridad nacional e infraestructura crítica, debe considerarse que, a medida que se introduce la utilización de sistemas de IA en las infraes-

tructuras centrales, desde hospitales hasta la red eléctrica, los riesgos que estos presenten errores aumentan. Por esta razón, se requiere estudiar en detalle las formas de integración responsable de la IA en la sociedad[26].

* * *

De la observación de las complejidades y la relevancia jurídica de las cuestiones generadas por los avances y aplicaciones en IA, queda de manifiesto la necesidad de encontrar el equilibrio correcto entre regulación e innovación. Para estos efectos, se han realizado esfuerzos en el ámbito nacional e internacional para acordar los lineamientos generales con arreglo a los cuales se debe desarrollar la tecnología de la IA en el mundo.

En Chile, el gobierno trabaja en un documento denominado "Política nacional de inteligencia artificial", en el seno del Comité Interministerial de Inteligencia Artificial. En el contexto internacional destaca el Reglamento General de Protección de Datos (2018)[27]. Por otra parte, en mayo de 2019, los países miembros de la OCDE y otros asociados, suscribieron el documento denominado "Principios de la OCDE sobre la Inteligencia Artificial" (2019), conforme al cual se adoptaron formalmente las siguientes directrices de políticas intergubernamentales sobre IA:

1) Bienestar social y ambiental: La IA debe estar al servicio de las personas y del planeta, impulsando un crecimiento inclusivo, el desarrollo sostenible y el bienestar.
2) Estado de derecho, supervisión humana, privacidad, justicia, diversidad, no discriminación: los sistemas de IA deben diseñarse de manera que respeten el Estado de Derecho, los derechos humanos, los valores democráticos y la diversidad, e incorporar salvaguardias adecuadas –por ejemplo, permitiendo la intervención humana cuando sea necesario– con miras a garantizar una sociedad justa y equitativa.
3) Transparencia: los sistemas de IA deben estar presididos por la transparencia y una divulgación responsable a fin de garantizar que las personas sepan cuándo están interactuando con ellos y puedan oponerse a los resultados de esa interacción.
4) Robustez técnica y seguridad: los sistemas de IA han de funcionar con robustez, de manera fiable y segura durante toda su vida útil, y los potenciales riesgos deberán evaluarse y gestionarse en todo momento.

[26] Véase infra, sección II.3.3.

[27] Reglamento (UE) 2018/1807.

5) Responsabilidad: las organizaciones y las personas que desarrollen, desplieguen o gestionen sistemas de IA deberán responder de su correcto funcionamiento en consonancia con los principios precedentes.

Si bien ya existe en el ámbito internacional un acuerdo respecto de cierto catálogo de principios que deben gobernar la IA, el debate actual está cambiando su foco, para pasar de los principios, a normas jurídicas concretas que contemplen regulaciones más detalladas.

Con todo, legislar de manera concreta y detallada para dar vida a estos principios es un proceso lento, que requiere conciliar una multiplicidad de enfoques culturales, políticos y disciplinarios de los distintos actores sociales, y que, como hemos señalado, intente conciliar que las normas no sofoquen la innovación, pero, a la vez, protejan eficazmente los derechos y libertades de las personas.

3) Cibercrimen

La penetración de las nuevas tecnologías en todos los ámbitos de la sociedad, ha significado que también la actividad ilícita y criminal haya extendido su acción al ámbito digital, vulnerando las garantías individuales y colectivas de sus víctimas.

A este respecto, es posible identificar al denominado "cibercrimen puro", que se refiere a delitos contra computadoras y sistemas de información, donde el objetivo es obtener acceso no autorizado a un dispositivo o negar el acceso a un usuario legítimo. Las formas de ciberataques más comunes son el *malware*[28], el *phishing*[29], la ingeniería social[30], la denegación de servicio (DoS)[31] y los botnets[32]. Comprender qué hay detrás de estos términos es un primer paso

[28] El *malware*, abreviatura en inglés de la expresión software malicioso, incluye virus, gusanos, *spyware*, y todos aquellos programas que intentan dañar computadoras y dispositivos.

[29] El *phishing* es un ataque cibernético en que los delincuentes intentan extraer datos confidenciales como contraseñas o información de pago, en especial con la ayuda de correos electrónicos falsificados y la suplantación de URL y sitios web engañosos..

[30] La expresión "ingeniería social" (en inglés, social engineering) se refiere al aprovechamiento o explotación de descuidos o vulnerabilidades humanas que permiten a los delincuentes eludir las medidas de seguridad y obtener datos confidenciales. Sus técnicas van desde la solicitud de ayuda y la simulación de una urgencia, hasta la extorsión real.

[31] La "denegación de servicio" o DoS (acrónimo de Denial of Services) tiene por objetivo comprometer la accesibilidad de los servicios de Internet, como el acceso a un sitio web. Las compañías temen los ataques DoS porque la inaccesibilidad del sitio puede causar pérdidas, incluidas las económicas. Una variante común son los ataques de denegación de servicio distribuido (DDoS), en los que diferentes equipos atacan la infraestructura informática de una empresa para sobrecargarla.

[32] Una botnet o "red de bots" (también conocida como ejército zombi), es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por *malware*,

para enfrentar el problema de seguridad de los sistemas informáticos en el ámbito público y privado.

Por otra parte, las formas tradicionales de delincuencia también han evolucionado en la medida que las organizaciones criminales recurren cada vez más a Internet para facilitar sus actividades y maximizar sus ganancias en el menor tiempo. Estos "delitos ejecutados por medios cibernéticos" no son necesariamente nuevos, a saber: el robo, la estafa, el juego ilegal, la venta de medicamentos falsos, etc. Pero, en definitiva, estos delitos han adquirido una nueva dimensión por medio de su perpetración en línea. Dentro de este campo se encuentran también las figuras como el *ciberbullying*, *sexting*[33], terrorismo digital, pornografía infantil y otros delitos sexuales, tráfico ilícito de todo tipo de bienes y servicios, y en general, toda otra actividad ilícita disponible en la denominada "red oscura".

El delito cibernético, en sus dos acepciones vistas, está progresando a un ritmo muy rápido[34], con nuevas tendencias constantemente emergentes. Por lo tanto, las autoridades, reguladores, policías y usuarios deben mantenerse al día con las nuevas tecnologías para comprender las posibilidades que ellas crean para los delincuentes, y de esta manera diseñar e implementar las medidas a adoptar para combatir el delito cibernético. De manera adicional, debe considerarse que a mayor digitalización de las estructuras organizacionales públicas y privadas, mayor es la exposición de estas a ser víctimas de ataques cibernéticos.

Para los efectos de contrarrestar el avance del cibercrimen, la ciencia denominada ciberseguridad[35], también conocida como seguridad informática o seguridad de la tecnología de la información, ha tenido un enorme desarrollo en las últimas dos décadas. La ciberseguridad tiene por objetivo proteger la infraestructura computacional y todo lo relacionado con ella, en especial, la información contenida en computadoras o que circula a través de redes de computadoras.

---

de forma que quedan a disposición de un *hacker*. Al tomar el control de cientos o miles de equipos, las botnets se suelen utilizar para enviar *spam* o virus, para robar información personal o para realizar ataques de DDoS. En el presente, se consideran una de las mayores amenazas en Internet.

[33] Su nombre es un acrónimo de "sex" o "sexo", y "texting" o "escribir mensajes". Consiste en enviar mensajes, fotos o videos de contenido erótico y sexual personal a través del móvil mediante aplicaciones de mensajería instantánea o redes sociales, correos electrónicos u otro tipo de herramienta de comunicación.

[34] Interpol (2020).

[35] De la combinación de las expresiones 'ciber', que "indica relación con redes informáticas", y 'seguridad', que consiste en "la cualidad de seguro y exento de todo peligro, daño o riesgo. Real Academia de la Lengua (2020).

De acuerdo con el documento denominado "Política nacional de ciberseguridad (2017-2022)" del gobierno de Chile[36], la ciberseguridad es

> "tanto una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información[37], y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición"[38].

Por lo tanto, los ataques y las defensas que constituyen el objeto de la ciberseguridad se manifiestan en la triple dimensión que configura el ciberespacio, y que consiste en la capa física (infraestructura tecnológica), la capa lógica (componentes físicos de la información), y la capa humana (las interacciones entre usuarios).

La ciberseguridad, tanto preventiva como sancionatoria, a menudo requiere de la coordinación multidisciplinaria entre organizaciones del sector público y privado, las cuales deben buscar una comprensión integral de las dimensiones comerciales, regulatorias y técnicas de la gestión del riesgo cibernético[39].

4) Libertad de expresión y contenido digital

Históricamente, los gobiernos y las legislaciones de las democracias occidentales se han mostrado reticentes a regular los contenidos difundidos por los medios de comunicación social, en gran parte, por el respeto que se debe en las sociedades abiertas a la libertad de expresión y de prensa. Lo anterior es en especial cierto en el caso de los contenidos digitales, los que hasta ahora habían gozado del beneficio de ser considerados "puertos seguros", de modo

[36] Gobierno de Chile (2017).

[37] "Componentes lógicos de la información: los componentes lógicos de la información corresponden a la capa abstracta de datos que fluyen a través de las infraestructuras físicas de la información. Son componentes lógicos de la información, todos los programas computacionales, los protocolos técnicos de transmisión y almacenamiento de datos en todas sus capas, y en general todas las infraestructuras lógicas que sustentan las interacciones humanas en el ciberespacio",*op. cit*.

[38] Para estos efectos, se entiende por ciberespacio el "ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior", *op. cit*.

[39] Como marco regulatorio, en el ámbito nacional, destacan la Política Nacional de Ciberseguridad 2017-2022, del Gobierno de Chile (2017) y el decreto supremo n.º 533 (2015), que crea el Comité Interministerial sobre Ciberseguridad. En el contexto internacional, Chile es parte del Convenio de Budapest sobre Ciberdelincuencia (2017). Adicionalmente, se encuentra en tramitación en el Congreso Nacional el *Boletín* n.º 12 192-25, sobre el proyecto de ley de Delitos Informáticos.

que las restricciones y obligaciones de contenido han recaído en su mayoría sobre los medios tradicionales de comunicación.

Esta realidad ha permitido la entrada de actores nuevos al mercado de las comunicaciones digitales, posibilitando el surgimiento de plataformas innovadoras que permiten a los individuos crear y compartir contenidos como nunca antes[40]. Sin embargo, las expectativas y niveles de confianza públicos en torno a los medios de comunicación y a los servicios de noticias alternativos, las presiones existentes sobre el periodismo que aborda materias de interés púbico, las tensiones del mercado de los medios, y la necesidad de resguardar la honra de individuos e instituciones frente al masivo impacto de las difusiones en la red, han cambiado profundamente en los años recientes, y la era de la inercia regulatoria de contenido parece estar llegando a su fin.

Hechos tales como la intervención en procesos eleccionarios, las campañas de desinformación o "noticias falsas" (en inglés, fake news), la difusión de contenidos y propaganda relacionados con el terrorismo y violencia extrema[41], y contenidos tales como el discurso del odio, el acoso cibernético[42], la pornografía, el abuso infantil y otros comportamientos que importen la agresión y daño en línea, son los que han impulsado la tendencia regulatoria de plataformas y medios alternativos de comunicación disponibles en la red. Asimismo, eventos actualmente en desarrollo en el ámbito global, tales como la pandemia Covid-19 o las elecciones presidenciales en Estados Unidos y en el contexto local, como el proceso constituyente y los movimientos sociales y políticos en Chile, hacen prever que se continúe con la tendencia de aumento regulatorio de contenido.

Por último, se espera que la nueva tendencia regulatoria del contenido digital esté ampliando su rango de acción, para alocar responsabilidades a las plataformas de intercambio de videos mismas, exigiéndoles implementar cambios profundos en la forma de estructurar sus sistemas de admisión y moderación, para prevenir la difusión de contenido digital impropio.

[40] Los medios informativos alternativos o "medios ciudadanos" (en inglés, Citizen Media) basados en la red, incluyen blogueros, comentaristas de sitios web y otros oradores en línea.

[41] En 2019, luego de los trágicos eventos que rodearon los ataques terroristas en Christchurch, Nueva Zelanda, se generó una conciencia mundial, propiciada por la propia Nueva Zelanda y el gobierno de Francia, sobre la necesidad de cooperación intergubernamental y de los proveedores de servicios en línea, para regular los contenidos de terrorismo y violencia extremista en línea.

[42] *Ciberbullying* y *trolling*.

4. Tecnología financiera

La banca, industria única y sistémicamente relevante para la economía, ha sido según la tradición uno de los sectores empresariales más resistentes a las irrupciones tecnológicas. Sin embargo, la revolución digital, a través de un mejorado sistema de conectividad y la proliferación masiva del uso de dispositivos móviles, ha comenzado a cambiar la forma en que las personas acceden a los servicios financieros.

La tecnología financiera (en inglés, FinTech, contracción de las palabras 'finanzas' y 'tecnología'), consiste en el uso de la tecnología en la industria de servicios financieros, lo que resulta en la introducción de innovadores productos y servicios, principalmente a través del *software*. Al mismo tiempo, sin embargo, la tecnología financiera constituye un desafío para la existencia y funcionamiento de los servicios y productos financieros convencionales, ya que, a través de servicios alternativos, otorga acceso a mercados no transitados, contando con el respaldo de la tecnología.

La tecnología financiera ha dado lugar al surgimiento de financiamientos alternativos a través de préstamos entre pares y al financiamiento comercial por parte de operadores de mercados electrónicos a favor de comerciantes. Otros avances de esta tecnología incluyen el micromecenazgo o *crowdfunding* de capital[43]; las monedas digitales[44] que operan de forma independiente de cualquier autoridad central o banco; los sistemas de pago y remesas que evitan los canales bancarios tradicionales; y el uso de macrodatos (Big Data)[45] y análisis para maximizar los datos disponibles de clientes para obtener el máximo provecho de las relaciones existentes con ellos.

La tecnología financiera se apoya, para su funcionamiento, en diversas nuevas tecnologías y aplicaciones, entre las que se cuentan, la autenticación biométrica, la computación en la nube, la IA y el aprendizaje automático,

[43] El "crowdfunding de proyecto", "crowdfunding de capital" o "equity crowdfunding" permite hacer pública una idea empresarial y que multitud de pequeños y grandes inversores tengan acceso a ella y puedan invertir su dinero, entrando en el capital social de la empresa.

[44] La moneda digital es un medio de intercambio disponible en forma digital, no en forma física, que posee propiedades similares a las monedas físicas, y permite transacciones instantáneas y transferencia de propiedad sin fronteras. Una criptomoneda es una moneda digital que utiliza criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido.

[45] Los macrodatos (en inglés, Big Data), es un término que hace referencia a conjuntos de datos tan grandes y complejos, que requieren aplicaciones informáticas no tradicionales de procesamiento de datos para ser tratados adecuadamente. Por ende, los procedimientos usados para encontrar patrones repetitivos dentro de esos datos son más sofisticados y requieren un *software* especializado.

los pagos digitales y móviles, las tecnologías de registros distribuidos y de cadena de bloques (en inglés, Distributed Ledger Technology y *Blockchain*, respectivamente)[46], los macrodatos, las plataformas flexibles, la ciberseguridad y los censores avanzados.

Las posibles aplicaciones de las tecnologías de registros distribuidos y de cadena de bloques no se limitan a operar en monedas virtuales o productos financieros básicos. El hecho mismo de que estas tecnologías permitan que los participantes de la red transfieran y actualicen información o registros, y que esto se haga de manera confiable, segura y eficiente, tiene un potencial gigante, con enormes implicancias no solo en materia de finanzas, sino que, también, en diversas otras áreas como la propiedad intelectual y el derecho bancario. Estas tecnologías aportan grandes ventajas para efectos de seguridad de las transacciones que se realizan a través suyo, lo que en el ámbito jurídico tiene manifestación mediante el uso de los "contratos inteligentes" (en inglés, Smart Contracts)[47] que entre otras cosas, permiten automatizar ciertas transacciones y obtener la rastreabilidad de algunas operaciones.

Sin embargo, aunque la valorización de las tecnologías de registro distribuido se está materializando de forma gradual, sus usos en materia de servicios financieros está introduciendo también nuevos riesgos y dando lugar a nuevas cuestiones legales y de gobernanza.

El desafío que enfrentan los legisladores y la autoridad en general en esta materia, es el mismo que hemos observado a lo largo de este trabajo en

[46] La tecnología de registro distribuido, es una base de datos que gestionada por varios participantes de manera NO centralizada (no existe una autoridad central que ejerza de árbitro y verificador). El registro contable (*ledger*), permite soportar y garantizar la seguridad del dinero digital distribuido, aumentando la transparencia del sistema y dificultando cualquier tipo de fraude o manipulación. La tecnología de cadena de bloques (*Blockchain*), es un tipo de tecnología de registro distribuido, que cuenta con una serie de características particulares. También es una base de datos o registro contable compartido, pero que funciona mediante bloques que, como indica su propio nombre, forman una cadena. Los bloques se cierran con una especie de firma criptográfica llamada *hash*; el siguiente bloque se abre con ese *hash*" a modo de sello lacrado. De esta forma, se certifica que la información, encriptada, no se ha manipulado ni se puede manipular. *Blockchain* debe su fama, entre otras cosas, a que es la tecnología detrás de la famosa criptomoneda Bitcoin.

[47] Un "contrato inteligente" es un programa informático que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes. El programa ayuda en la negociación y definición de los acuerdos, causando que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas. El contrato inteligente es un programa que forma parte de un sistema no controlado por ninguna de las partes, ni sus agentes, y que ejecuta un contrato automático el cual funciona como una sentencia *if-then* (si-entonces) de cualquier otro programa de ordenador. Cuando se dispara una condición preprogramada, no sujeta a ningún tipo de valoración humana, el contrato inteligente ejecuta la cláusula contractual correspondiente.

materia de regulación de nuevas tecnologías, a saber, conciliar la necesidad de fomento del desarrollo, la innovación y la libre competencia, con el imperativo de limitar los riesgos para los consumidores, proteger sus derechos y libertades, y en esta área en particular, velar por la estabilidad financiera. Asimismo, la autoridad debe proporcionar orientación normativa a todos los actores del mercado respecto de los nuevos tipos de productos, servicios, modelos comerciales y mecanismos de entrega, que pueden no estar cubiertos por los marcos regulatorios tradicionales.

Entre las soluciones que se han propuesto a escala global para los referidos desafíos regulatorios de modelos financieros emergentes, destacan los denominados "sandboxes regulatorios"[48]. Estos consisten en campos de pruebas para nuevos modelos de negocio que aún no están protegidos por una regulación vigente, supervisados por las instituciones regulatorias, en los que los participantes del mercado pueden probar sus innovaciones en un entorno controlado sin incurrir de inmediato en todas las consecuencias regulatorias normales. Su objetivo es ayudar a determinar el tratamiento regulatorio más apropiado a la innovación, identificar las brechas existentes en el marco regulatorio, y proporcionar el conocimiento y capacitación a los reguladores, que intentan mantenerse al día con el ritmo de la innovación. De esta forma, se concilia el cumplimiento de las estrictas regulaciones financieras con el crecimiento y los tiempos de las empresas más innovadoras, evitando coartar con normas al sector de la tecnología financiera, pero también protegiendo los derechos de los consumidores.

5. *Gobierno y tecnología*

Para entender el impacto transformador de la revolución digital en la organización y funcionamiento del Estado, y cómo el derecho se encarga de regular dicha realidad, resulta útil distinguir las nociones de gobierno digital, política de datos abiertos y neutralidad tecnológica.

1) Gobierno digital

El gobierno digital, también denominado gobierno electrónico o e-gobierno (en inglés, e-government), consiste en el uso de las TIC, para mejorar la prestación de los servicios públicos a los habitantes de un país o región. El gobierno

[48] La palabra '*sandbox*', literalmente, "caja de arena", hace referencia a un arenero, es decir, un recinto pequeño donde los niños pueden jugar y experimentar en un entorno controlado. El término ha ido adquiriendo nuevos significados en el mundo de la informática, para referirse a un entorno de pruebas cerrado, diseñado para experimentar de forma segura con proyectos de desarrollo web o de *software*.

digital ofrece nuevas oportunidades para un acceso ciudadano más directo y conveniente al gobierno, y para la provisión de servicios gubernamentales directamente a los ciudadanos.

La modernización del Estado por medios digitales se extiende a las relaciones reciprocas entre los ciudadanos, instituciones privadas, las autoridades y todos los organismos que forman parte del Estado.

En el caso chileno, el proceso de modernización estatal por medio de la digitalización de sus instituciones se rige por la Ley n.° 21180 sobre Transformación Digital del Estado (2019), la que junto con otras regulaciones de carácter legal y reglamentario, tienen por objetivo promover la transformación digital estatal, cuidando estandarizar los procesos y procedimientos relevantes, para asegurar la coordinación y coherencia en la implementación de las políticas de transformación digital. Su ejecución se canaliza a través del Consejo Asesor Permanente para la Modernización Estado y del Consejo Ejecutivo de la Modernización del Estado. De este último, a la vez, dependen las divisiones de Gobierno Digital y Laboratorio de Gobierno y la Secretaría de Modernización.

Las aplicaciones concretas de estos esfuerzos digitalizadorase del aparato estatal pueden observarse en todas las plataformas de tramitaciones en línea disponibles,tales como ocurre con el portal del Servicio de Impuestos Internos, el Registro Civil, las comisarías virtuales, el Portal Unificado de Fondos Concursables del Estado, Chileatiende.cl, por nombrar algunas.

2) Estado abierto y transparencia

Un segundo aspecto a considerar en relación con al impacto de las nuevas tecnologías en el funcionamiento del Estado y su necesidad de regulación, se refiere a la denominada "política de datos abiertos", que no es más que la concreción, en la era digital, del principio de transparencia que rige la actuación estatal, y que en nuestro ordenamiento jurídico, ha sido elevado a rango constitucional[49].

La tendencia de "datos abiertos", en materia de intercambio de datos en la era digital, corresponde a

> "aquellos datos digitales que son puestos a disposición de los usuarios de la red, con las características técnicas y jurídicas necesarias para que puedan ser usados, reutilizados y redistribuidos libremente por cualquier persona, en cualquier momento y en cualquier lugar"[50].

[49] Art. 8 de la Constitución Política de la República de Chile (1980).

[50] Open Government Partnership (2015).

Por su parte, el "Estado abierto" o "gobierno abierto", se basa en una política pública de datos, consistente en principios de conducta y praxis legal, que persigue que el Estado haga disponibles determinados tipos de datos de forma libre, sin restricciones de derechos de autor, de patentes o de otros mecanismos de control.

En el ámbito mundial, la política de datos abiertos comenzó con la iniciativa de la banca abierta en el Reino Unido, donde el gobierno requirió que los nueve bancos minoristas líderes del Reino Unido permitieran a los clientes acceder a sus propios datos y, con el consentimiento del cliente, compartirlos con terceros autorizados. Francia, por su parte, manteniendo su tradición de transparencia democrática y de compartir información en poder de las autoridades públicas, lanzó una ambiciosa política en 2016, en relación con la apertura de los datos públicos, convirtiendo los datos abiertos en un sinónimo de gobierno abierto, apoyándose en grupos de trabajo como "Etalab", que coordina la acción del gobierno sobre datos abiertos, desarrolla y administra un portal en línea relacionado con datos abiertos, y apoya la reutilización de datos públicos.

En Chile, DatosGob es un portal que funciona como un "repositorio central de datos abiertos", donde las instituciones de la administración pública chilena deben publicar sus datos abiertos, de modo tal que los usuarios puedan encontrar conjuntos de información pública del gobierno de manera fácil y confiable. Asimismo, Chile suscribió la Carta Internacional de Datos Abiertos (2015), en el contexto de la Cumbre de Alianza para el Gobierno abierto que se realizó en México de 2015.

Es evidente que los beneficios que reportan la digitalización estatal y el "Estado abierto" son enormes, en términos de eficiencia y transparencia. Con todo, cabe recordar aquí que a mayor digitalización, mayor es el grado de exposición digital que experimenta el aparto estatal, ya sea a consecuencia de fallos espontáneos del sistema o, bien, de la acción directa del cibercrimen[51].

3) Neutralidad tecnológica.

Finalmente, en materia de interacción entre Estado y tecnología, y sus implicancias para el derecho, es relevante referirse al principio de neutralidad tecnológica, en virtud del cual las iniciativas públicas diseñadas para promover y fomentar la innovación tecnológica en el sector privado, deben respetar la libre competencia, y el principio de no discriminación arbitraria en el trato que deben dar el Estado y sus organismos en materia económica[52].

[51] Véase supra secciones II.3.3. y 3.4.

[52] Art. 19 n.^{os} 21 y 22 de la Constitución Política de la República de Chile (1980).

En general, el concepto de neutralidad tecnológica se entiende en relación con la atribución (poder-deber) del Estado, para seleccionar libremente al proveedor de tecnología que representa la mejor opción en términos de calidad, eficiencia y costo, en el contexto de un proceso de contratación público-privada determinado. Para efectos de esta selección, el Estado debe sujetarse al cumplimiento de los principios y procedimientos concesionales administrativos.

En consecuencia, la neutralidad tecnológica no consiste en que los proveedores de bienes y servicios tecnológicos tengan cuotas de mercado equivalentes, ni en que la Administración deba implementar, por medio de sus contrataciones, mecanismos compensatorios respecto de actores comerciales que no han tenido éxito en el mercado. Tampoco debe interpretarse, en el contexto del Estado de derecho democrático, donde rige el principio de juridicidad o legalidad de los actos de la Administración[53], que el Estado sea libre para de forma arbitraria escoger al prestador de bienes o servicios tecnológicos que demanden las necesidades públicas. Por el contrario, estando dotado el Estado de un poder-deber de selección del mejor oferente de tecnología privado, necesariamente deberá fundar su selección en criterios racionales y de bien común, para lo cual debe ajustarse tanto en la selección como en la adjudicación a los procedimientos concesionales preestablecidos, actuando bajo los principios de transparencia e igualdad a la hora de contratar con las empresas privadas de tecnología. Así debe ocurrir por lo demás, de acuerdo con la normativa chilena vigente[54].

En este sentido, resulta interesante contrastar las políticas europeas de concurso público para la asignación del espectro 5G, donde las licitaciones se sujetan a modelos preestablecidos de asignación de frecuencia/espectro, respecto de la modalidad China, que simplemente autoriza al órgano administrativo del sector de telecomunicaciones (es decir, el Ministerio de Industria y Tecnología de la Información,) para asignar dicha frecuencia/espectro, sin mediar proceso de licitación previo alguno[55].

[53] Arts. 6 y 7 de la Constitución Política de la República de Chile (1980).

[54] El art. 8 bis de la Ley de Bases Generales de la Administración del Estado (1986), señala: "Los contratos administrativos se celebrarán previa propuesta pública, en conformidad a la ley. El procedimiento concursal se regirá por los principios de libre concurrencia de los oferentes al llamado administrativo y de igualdad ante las bases que rigen el contrato. La licitación privada procederá, en su caso, previa resolución fundada que así lo disponga, salvo que por la naturaleza de la negociación corresponda acudir al trato directo".

[55] En comparación con su predecesor 4G, la tecnología 5G proporciona velocidades hasta mil veces rápidas, de latencia más bajas, y puede admitir una mayor cantidad de dispositivos (aproximadamente cien veces más). La tecnología 5G también proporcionará la infraestructura y los datos que son necesarios para entrenar y nutrir la tecnología de IA.

III. Conclusiones

1. La revolución digital ha significado enormes y aceleradas transformaciones sociales a partir de la segunda mitad del siglo XX, y en especial, durante las primeras dos décadas del siglo XXI. Los cambios experimentados en un periodo relativamente acotado de tiempo, han supuesto grandes beneficios para la calidad de vida de las personas, pero, al mismo tiempo, han impuesto desafíos éticos y prácticos, que demandan nuevas respuestas al derecho en materia de justicia, seguridad y orden.
2. A partir del análisis de las distintas áreas de innovación tecnológica que resultan relevantes para el derecho en la actualidad, queda de manifiesto que la incorporación de las nuevas tecnologías ha provocado dilemas éticos profundos y generado tensiones entre, por una parte, la innovación y el progreso que conlleva el avance tecnológico y, por la otra, el debido resguardo de ciertos derechos y libertades fundamentales.
3. Esto ocurre porque el intercambio de datos y la integración de la inteligencia artificial y de sus aplicaciones, en los ámbitos público y privado, son una realidad presente y, a la vez, un presupuesto básico para el desarrollo y la innovación. Los avances científicos en medicina y en las industrias farmacológicas y alimentaria, los beneficios en materia de seguridad pública, educación, transporte, comunicación, transparencia y libertad de información, así como la simplificación de una infinidad de tareas, son una realidad tangible. Sin embargo, también es cierto que tanto el intercambio de datos masivo como varias de las aplicaciones de IA se presentan como amenazas latentes para la privacidad y dignidad de las personas y otros seres vivos, la igualdad ante la ley, la estabilidad laboral y financiera e, incluso, para la seguridad nacional.
4. Ante estos dilemas, autoridades, reguladores y los demás actores sociales, parecen haber alcanzado un consenso en cuanto a la imperiosa necesidad de regular la actividad científica y tecnológica con arreglo a ciertos parámetros de ética y eficacia normativa para el logro de la justicia, la seguridad y el orden. Con todo, no existe acuerdo en cuanto a la forma adecuada de materializar dichas regulaciones, considerando el delicado equilibrio que se busca, consistente en proteger las garantías individuales sin ahogar la innovación y el progreso técnico.
5. Con todo, a partir de la observación de la realidad regulatoria nacional y comparada, es posible advertir que ciertas técnicas en el

ámbito legislativo y de las políticas públicas han ido presentándose como alternativas valiosas para el cumplimiento de los desafíos normativos propuestos por la innovación a la ciencia del derecho.

6. Primeramente, si bien la tendencia regulatoria actual se mueve hacia un endurecimiento de las normas de protección de las garantías individuales en desmedro de la libre competencia, parece razonable que dicha regulación considere apartarse de prohibiciones generales abstractas, para concentrarse en la identificación y proscripción de las situaciones precisas que causan la potencial vulneración de derechos mediante leyes específicas de daños. Así, citamos, por ejemplo, que si el intercambio de datos personales supone un riesgo de prejuicio en contra de los individuos en el contexto de procesos selectivos laborales o de seguros, la norma debiese propender a la prohibición de las conductas discriminatorias, y no necesariamente atacar el flujo de datos personales implementado como corresponde. La técnica legislativa en este caso, puede inclinarse por asignar responsabilidades y extender su ámbito aplicación, sobre plataformas y otros actores relevantes, más que inclinarse por derechamente prohibir una determinada actividad.
7. En segundo lugar, y considerando que los cambios tecnológicos se suceden a un ritmo que no da tregua, ni posibilidad de respuesta inmediata al derecho mediante normativas detalladas, se ha puesto en práctica la costumbre de acordar textos y documentos en que gobiernos y actores privados enuncian principios o, lo que es lo mismo, definen marcos ético-regulatorios dentro de los cuales se comprometen a circunscribir su actuar, y en el futuro, a normarlo de manera vinculante. Este trabajo es netamente colaborativo, y se presenta como una alternativa real de cambio, que se caracteriza por tratarse de una acción que traspasa las clásicas divisiones jurisdiccionales, disciplinarias y publico-privadas. En efecto, la acción conjunta entre gobiernos, organismos multilaterales y empresas tecnológicas, aunando por la vía de criterios multidisciplinarios de carácter técnico, científicos y jurídicos, ha permitido ciertos avances en materias que otrora parecían inasibles. En este contexto, cobran especial importancia los documentos de autorregulación de las empresas tecnológicas, las que entienden que su disposición colaborativa es indispensable para temperar el rigor legislativo y, además, visualizan esa opción por la empatía de los requerimientos éticos y sociales como una ventaja comparativa respecto de sus competidores.
8. Por último, modelos regulatorios preparatorios como los "sandboxes" utilizados en materia de tecnología financiera, donde reguladores y

regulados acuerdan los términos de una especie de marcha blanca operativo-regulatoria limitada en tiempo y efectos, y que conjuga la implementación de las innovaciones con el espacio para que el derecho aprenda, se ajuste y corrija la integración responsable de la tecnología, se asoman como alternativas normativas que pueden ampliarse a los demás ámbitos de la regulación de las nuevas tecnologías.

Bibliografía

Determann, Lothar (2020). "Personal Data Regulation: What is on the horizon?", in *Technology, Media and Telecommunications Looking Ahead*, Palo Alto, California, Baker & McKenzie, pp. 6-7.

Electronic Frontier Foundation, E. (2004). "Las consecuencias no deseadas: Cinco años bajo la Digital Millenium Copyright Act", en *Revista Chilena de Derecho Informático*, n.º 4, pp. 17-35. Disponible en https://revistas.uchile.cl/index.php/RCHDI/article/view/10671 [fecha de la consulta: 10 de mayo de 2020].

Giarda, Raffaele (2020). "New Technology. Artificial Intelligence, 5G, Trust and Beyond", in *Technology, Media and Telecommunications Looking Ahead*, Palo Alto, California, Baker & McKenzie, pp. 10-18.

Lagriguet, Guillermo (2007). *Dogmática jurídica y aplicación de normas. Un análisis de las ideas de autonomía de ramas jurídicas y unidad del Derecho*, Ciudad de México, Editorial Fontamara.

Organización Mundial de la Propiedad Intelectual (2006). "La bioética y el derecho de patentes: El caso del oncomouse", en *Revista de la Organización Mundial de la Propiedad Intelectual*, n.º 3/2006. Disponible en www.wipo.int/wipo_magazine/es/2006/03/article_0006.html [fecha de la consulta: 10 de mayo de 2020).

Real Academia Española (2020). *Diccionario de la lengua española*, 23ª ed., versión 23.3 en línea. Disponible en https://dle.rae.es [fecha de la consulta: 10 de mayo de 2020].

Vergara Blanco, Alejandro (2014): "Sistema y autonomía de las disciplinas jurídicas. Teoría y técnica de los núcleos dogmáticos", en *Revista Chilena de Derecho*, vol. 41, n.º 3, pp. 957-971.

Normas

Boletín n.º 11 144-0: Proyecto de Ley sobre Ley de Protección de Datos Personales.

Boletín n.º 12 192-25: Proyecto de Ley de Delitos Informáticos.

Constitución Política de la República de 1980.

Decreto n.º 83 del Ministerio de Relaciones Exteriores, Convenio de Budapest sobre Ciberdelincuencia, 28 de agosto de 2017.

Decreto supremo n.º 533, crea el Comité Interministerial sobre Ciberseguridad (CICS), 27 de abril de 2015.

Ley n.º 17336, sobre Propiedad Intelectual, 2 de octubre de 1970.

Ley n.º 18575, fija las Bases Generales de la Administración del Estado, 5 de diciembre de 1986.

Ley n.º 19039, sobre Propiedad Industrial, 25 de enero de 1991.

Ley n. 19223, Tipifica Figuras Penales Relativas a la Informática, 7 de junio de 1993.

Ley n.º 19628, sobre Protección de la Vida Privada, 28 de agosto de 1999.

Ley n.º 20243, sobre Derechos Morales y Patrimoniales de los Intérpretes de las Ejecuciones Artísticas fijadas en Formato Audiovisual, 5 de febrero de 2008.

Ley n.º 21180 (2019), sobre Transformación Digital del Estado, 11 de noviembre.

Public Law 105-304 (1998), Digital Millenium Copyright Act, October 28, 1998. Disponible en www.govinfo.gov/content/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf [fecha de consulta: 10 de mayo de 2020].

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (2016), Reglamento General de Protección de Datos, 27 de abril de 2016. Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [fecha de consulta: 10 de mayo de 2020].

Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo (2018), Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1807&from=EN [fecha de consulta: 10 de mayo de 2020].

S.847 - Commercial Facial Recognition Privacy Act of 2019. Disponible en www.congress.gov/bill/116th-congress/senate-bill/847/text [fecha de consulta: 10 de mayo de 2020].

Otros documentos

Berkely Center for Law & Technology (2019): 2019-2020 *Annual Bulletin*. Disponible en https://issuu.com/berkeleylaw/docs/bclt_annualbulletin2019-20 [fecha de consulta: 10 de mayo de 2020].

Gobierno de Chile (2017). Política nacional de ciberseguridad 2017-2022. Disponible en www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf [fecha de consulta: 10 de mayo de 2020].

Interpol (2020). Cybercrime. Disponible en www.interpol.int/Crimes/Cybercrime [fecha de consulta: 10 de mayo de 2020].

Open Government Partnership (2015): Carta Internacional de Datos Abiertos, 29 de octubre de 2015. Disponible en https://opendatacharter.net/principles-es/ [fecha de consulta: 10 de mayo de 2020].

Organización para la Cooperación y el Desarrollo Económico (2019). Principios de la OCDE sobre Inteligencia Artificial. Disponible en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [fecha de consulta: 10 de mayo de 2020].