

Justicia: Los desafíos ante el avance de las tecnologías

Por Juan Carlos Manríquez R.



Socio del Estudio de Abogados MBCIA, LLM (CWSL, USA); Profesor LLM UC, Especialista en Derecho Penal Económico y de la Empresa (UC-LM, España), AD en Derecho Penal Internacional (Siracusa, Italia) Litigante ante la Corte Penal Internacional (La Haya, Holanda).

MANRIQUEZ
BENAVIDES & CIA

VALPARAÍSO:

ALMIRANTE SEÑORET 70, PISO 9

OFICINAS 91-92,

TELÉFONOS: (56) 32 2231080 – (56) 32 2256926

FAX: (56) 32 2595345

EMAIL: INFO@MBCIA.CL

SANTIAGO:

BANDERA 341, PISO 7, OFICINA 759

TELÉFONOS: (56) 2 24896000 – (56) 24896009

EMAIL: INFO@MBCIA.CL

ÍNDICE

Reformas judiciales en curso: telemática, IA, eficiencia del dinero público y acceso a la justicia.	4
Ecosistema digital y sistemas de justicia: ¿hay machismo y misoginia en la IA?	6
Reconocimiento facial y tecnología intrusiva: por qué la moratoria de la ue y cuáles criterios las hacen admisibles.	9
Neuroderechos, brain privacy, inteligencia artificial y predictibilidad delictiva por uso de algoritmos.	10
Marco normativo de los delitos informáticos y cibernéticos en Chile.	12
Fake news en pandemia: mentira, cyberwar y riesgo de daño a la vida y salud.	15
Evidencia digital, análisis forense, IA y algoritmos predictivos: retos de litigación moderna para el Código Procesal Penal de Chile.	16
Programación algorítmica y su impacto en industria del juego	26

REFORMAS JUDICIALES EN CURSO: TELEMÁTICA, IA, EFICIENCIA DEL DINERO PÚBLICO Y ACCESO A LA JUSTICIA.

El Estado de Excepción Constitucional por Emergencia Sanitaria debido a la pandemia por covid19 termina el 30.06.2021, si es que las condiciones lo permiten, y tanto la Corte Suprema, el Ministerio de Justicia y el Parlamento, junto a los Colegios de Abogados, han manifestado su preocupación por la enorme cantidad de audiencias diferidas en áreas tan sensibles como son los asuntos de Familia, Laborales y Penales.

Esos procesos de algún modo han podido avanzar, pero las causas civiles han sufrido un enorme rezago.

El desafío para todos los operadores del sistema legal es tremendo, y más aún, considerando lo preceptuado en el art. 5 inciso 2 de la Constitución, y por esa vía, enfrentados a la obligación internacional de cumplir con lo pactado en la CADH y en el PIDCP, en cuanto a que todo obstáculo que demore o impida el acceso a la Justicia debe ser removido con celeridad, cuando es posible, hacer realidad la Tutela Judicial Efectiva de los derechos de los justiciables no será nada de fácil, y quizás, tampoco oportuno.

Si bien el estándar de actuación de los órganos de justicia en “plazo razonable” no es una regla positiva del derecho internacional de los DDHH, si es un principio rector que debe observarse por los Estados signatarios de las Convenciones indicadas y en Chile debe serlo a consecuencia del texto constitucional por toda autoridad, órgano o persona, por cuanto es un componente primordial del “Debido Proceso” (Digesto: 2020, Comisión Int DDHH).

La telemática, la digitalización de los procesos y de las audiencias han sido la primera forma de operar en el país desde abril de 2020. Las leyes 21.226 y 21.227, así como las Actas 13, 41 y otras de la Excm. Corte Suprema han regulado esta realidad que es, para citarla, uno de los mejores ejemplos de una “fuente material” del Derecho que pueda hallarse fuera de los textos de Ciencia General. Por eso es que todo lo aprendido en este tiempo, así como las destrezas adquiridas o desarrolladas para tratar con las

herramientas que nos entrega la Inteligencia Artificial (IA), la Predictibilidad Algorítmica y la “Presencialidad Remota” no pueden quedar fuera del análisis del legislativo y del Gobierno colegislador al momento de diseñar soluciones normativas para el retardo procesal y afrontar la avalancha post Covid.

En materia civil, la reforma en curso debe considerar la generación, percepción y examen de la prueba digitalmente obtenida mediante plataformas informáticas que hacen más fácil compartir planos, fotos, pericias y gráficos que extenderlos sobre mesones de madera del S. XIX, que por piezas de ebanistería que sean y de alto valor histórico, ya no son el mejor soporte. Los jueces civiles y mediadores, asistidos por uno o dos funcionarios especializados podrían despachar miles de audiencias detenidas de menor complejidad mediante una agenda digital formada meses antes con día y hora aceptada por ambas partes, con escasísimas posibilidades de re agendamiento y con sanciones duras para el litigante de mala fe o para el abogado que las procrastine sin más razón que molestar a los otros.

Si se quiere reformar los procesos civiles, mírese el futuro que llegó adelantado 15 años y superemos modelos escritos, añejos y lentos. La Comunidad Europea ya está haciendo lo suyo.

En materia penal, la APP sobre Predictibilidad Algorítmica de escenarios y resultados potenciales desarrollada para las audiencias que la Defensoría Penal Pública ha puesto en funcionamiento piloto es una muestra de que la IA ya está presente en el sistema de justicia nacional.

Igual técnica de detección de patrones e ideas-fuerza que pueda agrupar y procesar criterios a través de algoritmos cabría ser aplicada en la Sistematización de Líneas Jurisprudenciales que la Excm. Corte Suprema lleva adelante con el trabajo de varias Universidades, a cargo de la ex Ministra de la Corte Dña. María Eugenia Sandoval (el llamado “Proyecto Bus-

gador Integrado (IA) de la Corte Suprema”) haciendo así mucho más eficiente la preparación del litigio o la evaluación de la probabilidad de cómo un caso podría ser resuelto o desestimado, lo que bajaría de manera relevante la incerteza o alta variación de criterios para casos casi idénticos, facilitando la gestión de jueces y abogados.

En los alegatos en las Cortes Superiores y en primera instancia una conexión remota ha permitido a los intervinientes seguir siendo representados por los abogados que mejor conocen el caso desde el origen, sin tener que gastar enormes sumas de dinero en viajes o alojamiento para ver suspendidas sus audiencias muchas veces sin la deferencia contraria del aviso oportuno, y/o por todo eso, verse privadas de acceder a la Justicia al carecer de dinero para costear la pesada carga del litigio.

En el Colegio de Abogados de Valparaíso ya en 2015 habíamos propuesto que determinadas actuaciones simples (como anuncios para alegar y comparencias desde San Antonio o San Felipe) se hicieran por mail o video llamadas, para acercar la Justicia a las personas, cuando hubo largas demoras en los tiempos de desplazamiento por arreglos en las carreteras, pero fue en el sur de Chile donde se les dio su primera oportunidad, y vean donde estamos hoy, en que Microsoft ha dado a conocer su herramienta de reuniones con holografías de realidad aumentada, y quizás así dentro de poco se harán también la mayoría de los alegatos.

¿Tiene algún sentido que todas las audiencias concentradas, las de salidas alternativas, formalización, simplificados con admisión, abreviados o APJO más sencillas o en las que hay acuerdo obliguen a todos los intervinientes a moverse con largas horas de tiempo muerto al Centro de Justicia de Avenida Pedro Montt o a otros edificios del país si se pueden hacer por zoom u otra plataforma similar?

El punto más complejo parece no ser ese, sino qué se haría para reconvertir ese espacio que quedaría ocioso y cómo resolver el gasto fiscal de mantener un edificio que habría perdido su utilidad inicial en un alto porcentaje de ocupación y con un leasing de largo aliento de por medio.



Dado que el futuro se adelantó 15 años, y que cuidando de la seguridad y la privacidad del tráfico jurídico en balance con los derechos fundamentales de los justiciables, insistir en modelos de justicia y servicio judicial de hace más de un siglo carece de sentido, sería muy razonable tomarse en serio que llegó el momento de adoptar los cambios que son realmente urgentes para que la Justicia (con mayúscula) sea un bien alcanzable y concreto incluso para los que están físicamente lejos de los centros urbanos.

El ciudadano digital hoy es menos virtual y a cada momento más real, algo que nuestras autoridades judiciales, parlamentarias y gubernamentales seguramente no ignoran y por eso actuarán en consecuencia.

1- Modernización de los sistemas judiciales en la UE – preguntas y respuestas.
https://ec.europa.eu/commission/presscorner/detail/es/qanda_20_2247.

2- Defensoría estrena aplicación que permitirá agilizar procesos y proyectar formas de término de la audiencia de control de detención.
http://www.dpp.cl/sala_prensa/noticias_detalle/10904/defensoria-estrena-aplicacion-que-permitira-agilizar-procesos-y-proyectar-formas-de-termino-de-la-audiencia-de-control-de-detencion

3- Microsoft presenta plataforma que permite comunicarse con hologramas.
<https://cnnespanol.cnn.com/video/microsoft-mesh-hologramas-realidad-mixta-hololens-iklv-cnn-dinero/>

ECOSISTEMA DIGITAL Y SISTEMAS DE JUSTICIA: ¿HAY MACHISMO Y MISOGINIA EN LA IA?

1-Einstein y el Prejuicio.

El 08 de marzo celebramos otra vez el Día Internacional de la Mujer, y claro que es impresionante y motivador ver hoy cómo desde ese lejano 23 de febrero en el calendario Juliano de la Rusia Zarista (8M en el Gregoriano), la base cultural, filosófica, argumental, política, pragmática y activista de aquello en lo que ha devenido el Feminismo, en sus diversas acepciones y corrientes (Feminist Theory And The Law, Judith A. Baer, The Oxford Handbook of Political Science, Edited by Robert E. Goodin, July 2011) ha logrado hacer visible lo que nos parece de toda evidencia, como la igualdad salarial a igual trabajo o la no “condenación por el rol” y ha puesto en tensión algunos temas tabú,

como el miedo masculino endémico a la alfabetización y empoderamiento de la mujer.

Pero como quiera que sea, hay una línea central que es irrefutable en el actual estado de cosas. Se debe avanzar definitivamente en la evitación o eliminación del prejuicio en todo tipo de sistema de aquellos que tratan con “el otro”, y particularmente, si esa alteridad se practica con una mujer, y más aún, si hablamos de los sistemas de justicia. Como dice este trabajo: “La Otridad tiene rostro de mujer”.

El lenguaje no sólo expresa realidad, la construye y define sus límites, es gran parte una acción política en el sentido amplio, que levanta, derriba o abre muros de comprensión del otro, y por cierto ayuda a superar el prejuicio, si el lenguaje es dialogal. Hernández Castellanos (2011), lo dice bien en su artículo Formas de la alteridad: un reto epistemológico y político .

Albert Einstein dijo que “es más fácil dividir el átomo, que terminar con un prejuicio”. Como ya dividimos el átomo, ahora cabe ocuparse del prejuicio.

Misoginia Judicial y Gender Justice.

Estudios reputados, opiniones respetables y noticias varias han detectado que los sistemas de justicia han discriminado negativamente en forma histórica a la mujer cuando es sujeto/objeto de una indagación (así, fuente probatoria primaria [víctima] o secundaria [testigo, perita o experta]) de un caso penal por agresión sexual, o reclamante en juicio civil o de familia, o postula a cargos de relevancia en la estructura de gobierno o en la alta jerarquía judicial, pues se le cree menos, o se le impugna más que a un par hombre en igual situación.

Así lo dicen también en Chile recientes publicaciones, como la nota en el diario La Tercera titulada “Sistema judicial y mujeres: “La justicia no se da solo en un juicio en particular; significa tener derechos y poder vivir vidas dignas”.

La Oficina del Alto Comisionado de Naciones Unidas y la Comisión Interamericana de DDHH han expresado también su preocupación y recomendaciones, como puede verse en los siguientes estudios de Naciones



Unidas sobre La lucha contra la discriminación de la mujer.

Se ha detectado que el trato prejuicioso lo es más cuando quienes las evalúan o deciden son mujeres en causas en que intervienen mujeres en un rol relevante.

Eso es lo que se conoce como Misoginia Judicial, y cuyo reconocimiento y combate ha llevado, entre otras consecuencias positivas, a la progresiva instalación de conceptos tales como la paridad de género y a corrientes más modernas en la Victimología, como lo es la aparición de la Víctimo–Dogmática, de la Justicia de Género, o con perspectiva de género (Gender Justice).

Especialmente duro es conocer del trato cruel e inhumano recibido por niñas esclavas, prisioneras o violadas sistemáticamente en medio de las matanzas y guerrillas de África reciente, en razón de su condición de mujeres, cuestión que ha sido materia de recientes fallos ante la Corte Penal Internacional, dado que conforme al Estatuto de Roma estas conductas son de esas grandes atrocidades consideradas crímenes globales de guerra o contra la humanidad toda, y deben ser tanto reprochados como llamar enérgicamente la atención para que se adopten los grados de consciencia que impidan su repetición.

Así en el Caso Ongwen, lo destacaba ya UNICEF desde el año 2012 y es asunto de otras causas en curso.

En marzo de 2019, por invitación de la Asociación de Mujeres Abogadas de África (AWLA), expuse en la NGO CW63 de Nueva York, USA, en la preparatoria de la Conferencia Mundial del estatus de la Mujer en el Mundo, Beijing25+, al amparo de Naciones Unidas, el estado de la Jurisprudencia de la CPI acerca de los delitos internacionales contra mujeres, y en el Panel, destacadas académicas y Juezas Federales de Estados Unidos levantaron en la agenda estadísticas analizadas sobre cómo en sistemas más modernos de sociedad, la misoginia judicial aparecía muy presente en temas laborales, de inmigración, familia, raciales o de control del orden público, etc.

Ver <https://www.unodc.org/dohadeclaration/en/news/2019/01/the-role-of-women-judges-and-a-gender-perspective-in-ensuring-judicial-independence-and-integrity.html>

Pero de todos modos hay que practicar la ponderación y la prudencia, porque el lenguaje fácil aplica muy velozmente la “Ley del Péndulo”, como se ha visto en esos casos de jueces y sus familias amenazados por dictar sentencias “machistas” o “misóginas”, que a veces, menos que eso, parecen ser decisiones no del todo bien fundadas, que no gustan a quien pierde, como se lee en el artículo de ABC News titulado “Las amenazas a los jueces están aumentando y los expertos dicen que la misoginia es un problema”.

Espacio Digital y Machismo

A poco andar de esa Conferencia mundial, y a propósito del estudio del riesgo de prejuicio, sesgo o de intromisión indebida en la privacidad del ámbito de seguridad del ciudadano, a través del uso de las herramientas de Inteligencia Artificial (IA), los desarrollos de Machine Learning, y del avance den uso del Reconocimiento Facial (FR), Apps Biométricas y Algoritmos Predictivos en el sistema procesal penal comparado , fuimos detectando las alertas de diversas fuentes que llamaban la atención sobre la aparición de los primeros atisbos de que, al parecer, en el ecosistema digital y en la vida en la Net, así como en las herramientas de vigilancia digital de calles y de tráfico en la red, se estarían replicando modelos misóginos o machistas de la vida real, con mayor énfasis (otra vez) puesto en las mujeres.

Interesante es leer la nota de EuroNews que el pasado 8M21 se preguntaba en la Efeméride: ¿Cuan sexistas pueden ser los algoritmos?

Así, por ejemplo, se dice que ocurre al buscar perfiles de trabajo, los que en razón del color de piel, o si la mujer es latinas, etc. la navegación conduce más rápido a páginas de record criminales o a sitios de pornografía, que cuando se usa la biometría o FR de mujeres caucásicas blancas,, y que también por eso en un aeropuerto con cámaras para pasaporte covid19 si es rubia o blanca, entre otras razones puede saltar la fila más rápido que la afro americana, asiática o latina, las



que tienen “más probabilidades de volver a la fila de espera” que aquellas.

Esto pasa, señalan los expertos, porque las grandes compañías de RRSS obtienen los estereotipos con que alimentan los algoritmos desde los millones de fotos de seres humanos de lo que las personas suben, o de sus navegaciones trackeadas y perfiladas, con los que luego las tecnológicas arman las bases de datos que comercian con Estados, Gobiernos y Empresas, como quien hace minería digital de millones de Teras de datos hallados en una cantera gratis.

En consecuencia, tenemos otro estímulo para avanzar en la regulación constitucional del Estado de Derecho Digital, igual como queremos la menor latencia de espera que daría la 5G.

- 4- *Feminismo en Chile: Una lucha centenaria y vigente en la voz de sus protagonistas.* <http://www.humanas.cl/16196/>
- 5- <https://revistaderecho.ucn.cl/index.php/teologia/article/download/3341/3057/10839>
- 6- *Formas de la alteridad: un reto epistemológico y político.* Donovan Adrián Hernández Castellanos. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-00632011000200002
- 7- <https://www.latercera.com/paula/el-patriarcado-es-un-juez-por-que-la-practica-judicial-es-discriminatoria-contras-las-mujeres-en-chile/>
- 8- <https://www.ohchr.org/SP/AboutUs/Pages/DiscriminationAgainstWomen.aspx> y <https://www.cidh.oas.org/women/acceso07/cap1.htm>
- 9- <https://www.theleaflet.in/unmasking-the-misogyny-of-indian-courts/>
- 10- <https://dpej.rae.es/lema/victimodogm%C3%A1tica>
- 11- <https://www.iccpi.int/Pages/item.aspx?name=pr1564>
- 12- https://www.unicef.org/spanish/protection/57929_62002.html
- 13- <https://www.corteidh.or.cr/tablas/r37874.pdf>
- 14- <https://abcnews.go.com/US/threats-judges-increasing-experts-misogyny-problem/story?id=72061296>
- 15- <https://enestrado.com/inteligencia-artificial-sistema-de-justicia-derecho-penal-e-commerce-y-democracia-donde-estamos-y-para-donde-vamos-por-juan-carlos-manriquez>
- 16- <https://enestrado.com/reconocimiento-facial-y-tecnologia-intrusiva-porque-la-moratoria-de-la-ue-y-cuales-criterios-las-hacen-admisibles-por-juan-carlos-manriquez/?fbclid=IwAR2ThG3uacbvLJPMRjLcEGB5Gmfqcq4IHxUNxDEtq9Vzv8B9iN6SZTS4>
- 17- <https://www.euronews.com/2020/03/08/international-women-s-day-our-algorithms-are-sexist>

RECONOCIMIENTO FACIAL Y TECNOLOGÍA INTRUSIVA: POR QUÉ LA MORATORIA DE LA UE Y CUÁLES CRITERIOS LAS HACEN ADMISIBLES.

EUROPOL, EDEN y ERA llevaron a cabo el 16.12.2020 desde La Haya y Londres un Panel Internacional por medio de una novedosa plataforma interactiva, una “isla virtual”, dedicado en extenso al tema “Reforzando la legalidad en la era de la Inteligencia Artificial y Big Data: la Democracia bajo amenaza”.

La mesa sobre Reconocimiento Facial dejó planteado porqué en Europa se ha optado por una “moratoria” en la aplicación de esta tecnología, dado, entre muchos aspectos de cuidado, su alto nivel de error 1:N, sesgo, prejuicio racial, falta de control del insumo con que las policías alimentan las bases de rostros, cómo y de dónde los obtienen, y por el peligro de afectar la presunción de inocencia y otras libertades civiles de manera innecesaria o desproporcionada. Ejemplos hay con la Policía de New York y con la Policía Metropolitana de Londres.

El lector interesado podrá hallar acá el estado del asunto y ver el mapa completo de Europa sobre la permisividad, la prohibición, restricción o regulación del RF en el espacio común y por qué las organizaciones civiles se oponen.

De igual modo, EUROPOL y la Academia están relevando un aspecto procesal penal relativo a la “prueba o herramientas digitales o de recolección de evidencia por Inteligencia Artificial”, por ejemplo, como ocurre con el “reconocimiento de emociones” asociado al reconocimiento facial, aditivo que podría ser presentado por las Policías o las Fiscalías como “indicios serios” de conexión con un hecho penal o con la voluntad o propósito y fin de llevarlo a cabo, cuando no se tiene evidencia directa o una confesión.

O sea, han detectado el peligro que sin mayor filtro y control judicial estricto, se sumen como un ingrediente más en el debate de audiencias o juicios para fijar “hechos” por medio de esa técnica de “neo evidencia”

que podría establecer indicios que den base a una su-puesta prueba indirecta, desarrollada sugestivamente cuadro a cuadro por quien exponga el caso ante el tribunal. Así lo ha ido tratando la ABA (American Bar Association) en el artículo de Kristine Hamann y Rachel Smith titulado “Tecnología de reconocimiento facial: ¿a dónde nos llevará?”.

La UE, si bien tiene una fuerte legislación de protección de la privacidad incluso en lugares públicos, no ha definido del todo que se hará con el RF, como lo destaca el sitio de noticias de investigación BiometricUpdate.com en el artículo “La Comisión Europea no ha descartado por completo la prohibición del reconocimiento facial biométrico en espacios públicos”.

Sin embargo, se han ido creando criterios de Admisibilidad que podrían validar su uso y rendimiento ante los tribunales sin violar los derechos fundamentales de los ciudadanos, como puede verse en comparado entre USA y la UE en Celentino: 2016.

Invito a leer la práctica y dudas de los defensores públicos de USA en Jackson: 2019 https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf

En este contexto, preocupa que sin más en Chile se gaste muchos millones de dólares en tecnología de vigilancia por medio de herramientas de IA para generar evidencia, sin conocer bien su origen, si controlan la fuga de datos o cuál es su nivel de actualidad para superar las objeciones técnicas y legales que hemos venido expresando y, sobre todo, que pueda generarse una “Admisibilidad Automática” de sus hallazgos sin un contrapeso efectivo.

En tal sentido, un fallo quizás polémico por los hechos que encierra, pero que está en la línea de la Tutela Judicial Efectiva, es aquel del TOP de Santa Cruz (RIT 54-2020, RUC 1.901.382.973-2) que absolvió a imputados de traficar droga, porque la evidencia incriminante se logró con un dron que sobrevoló una propiedad privada sin autorización judicial previa, violando el art. 19.4 de la Constitución.

18- <https://euobserver.com/science/148839>

19- https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/

20- <https://www.biometricupdate.com/202009/european-commission-hasnt-completely-ruled-out-biometric-facial-recognition-ban-in-public-spaces>

21- <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1261&context=mlr>

NEURODERECHOS, BRAIN PRIVACY, INTELIGENCIA ARTIFICIAL Y PREDICTIBILIDAD DELICTIVA POR USO DE ALGORITMOS.

¿De qué estamos hablando?

El cerebro humano es al mismo tiempo que un almacenista, procesador, analista y clasificador de datos, un motor de búsqueda y ayuda en la toma de decisiones proyectivas que opera casi de forma instantánea, acogiendo y descartando alternativas en milisegundos, por múltiples razones, valoraciones y motivos de la persona a la cual pertenece. El Dr. Rafael Yuste, neurobiólogo de la Universidad de Columbia, hace años viene ocupado en su proyecto BRAIN alertando de los enormes beneficios y riesgos asociados al tema.

The Economist (4 de enero de 2018), informó hace un tiempo que desde 2013, diversas entidades públicas de Estados Unidos de América, la Unión Europea y China (principalmente) están invirtiendo miles de millones de dólares en el estudio del cerebro humano, en una competencia similar a la “Carrera Espacial”, entre EE.UU. y la ex URSS en el siglo veinte.

El mayor reto es “conectar el cerebro humano con los computadores”, para “aumentar su capacidad de funcionamiento”, y así lograr una simbiosis de común beneficio. (Neurotecnologías: los desafíos de conectar el cerebro humano y computadores. Mega iniciativas de investigación del cerebro humano Unión Europea: “Human Brain Project”, 2013./BCN: Roberts: Frontera 1: 2019).

Un marco normativo de frontera

Es en esta realidad que ha surgido la preocupación global, desde la Bioética y el Bioderecho, de avanzar hacia una regulación legal internacional y local para darle “protección a los neurodatos y generar neuroderechos”, y uno de los más relevantes es el derecho a la privacidad mental.

El “derecho a la privacidad mental” se orienta a refor-

zar la inviolabilidad del cerebro, que el contenido de la mente sea privado y que no se pueda ingresar a ese ámbito de protección sin consentimiento y advertencia expresa previas.

Se busca evitar la manipulación de los procesos cerebrales de toma de decisiones, ya que el avance imparable de la Inteligencia Artificial (AI) y el uso de algoritmos predictivos del comportamiento humano en diversas herramientas de conexión a las redes sociales y a las “carreteras de la información” que colman la NET mundial y a las cuales miles de millones de personas están conectadas permanentemente, permitirían aplicar técnicas de BIG DATA para generar campañas de bombing sobre los usuarios de los smartphones, principalmente en el e-commerce de “última milla”, bajo el paraguas de “facilitar la vida y la experiencia de compra”, pero en verdad, y al mismo tiempo, estarían determinando los espacios de libertad de decisión del titular, mediante una potencial invasión a la “privacidad cerebral”.

¿Por qué esta regulación es necesaria?

Las consecuencias del avance de la neurociencia y la “interconexión de ser humano y máquina” que ya trató el icónico filme Blade Runner (Scott : 1982) se dejan ver hoy en varios aspectos:

A) El cyborg como objeto- sujeto de regulación legal. Ya en un juicio civil del actor Arnold Schwarzenegger contra una empresa de robótica por usar la imagen suya en uno de sus más connotados personajes, y otra vez por usar el nombre del cyborg en una camioneta, ha hecho que la justicia de USA se haya ocupado del concepto de cyborg y sus efectos jurídicos.

También el caso del joven acromatopsico Neill ha dado la vuelta al mundo, al decir que los “cyborg reclaman sus derechos”.

B) La “libertad de contratación” en el derecho de protección al consumidor digital. El comercio electrónico se basa en la velocidad de oferta, venta y entrega “satisfactoria” al cliente, en el menor tiempo posible, por las mejores rutas, para que la “experiencia de compra” sea de la mayor aceptación. Y eso supone saber “todo lo posible” del cliente.

«El Big Data también juega un papel importante en la optimización de las rutas de entregas y mejoras de los procesos. A través de los datos en tiempo real del tránsito y el clima se pueden calcular las mejores rutas y realizar un seguimiento exhaustivo del estado y de la situación de todos los envíos para, entre otras cosas, detectar posibles incidentes. Esto supone un notable ahorro económico para nuestra empresa y un beneficio para el cliente», explica a iProUP Mauricio Boiko, CEO y cofundador de Welivery, una startup argentina que está comenzando su desembarco en Chile.

C) AI, Big Data y Algoritmos para Predicción Delictiva. De ello me ocupé en mi columna “Inteligencia Artificial en la ‘predicción delictiva’: Criminología y Política Criminal en base a Algoritmos. Ventajas y Riesgos”.

Entonces, el proyecto de ley sobre Neuroderechos que se pondrá a tramitación y debate muy pronto en el Congreso Nacional de Chile (El Mercurio, A10, 03.10.2020) abrirá espacio para analizar con la mayor profundidad posible el estado y consecuencias del problema, y poner en tensión el nuevo artículo 19. 4 de la Constitución Política, que considera la protección de la privacidad de los datos personales como un derecho humano, ya que solo ahí sabremos si el derecho a la BRAIN PRIVACY está o estará realmente protegido, o podríamos una vez más ser sujetos del riesgo de quedar expuestos, especialmente en el ámbito de la Seguridad Pública, de la Política Criminal y del Derecho Penal, a una modernísima policía del pensamiento, donde la máxima “Cogitationis Poenam Nemo Patitur” (los pensamientos no se castigan) que de sólo relegada a las añosas bibliotecas.



23- <https://amp.elmundo.es/papel/lideres/2018/07/07/5b3fa10122601d942c8b4593.html>
 24- https://elpais.com/elpais/2020/01/30/ciencia/1580381695_084761.amp.htm
 25- <https://www.whatsnew.com/2020/03/14/arnold-schwarzenegger-demanda-a-empresa-robotica-por-replicar-su-rostro-sin-permiso-para-crear-un-robot/amp/>
 26- https://www.bbc.com/mundo/noticias/2013/07/130702_tecnologia_cyborg_harbisson_aa.am
 27- <https://www.america-retail.com/e-commerce/e-commerce-sabes-el-secreto-de-la-ultima-milla-por-que-las-empresas-dicen-que-es-la-llave-para-bajar-costos-y-ganar-ventas/>
 28- <https://mbcia.cl/2020/05/04/inteligencia-artificial-en-la-prediccion-delictiva-criminologia-y-politica-criminal-en-base-a-algoritmos-ventajas-y-riesgos/>

MARCO NORMATIVO DE LOS DELITOS INFORMÁTICOS Y CIBERNÉTICOS EN CHILE.

Una reiteración y al enfoque nacional

El derecho penal económico moderno concibe a los delitos informáticos, cibernéticos y a los crímenes contra la ciberseguridad, cuando tienen una significación económica funcional, como afectaciones a sistemas, de un gran poder expansivo, y es así que la preceptiva objetiva nacional y los criterios sobre los que se dictó la ya añosa Ley 19.223, sobre delitos informáticos, ha llegado el último tiempo “dos veces tarde” para enfrentar la criminalidad que se da en la a-espacialidad, que es la gran característica de la web cuando se trata de situar el tempus y el locci delicti.

En el ámbito de la delincuencia cibernética, más que aplicar la “sociedad del riesgo global “ (Beck: 1995), en materia del tratamiento de la información, debemos tener en cuenta que el “objeto de deseo” hoy son los datos, los sistemas de información, las data bases que son sumamente valiosas: el dato es el nuevo petróleo, y particularmente la información financiera y la conducta del usuario, predecible luego de trackearla y procesarla usando algoritmos, Inteligencia Artificial (IA), herramientas biométricas (huellas y reconocimiento facial, FR), etc.

Esta neo-realidad no ocurre en un lugar como tradicionalmente lo concebimos. Se trata de la circulación por carreteras virtuales en que los datos se encuentran y entrelazan por miles de millones de TeraBytes por segundo.

Y es por eso que para la internet se ha tenido que ir generando necesariamente desde fuera una regulación, para que no se convierta en tierra de nadie: es lo que denominamos el Nuevo Estado de Derecho Digital 4.0. Aíí, ese “lugar” que es la web no podrá quedar entregado a las fuerzas innominadas e indómitas de cualquiera, sino que sujeto a reglas claras, precisas y universales. Aunque varios no lo quieran así.

¿Por qué regular la net?

Porque desde la Doctrina y la Ciencia se reconoce que

el uso y expansión de los mecanismos del alter ego digital, anonimización, seudonimización, el block chain y otra serie de cuestiones vinculadas a la protección de datos y la ciberseguridad, hacen necesario generar reglas, límites protecciones y sanciones que permitan a los Estados y a las personas y empresas saber cómo y hasta dónde actuar en el ámbito de la seguridad y protegerse de amenazas.

También para saber dónde están los límites y sobre todo, para que los Estados y sus parlamentos sean capaces de tipificar conductas con una técnica legislativa de buena factura, y que estos tipos de ilícitos dejen de ser considerados más que simple felonías para tratarlos como verdaderos crímenes o delitos muy lesivos con efectos expansivos enormes, por ejemplo en el sistema de pensiones (pensemos en el Caso Enron en su época), aunque no sean aparentes, porque no hay sangre, y no se tomen en principio tan en serio, más aún a propósito de amenazas especialmente graves, como el ciberterrorismo, los secuestros informáticos de bases de datos, de mail; la piratería, el pillaje de datos y el robo, comercialización a competidores de secretos informáticos, etc.

De ahí que sea necesario sobre esta realidad, valerse de herramientas nuevas que puedan quedar sujetas al marco normativo global, y a pesos y contrapesos, a objeto que en Chile se aplique una normatividad positiva vigente.

¿Qué ocurre en Chile? ¿Qué ha pasado con la Ley 19.223?

La Ley 19223, sobre delitos informáticos, pretende proteger, al igual que las reglas penales generales, bienes jurídicos, o sea, intereses de especial relevancia para sus titulares, en tanto sujetos, personas naturales o jurídicas dignas de protección criminal frente a conductas que los pueden dañar o poner en riesgo jurídicamente relevante.

El problema comienza ya con el bien jurídico protegido. La ley quedó demasiado sujeta al concepto tradicional de la propiedad dominical de cosas corporales, sabiendo que la información y los datos son inmateriales, y bien pueden estar alojados en bandas magnéticas, chips o iCloud de una tarjeta de débito o crédito,

por lo que no son más que un conjunto de pulsos electrónicos.

De ahí que cuando se tuvo que dictar y luego aplicar la Ley 20.009, sobre uso malicioso o apoderamiento de tarjetas de crédito o débito, se generó un arduo debate: determinar si se trataba de apoderamiento de cosas muebles o no; si la tarjeta de un cajero era una llave o no y si a alguien le sustraían la tarjeta verdadera y si apoderaban de su clave y sustraían el dinero en cuenta corriente, acaso eso no era el robo, en lugar cerrado con ingreso con llave verdadera sustraída del art. 440 del Código Penal.

Ante la realidad y el avance tecnológico es que nos hemos ido dando cuenta el nivel de insuficiencia de esta preceptiva para tratar con estos problemas tan reales, nuevos y acuciantes, al no dar las respuestas adecuadas. Así, ¿La banda magnética? ¿La tarjeta? ¿La clave? ¿El mecanismo Touchless? ¿El medio Bluetooth? ¿El cajero sobre el cual recae la digitación de la clave? Cuál es el objeto de ataque y cuál el objeto material y/o el objeto jurídico protegido en la norma? ¿O se trata de tipos pluri ofensivos?

Nada de lo que interesa apropiarse a los hechos es una cosa corporal mueble allí. Entonces, si no es así el hurto del 432 del CP, el robo del 436 y del 440 del CP quedan completamente desplazados.

(Gómez Mieres).

La ley 19. 223 buscó proteger un “nuevo” bien jurídico, surgido a propósito de las tecnologías computacionales y ese bien jurídico sería la calidad y la pureza de la información en cuanto tal, ya que no es la propiedad corporal mueble, pasa a ser la idoneidad de la información, y en otros casos, la integridad del sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. La Prof. Laura Mayer se ha hecho cargo el asunto del bien protegido.

En 4 artículos se definieron diversas formas de delito informático, que como dicen los autores “son todas aquellas acciones u omisiones, típicas antijurídicas y dolosas, cometidas ya sea todos o aislados contra personas naturales o jurídicas, que se realizan con uso de un sistema de tratamiento de información destinadas al perjuicio de la víctima.” (Huerta y Líbano: 1996).

¿A través de qué? De atentados a la tecnología informática, lo cual normalmente va a producir daños colaterales, lesiones de carácter patrimonial, con tal que se actúe con ánimo de lucro, o solo por dañar, o por injerir en un ámbito de protección y privacidad ajena y apoderarse o destruir los datos que allí están etc.

Pero los dos grupos de ilícitos que contiene la ley:



- a) El primero es sabotaje informático,
- b) El segundo dice relación con espionaje informático, y a su vez se dividen en dos categorías distintas:
 - i. Atendiendo al objeto al que se atenta, o
 - ii. Al modo de operación.

Han sido insuficientes para el caso de secuestro de datos o ransomware que afecta a BancoEstado.

¿Qué debemos hacer?

Además de una verdadera política integral de ciberseguridad, votar la ley que acoge el Convenio de Budapest para el ordenamiento jurídico nacional, que sustituye la Ley 19.223 e incorpora nuevas herramientas de tipicidad, persecución y descubrimiento de estos ilícitos económicos modernos.

Las actuales formas de fraude de identidad o de malware, e incluso el caso del Garbaging (robo de la información que entrega la basura), que ejemplifico como el “Crimen del Pingüino” (el archienemigo de Batman, que se hizo poderoso y rico recolectando en las esclusas y túneles subterráneos donde vivía, la información destruida por los influyentes de Gótica, para luego extorsionarlos), no pueden pesquisar con eficiencia.

Todas estas figuras de sabotaje informático, de acceso no autorizado, etc, han quedado atrasadas y también los tipos penales de la Ley 19. 223.

Los invito particularmente a ver el FBI Report y el Europol Report 2020 en la materia. (FBI Report: <https://www.justice.gov/elderjustice/internet-crimes>).

Por eso, en el Programa Derecho, Ciencia y Tecnología de la UC abordamos con mucho detalle, días antes del delito que afecta a BancoEstado, y en el contexto del Diplomado en Protección de Datos, estos asuntos tan actuales que el Parlamento debiera votar con suma urgencia, pues la tramitación legislativa está agotada.



Fake News en Pandemia: mentira, cyberwar y riesgo de daño a la vida y salud.

Las Fake News son “la divulgación de noticias falsas que provocan un peligroso círculo de desinformación, la difusión de contenido engañoso, falso o fabricado, en un contexto de pos verdad”. (IFJ/FIP: Federación Internacional de Periodistas).

Hoy su uso masivo se sitúa en el contexto de la guerra cibernética, de las tácticas de desinformación y de contra inteligencia digital, apelando a la capacidad de generar relato instantáneo que tiene el meme, y a la hiper expansión en tiempo real hacia plataformas tales como Twitter, Facebook, Instagram y otras, que repercuten en milésimas de segundo una “realidad” de likes muchas veces alimentados por Bots dependientes de campañas masivas de formación de opinión, que millones de destinatarios suelen asumir como “verdad” inmediata, instalando una “versión” oficial de algo que no existe.

No cabe confundirlas con las filtraciones de hechos (fact) de la vida privada o pública de una persona pública, que pueden ser de legítimo interés común, pues las motivaciones o fines que condicionan la actuación de gobernantes, altos funcionarios internacionales, líderes de opinión, Gurús, Popes, o incluso de “influencers”, deberían ser conocidas para un real control de legitimidad y licitud de sus actos, cuyas consecuencias gobiernan nuestras vidas a nivel global, nacional o comunal.

El tradicional respeto a la libertad de expresión (“free speech”) de la Primera Enmienda a la Constitución de USA, y su moderna expresión del “derecho a saber”, como base del “derecho a informar y a ser informado” es una piedra angular de la democracia liberal occidental. En ella se han parado los defensores de Assange, de Anonymous y de Manning, entre otros, para alegar que no pueden ser censurados por sus publicaciones masivas de archivos secretos o robados, ya que la I Enmienda dispone que debe ser incluso tolerado el discurso más ácido y no por eso ha de ser tenido por difamatorio. Luego del Affaire Clinton el Gobierno norteamericano ha catalogado a Wikileaks como una

organización terrorista, pesquisable de acuerdo a la PatriotACT.

Chile recoge esos principios en los arts. 5 inciso 2, 19 de la Constitución y en la Ley 19.733, sobre ejercicio del periodismo y profesiones afines, y no son pocos los fallos en sonoros casos penales que han dictaminado que difundir hechos que pueden revestir interés público no son injuria. El Séptimo Juzgado de Garantía de Santiago lo dijo el 7. 8.2006 cuando absolvió al ex Senador Nelson Ávila de una querrela que le iniciara otro ex parlamentario por supuesta difamación, al estimar que en sus dichos primó el interés público.

Sin embargo, las Fake News son un arma peligrosa y sin duda éticamente inaceptables. El CNTV el 26.12.2019, en su informe “Noticias Falsas y Regulación” ha dicho que se vio en la necesidad de dar directrices “de fomento a la alfabetización mediática” dada la expansión del fenómeno.

Es un esfuerzo que debe ahondarse ¿Por qué?

Porque incluso las noticias falsas de tono menor, que dan alarma de calamidad a la población, por medio de la aseveración de hechos falsos, son delito, según el art. 268 Bis del Código Penal. Por ende, la conducta de distribuir esos audios de WhatsApp alarmistas de “un tío de un amigo, que tiene un primo que va a dejar insumos a tal o cual hospital le dijo que ...”, bien pueden quedar captada por este tipo penal.

Los otros mails o tweets que están en la raya con el fraude informático (por ejemplo, los que promueven la bondad de ciertos o tales productos químicos que matan el Covid-19, o que ingeridos, le dan inocuidad al virus), pueden ser considerados autoría por inducción de lesiones graves (art. 15 número 2 y art. 398 del Código Penal), pues hacen nacer en otros el ánimo de suministrarse bebidas o sustancias nocivas para la salud individual, lo que puede aumentarse por la credulidad o flaqueza de espíritu de la gente. Peor aún, si alguien muere, el delito de homicidio simple también puede alcanzarlos (art. 391 número 2 del Código Penal).

Si alguien propala falsamente por RRSS que violar la cuarentena sin estar enfermo o siendo asintomático lo salva de la sanción, la autoría de noticia falsa será castigable en concurso con la autoría por inducción o mediata de los arts. 318 y 318 Bis del Código Penal, como infracción a las normas de salud pública impuestas por la autoridad.

EVIDENCIA DIGITAL, ANÁLISIS FORENSE, IA Y ALGORITMOS PREDICTIVOS: RETOS DE LITIGACIÓN MODERNA PARA EL CÓDIGO PROCESAL PENAL DE CHILE. POR JUAN CARLOS MANRIQUEZ.

Por Juan Carlos Manríquez R., Abogado, LLM (CWSL, USA); Profesor LLM UC, Especialista en Derecho Penal Económico y de la Empresa (UCLM, España), AD en Derecho Penal Internacional (Siracusa, Italia) Litigante ante la Corte Penal Internacional (La Haya, Holanda). Director de Compliance Academy.

¿Dónde estamos?

La ciberdelincuencia, las formas actuales de lavado de activos y el crimen organizado moderno plantean grandes retos para las ciencias penales y para la investigación de la criminalidad compleja. En Europa, Europol; en USA, el FBI; la Interpol, a nivel global, y en UK, con la creación de la plataforma cyberalarm.police.uk se ha advertido en particular sobre el desarrollo de la ciberdelincuencia. Se puede ver una verdadera campaña de prevención, educación pública y acceso oportuno a la respuesta en <https://www.fbi.gov/investigate/cyber/news>.

En Chile, Conversatorio Judicial hace unos pocos días llevó a efecto un interesante webinar internacional en que expusimos aspectos criminológicos, dogmáticos, normativos y procesales en relación con este fenómeno. (<https://enestrado.com/ciberdelitos-penalista-analiza-cual-es-perfil-y-sofisticacion-de-los-nuevos-delinquentes-de-la-red/>).

Se trata de desafíos que transitan desde las teorías y la dogmática de la imputación penal, pasan por el planteamiento de las nuevas formas de intervención y se topan con los aspectos que tienen su correlato en lo procesal penal, con la creación y aplicación de nuevas técnicas investigativas para hacerles frente. (Así se describe en <https://ficp.es/wp-content/uploads/2017/06/Lapuerta-Irigoyen.-Comunicaci%C3%B3n.pdf>).

Y en el centro de toda esta situación se halla la



explosión de la tecnología de las comunicaciones, la masificación de las herramientas y dispositivos digitales, los avances de la IA, del Machine Learning y de la Predictibilidad Algorítmica, que junto al uso de criptoactivos y del blockchain en el día a día de la “nueva realidad” post pandemia nos obligan a replantear especialmente los conceptos básicos acerca de la generación, obtención, tratamiento y rendición de la evidencia digital, bajo estándares aceptables de Debido Proceso y pleno respeto a los DD.HH. Así lo tratamos, entre otras publicaciones, en <http://enestrado.com/neuroderechos-brain-privacy-inteligencia-artificial-y-predictibilidad-delictiva-por-uso-de-algoritmos-por-juan-carlos-manriquez/>.

Los efectos de esta ola o salto tecnológico se hacen sentir no sólo sobre las relaciones económicas, sino que también en los sistemas de justicia civiles, comerciales y penales, domésticos e internacionales, que deben hacerse cargo de ellos de modo innegable. Algo dijimos en <http://enestrado.com/inteligencia-artificial-sistema-de-justicia-derecho-penal-e-commerce-y-democracia-donde-estamos-y-para-donde-vamos-por-juan-carlos-manriquez/>.

Es tal la relevancia que ha ido adquiriendo la aplicación de la IA y el uso de las herramientas cibernéticas en el ámbito jurídico, nacional, internacional y transfronterizo, que la Asociación Internacional de Derecho Penal (AIDP) ha convocado a su Congreso Mundial a los especialistas de las ciencias criminales y forenses para abordar las diferentes aristas del asunto, haciendo énfasis en el peso que pueden tener sobre cómo se adopten las decisiones en la Justicia Criminal de acá en adelante, como lo deja en claro <http://www.penal.org/es/call-papers-ai-big-data-and-automated-decision-making-criminal-justice>.

Y es en este contexto donde especialmente debemos poner atención a la generación y uso de la evidencia proveniente del ecosistema digital que pretenda ser validada en los procesos penales con fines incriminantes o defensivos y tratar de indagar dónde están sus bases y límites legitimantes, como ya se debate a nivel global. En tal sentido Blanco: 2020, Tecnología Informática e Investigación Criminal (Thomson Reuters).

¿PARA DÓNDE VAMOS?

A) Qué es la evidencia digital.

Para Taruffo la evidencia es un antecedente que permite reconstruir o establecer los hechos, y que especialmente en materias científicas, ha de ser sometida a un arduo escrutinio, como bien lo dice Meneses (2009), en una reseña sobre La Prueba, dada: “...la necesidad de someter a crítica los antecedentes probatorios, para obtener de ellos una información relevante y jurídicamente admisible, y a la vez un sustento empírico adecuado para la decisión del conflicto. Especialmente categórico es el trabajo sobre la prueba científica (pp. 277-295), donde Taruffo enfatiza la importancia del control que deben hacer las partes y, en especial medida, el juez con respecto a las conclusiones que presenta la ciencia en las cuestiones sometidas a juicio; destaca algunos parámetros que deben considerar los tribunales para establecer la suficiencia de este tipo de probanzas y, sobre todo, a partir del precedente dado por la Suprema Corte estadounidense en el caso Daubert, subraya la necesidad de operar de un modo falsacionista, sometiendo a extrema crítica las opiniones de los expertos y velando por la validez y fiabilidad de los métodos empleados en este tipo de evidencias (pp. 283-285, 293-295)”

En el sistema procesal civil y penal se hace cierto distinguo entre antecedente, evidencia y prueba, en una relación de género a especie, atendiendo a su funcionalidad, intensidad y capacidad de “generar convicción” o capacidad de ser “preferida” a otras que pretenden igualmente persuadir a los jueces de las respectivas Teorías del Caso. Así, Miranda Estrampes, Cerda San Martín y Hermosilla Iriarte, en Práctica de la Prueba en el Juicio Oral (Librotecnia: 2012).

La Evidencia Digital (ED), o la prueba electrónica, es de este modo “cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio”. Así se trata en este artículo.

O podría ser concebida también como “... un registro de la información guardada o difundida a través de un sistema informático que puede utilizarse como prueba en un proceso”. Interesante es estudiar el Manual de Evidencia Digital publicado por la OEA y que entrega definiciones y distinciones muy útiles en https://www.oas.org/juridico/english/cyb_pan_manual.pdf.

Su característica principal es que se trata de información generada o almacenada en un ambiente digital, que por su pertinencia e importancia (en ese orden) puede ser usada en un proceso judicial.

El desarrollo de las tecnologías de la información y la capacidad de interconexión de saberes y habilidades ha ido abriendo campos de aplicación hasta hace poco impensados para la generación, aplicación y rendición de evidencia digital ante los jueces y un arsenal de nuevas herramientas para generarla, reunirla y sacarle rendimiento en los procesos civiles y penales. Son esas “nuevas formas de comunicación mediante Internet, la encriptación, la esteganografía, las herramientas para procurar el anonimato en la Red, las criptomonedas, la ‘Internet de las cosas’, el ‘Big data’, la inteligencia artificial, los algoritmos predictivos, los ‘programas espías’ (“spyware”) y otras novedosas herramientas de vigilancia digital, [cuyo] impacto de las mismas sobre el alcance de las tradicionales garantías constitucionales y sobre las facultades estatales para monitorear (legalmente) la actividad de los ciudadanos” a las que se debe atender, como bien dice Blanco.

La tecnología informática en la investigación criminal, como el uso de hackers por parte del Estado (spyware legal, nuevas técnicas de vigilancia, acceso remoto a datos informáticos, búsquedas transfronterizas, descriptación compulsiva y derecho a guardar silencio, anonimización y agente encubierto digital, big data y software predictivo; obtención, resguardo y análisis forense de la evidencia digital; deep fakes y prueba informática aportada por hackers) entre otros tópicos, ya no nos pueden ser ajenos.

Veamos dónde y cómo se han ido manifestando estas nuevas necesidades y problemas.



B) Nuevo análisis forense de campo: modelamiento de Sitios del Suceso y rol de la IA. La experiencia de la Justicia Penal Internacional.

Uno de esos casos ejemplares de uso de evidencia y procesamiento digital de información que puede ser usada en procesos complejos podemos hallar en la historia de “Digital Detective Agency”.

Ellos hacen análisis y cruce de Google Earth, YouTube y Redes Sociales con Big Data y otras herramientas para posicionar hechos e indagados en casos de posibles delitos contra la humanidad y crímenes de guerra y así darle soporte a las acciones que puedan llevar a los responsables ante la Corte Penal Internacional. Se destacan porque lo que realizan es llamado “Arquitectura Forense”, la modelar escenas del crimen y sus particularidades desde información recuperada en RRSS (<https://www.theguardian.com/law/2021/jun/27/berlins-no-1-digital-detective-agency-is-on-the-trail-of-human-rights-abusers>).

Sus productos evidenciarios han sido reconocidos y usados para condenar a un Líder NeoNazi griego por un discurso anti LGTBI+, y descubrir detalles de una cuestionada defensa que hizo Netanyahu sobre la “muerte accidental” de un profesor Beduino. La colaboración que hacen en sus recreaciones e indagaciones digitales expertos en AI, periodistas de investigación y

arqueólogos se complementa con la idea que en los procesos modernos “The Facts need good litigators” (Los hechos necesitan de buenos litigantes).

Para ellos el trabajo en causas de DD.HH. está cambiando, es un trabajo constante, integrado, como lo han aprendido de sus trabajos en Yemen, y revisando miles de videos de ataques aéreos de la guerra civil en el sudeste de la península arábiga. Han aplicado a su propio software de mapeo datos que “le permiten contar la historia a través del tiempo y del espacio”, o levantar indicios del origen de las municiones usadas desde la ubicación de sus fragmentos.

C) Aplicación de Algoritmos Predictivos en Litigios Laborales, de Familia y de Abuso Sexual Infantil.

Hemos hablado antes de la aplicación de algoritmos predictivos en el sistema de justicia, sus ventajas y riesgos.

En materia laboral se está experimentando su (no) aplicación y efectos en las entrevistas de trabajo o revisión de CV’s y hasta ahora su valoración ha sido controvertida, ya que se dice que dan lugar a una alta tasa de racismo y desigualdad de género, así como los sistemas de reconocimiento de emociones afectan a las minorías sexuales, mermando sus posibilidades de ascenso o de hallar ocupación. En estos casos se ha generado debate sobre si esa evidencia digital (en contra de la IA) serviría para fundar una acción por discriminación o vulneración de derechos del trabajador, por violar su privacidad. Por favor, para una lectura reciente ir a <https://www.brookings.edu/research/auditing-employment-algorithms-for-discrimination/>.

En casos de Abuso Parental y Vulneración de Derechos de Menores también ha habido experiencias y debates con el uso de algoritmos predictivos de conducta. No hay consenso en si ayudan u obstaculizan la adopción de una decisión adecuada, y por ello, si son confiables para decidir tuiciones o medidas de protección, en especial por los problemas de sesgo que se dicen asociados a las bases de datos desde donde perfilan comportamientos, particularmente los raciales y de género (Ver acá).

Advierten no creer en su confiabilidad opiniones diversas, como las que se expresan en este artículo y se refuerzan con sólidas dudas y críticas también en <https://proceedings.mlr.press/v81/chouldechova18a/chouldechova18a.pdf>, del mismo modo que se sostiene en <https://www.wired.com/story/excerpt-from-automating-inequality/amp>

Pero donde los algoritmos sí han logrado más espacio es en materia de obtención y análisis de datos tras colocación y generación de alertas y pesquisa de pedófilos, abusadores o acosadores sexuales de menores en la red y en la deep web. Su nivel de acierto ha dado lugar a una CyberPatrol eficiente y a iniciativas como EU Kids Online https://www.unicef-irc.org/publications/pdf/ict_spa.pdf.

Interpol y otros organismos nacionales competentes han creado bases de datos de imágenes de abusos sexuales infantiles. Mediante la aplicación de un sofisticado programa informático de análisis de imagen, la policía puede evaluar si la imagen de un niño que figura, por ejemplo, en una colección fotográfica que acaba de decomisar es idéntica a otras ya descubiertas por las autoridades policiales; en tal caso, la incluye en una base de datos de imágenes conocidas.

Algunos programas informáticos también sirven para identificar a los niños que han sufrido abusos sexuales durante largos períodos de tiempo, y cuya apariencia física puede haber cambiado radicalmente durante el crecimiento.

Esta información es importante tanto para establecer de manera exhaustiva los cargos contra el presunto autor del delito como para determinar la duración y la naturaleza de los abusos sexuales que ha sufrido un niño con el fin de ayudar a su recuperación.

Las bases de datos de fotografías de las víctimas son recursos valiosos. Pueden ahorrar una gran cantidad de tiempo a la policía y reducir la necesidad de agentes que examinen las imágenes de forma directa. Este último aspecto es muy importante. Hasta hace relativamente poco tiempo, el trabajo policial requería a menudo varias observaciones de las imágenes. Sin embargo, se ha desarrollado una nueva tecnología que reduce las imágenes fotográficas a un código

digital, conocido como hash, una función de trackeo que puede utilizarse para rastrear, localizar y comparar las imágenes sin necesidad de que un agente policial mire la imagen real.

El Relator Especial de las Naciones Unidas sobre la venta de niños, la prostitución infantil y la utilización de niños en la pornografía ha señalado la necesidad de contar con políticas éticas explícitas que aclaren la forma en que se utilizan las imágenes, quién tiene acceso a ellas, en qué circunstancias y cuáles son los derechos de las víctimas a la información sobre el lugar y la forma en que se guardan las imágenes. Las unidades policiales y las líneas de denuncia que se encargan de las imágenes de abusos sexuales de niños suelen establecer protocolos que regulan el período de tiempo y los lugares de inspección y almacenamiento de las imágenes.

Esa es la tendencia y el test último de admisibilidad de la evidencia digital es el balance o ponderación versus las garantías y DD.HH. que se debe hacer cuando se trata de examinar sus límites normativos, éticos y condiciones de legitimidad para que sea admitida en juicio, tal y como lo advertía Taruffo.

Privacidad, Vigilancia y Medidas Intrusivas.

Una mirada rápida sobre el test de legitimidad o ejercicio de ponderación en materia procesal penal, como lo propone Alexy (Derechos Fundamentales, Ponderación y Racionalidad: 2009), nos obliga de todas formas a describir el contexto normativo al que se enfrenta la ED por estos días:

A) Derecho Comparado.

El TEDH en ha dicho que para obtener ED de calidad

hay que cumplir al menos con exigencias éticas, como se lee en <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>, y es sabido que también es necesario ajustarse a parámetros de *lex artis* pericial estricta.

En efecto, La actuación de campo de la recopilación de las evidencias es una actividad extremadamente delicada y compleja. El valor legal y técnico de las evidencias en la mayoría de las ocasiones depende del proceso realizado en la recopilación y preservación de las mismas. La norma ISO/IEC 27037: 2012 “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence” vino a renovar a las ya antiguas directrices RFC 3227, dado que las recomendaciones de la ISO 27037 están más dirigidas a dispositivos actuales y están más de acorde con el estado de la técnica actual. Esta norma ISO 27037 está claramente orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la misma.

CIDH en el Marco de sus Audiencias Regionales se ha venido ocupando del tema, así en 2018 realizó la Audiencia pública “visibilizando el impacto de las tecnologías digitales en los DDHH”, cuya temática principal versó sobre “Inteligencia digital, ciberseguridad y libertad de expresión” en el marco del 167 periodo de sesiones extraordinarias de la Comisión Interamericana de Derechos Humanos que se celebró en Bogotá, Colombia.

El TC Alemán ha dicho que la cibervigilancia a los periodistas de investigación, al amparo de la Ley de Seguridad Nacional, es inconstitucional, y por ende,



ilícita la recopilación de las evidencias así conseguidas, como se puede leer acá y en el comentario de Ignacio Baeriswyl a esa decisión en <https://mbcia.cl/2020/05/26/limitaciones-constitucionales-a-la-vigilancia-de-las-telecomunicaciones-segun-el-tribunal-constitucional-aleman-por-ignacio-baeriswyl/>.

La NSA en USA requiere de autorización de la Corte Especial de Seguridad Nacional para recabar evidencia digital y hacer vigilancia remota, como ya lo comentáramos en la publicación: <https://mbcia.cl/2020/05/15/seguridad-nacional-privacidad-informatica-y-garantias-procesal-penales-en-usa-modificacion-de-la-seccion-215-de-la-ley-patriota-un-debate-de-consecuencias-globales/>.

En el ámbito de las comunicaciones y navegaciones privadas el fallo Carpenter v. US muestra porqué la Suprema Corte anuló una condena lograda por el método de evadir la orden previa para trackear los browser de un sospechoso pretextando que eran “opciones comerciales” cuando en verdad buscaban conectarlo con un delito, fallo que marcó la Jurisprudencia procesal penal más relevante de 2018 – 2019 en el país, al declararse que esa acción de las agencias había violado la IV Enmienda de la Constitución Federal de Estados Unidos.

B) Chile

Hemos dicho que es un problema de DD.HH. <https://mbcia.cl/2020/05/01/experto-en-ciberseguridad-el-problema-de-la-proteccion-de-datos-y-la-privacidad-es-un-problema-de-dd-hh-en-un-estado-de-derecho-digital-4-0/>.

El Marco Normativo viene dado por la CADH (arts. 8 y ss), el PIDCP (arts. 14 y ss); para ciertas materias, como el Lavado de Activos y el Tráfico de Drogas, Trata de Personas, Producción de Pornografía Infantil y Comercio Ilegal de Armas, la Convención de NU contra el Crimen Organizado, y el Protocolo de Palermo II.

Asimismo, los arts. 5, 19.4, 19.5, 19.26 y 38.3 de la Constitución fijan el piso mínimo de la vigencia de la privacidad de datos y comunicaciones, así como la regla general acerca de que toda medida que limita derechos – como las intrusivas de pesquisa criminal –

requieren orden judicial previa, con la excepción cuestionable del art. 31 de la Ley 19.913 ya reprochada en la STC Rol 6973 – 2021 – INA.

Obtención de Evidencia Ilícita y Excepciones.

Para evitar un caso de Violación de Garantías (art. 373 a) CPP) durante el procedimiento o al momento de evaluar la sentencia definitiva, no está demás tener presente algunas normas de detalle.

La tesitura normativa, en el asunto respectivo, enfrentaría al numeral 4 del art. 19 de la Constitución con la Ley de Seguridad Interior del Estado, N° 12.927; con la Ley de Inteligencia, N° 19.974, el DS N° 104, de Estado de Calamidad Pública por Catástrofe Sanitaria derivada de la pandemia de Covid19 y los arts. 222 y siguientes del Código Procesal Penal, entre otras.

Las herramientas y técnicas de investigación que quedan bajo análisis son las medidas intrusivas y que tocan a la privacidad de los datos que hay en el browser del navegador de un usuario nacional.

La necesidad de contar con una orden judicial previa y/o actuar en flagrancia, cuando se trata de invadir privacidad informática, es el nervio del problema.

¿Será lícita la invasión de la privacidad informática por “causas exigentes” de salud pública, consideradas como interés superior y circunstancialmente prevalente?

¿Podremos usar la información residual y/o recurrir al “hallazgo casual” o al “hallazgo inevitable” de indicios de atentado a la salud pública (arts. 318 y 291 del CP), cuando provienen de una investigación previa por Delito Informático (Ley 19.223), Delitos Económico-Financieros (Ley 20.009, Ley 19.913 y Ley 20.393), o Delito Terrorista?

¿Las diligencias de conexión con una imputación penal y sus efectos, efectuadas en este contexto, son diligencias nulas y su resultado es prueba ilícita?

Como podemos apreciar, son múltiples las interrogantes que produce en nuestro sistema el desarrollo de la evidencia digital y por eso razonamos en publicaciones previas cómo en que en Chile podría influencias

una modificación legal como la PatriotAct de USA, que se ve lejana, pero cuyos influjos de política – criminal son relevantes, sobre todo en las corrientes más pragmáticas de “prevención” o de “combate (anticipatorio) contra el delito.

Y toman valor estas dudas en el sistema procesal penal chileno, porque lo cierto es que el abanico de posibilidades para aplicar estas medidas es amplio. Por ejemplo:

- Ley N° 18.314, que determina conductas terroristas y fija su penalidad.
- Ley N° 20.000, que sustituye la Ley N° 19.366, que sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas.
- Código Procesal Penal.
- Ley N° 19.974, de 2004, Sobre Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia.
- Código Penal, en materia de delitos de producción, comercialización, importación, exportación, distribución, difusión o exhibición de pornografía infantil, promoción o facilitación de la prostitución infantil, obtención de servicios sexuales de mayores de catorce pero menores de dieciocho años de edad, a cambio de dinero u otras prestaciones de cualquier naturaleza.
- Ley N° 19.970, que Crea el Sistema de Registros de ADN.

Para estas labores las principales técnicas o métodos intrusivos son:

- Intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas.
- Escucha y grabación electrónica.
- Allanamiento encubierto.
- Levantamiento del secreto bancario.
- Intervención de sistemas y redes informáticas.

- Agente encubierto.
- Observación participante.

De la comparación de las medidas intrusivas existentes en diversas leyes, con las señaladas por el Ejecutivo, que serían materia de indicación al proyecto de ley que determina conductas terroristas y modifica los códigos penal y procesal penal (Boletines 9.692-07 y 9.696-07, refundidos), puede concluirse que todas las medidas señaladas por el Ejecutivo ya están contempladas en la Ley N° 20.000, y algunas de ellas en la Ley 18.314, salvo las de Agente Encubierto, Agente Revelador e Informante, que no se contemplan en esta última ley.

El estudio comparativo de la Biblioteca del Congreso Nacional (BCN), puede verse en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/25222/1/BCN_Medidas_intrusivas_2018.pdf.

El Agente Encubierto Digital.

¿Qué y quién es el agente encubierto en Internet?

El agente encubierto en Internet es aquella persona que actúa con una “identidad supuesta” en canales cerrados de comunicación con la finalidad de esclarecer determinados delitos.

Esta identidad ficticia le habilita para grabar conversaciones y obtener imágenes de encuentros entre el agente y el investigado, así como, para intercambiar y enviar archivos ilícitos por razón de su contenido en el curso de una investigación.

Ejemplo es la Ley 30096 del 22 oct/2013. Segunda disposición complementaria. Ley de delitos informáticos de Perú.

El Agente encubierto electrónico es una figura algo distinta a la del agente encubierto tradicional.

Podríamos decir que el digital actúa como un testigo. Hace exactamente lo mismo que hacemos el resto de personas presentes en Internet; esto es utilizar un nick, un pseudónimo, para no revelar la identidad, con el fin de realizar averiguaciones.

El agente encubierto digital no utiliza un nombre falso, simplemente no revela su verdadera identidad, que normalmente es la de Policía.

En España la STS 173/2018, de 11 de abril, ha dictaminado que en el uso del agente encubierto digital.

[...] no existe afectación del derecho al secreto de las comunicaciones en cuanto uno de los comunicantes es el propio agente. No hay inmisión en una comunicación que establecen terceros, sino comunicación entre agentes y recurrente que no precisa habilitación judicial ex ante del art. 18.3 CE .

Es relevante, de una parte, que en el mundo de la red el empleo de una identidad supuesta es la regla: todos se asoman a ese mundo usando un nick. En este punto el ciberagente encubierto se aparta del agente encubierto convencional en un dato: la asignación de identidad supuesta es una de las vertientes que impulsa a la conveniencia de una autorización. En la red no se produce engaño por la utilización de pseudónimo. Todos lo utilizan: es una regla de ese espacio de comunicación.

El derecho comparado muestra modalidades muy diversas de regulación. Doctrinalmente, se diferencia entre lo que se conoce como ciber patrulleo (el agente realiza exploraciones o indagaciones por canales abiertos de comunicación) y el estricto agente encubierto online que opera en canales cerrados. Solo en este segundo caso la legislación reformada en 2015 requiere autorización judicial, lo que no inexorablemente habría de proyectarse a casos como el ahora examinado en que no estamos ante una infiltración policial en la red, sino ante el uso por la policía del canal creado por quien ha sido detenido, valiéndose de su nickname. Precisamente estas valoraciones llevan a la acusación particular en su dictamen de forma atinada a evocar la jurisprudencia sobre ciber agentes, recaída antes de su plasmación legal en la legislación (reforma de 2015). Venía siendo admitida esa figura por el TS. Paradigmáticas son las SSTS 767/2007, de 3 de octubre; ó 752/2010, de 14 de julio .

Dice la Primera. «Tampoco cabe hacer objeción alguna al primer material grabado que le remite al agente

de la guardia civil, antes de su nombramiento como infiltrado. Por otra parte dicho agente fue moderado en los primeros contactos, hasta ganar la confianza del acusado, el cual poseía hasta el momento el dominio del hecho. El que en los últimos episodios delictivos fueran sugeridas por el agente policial las remesas de material pornográfico o se profundizara en los sentimientos del acusado para descubrir su pedofilia y la existencia de otros responsables, incluso el alcance y derivaciones del delito, o la captura de aquél, entran dentro de su cometido.

Pero es que además, la posible carga sugestiva de las conversaciones o contactos no puede ponerse en entredicho, por cuanto fueron grabadas las conversaciones posteriormente transcritas y no impugnadas, en las que podía conocerse el tono de los contactos y a partir de ellos confirmar o ratificar el testimonio del agente encubierto, en armonía precisamente con el contenido grabado y que ha de operar como prueba lícita y legítima con las demás para desvirtuar el derecho a la presunción e inocencia, que por cierto, el recurrente no ataca.

Por su parte, en la STS 752/2010 de 14 de julio leemos: «Se ha formalizado un solo motivo de casación fundado en los artículos 849.1 y 850.1 LECrim. En su desarrollo, sin ningún rigor casacional, se invocan los derechos fundamentales relativos a la presunción de inocencia y al secreto de las comunicaciones sin mayores precisiones. También subraya la información recibida a través de INTERPOL y no haberse admitido la prueba pericial consistente en que un intérprete jurado tradujese el contenido de las transcripciones en inglés enviadas por la policía australiana.

En relación con esta última cuestión, que ya fue suscitada en la instancia, debemos señalar que lo recibido por la policía española a través de INTERPOL es una denuncia sobre difusión de material pornográfico a través de la red, que da pie para iniciar en España la correspondiente investigación, de forma que no existe vulneración de derecho fundamental alguno cuando ni siquiera la declaración de la agente australiana ha sido utilizada por el Tribunal como prueba de cargo, simplemente se ha transmitido la noticia sobre la existencia de un posible delito en materia de explotación sexual

infantil captada a través de la red. Por otra parte, lo que se afirma en la sentencia, sin que ello haya sido desvirtuado por el recurrente, es que fue éste quien contactó con la agente policial de Australia «a través de internet en el chat de Yahoo Messenger y utilizando el nombre de <>». Esto significa, como también razona la sentencia con toda corrección, que no se trata de un delito provocado. Es cierto que la agente actuó de forma encubierta, haciéndose pasar por un usuario más de la red, pero ello no infringe ningún derecho del acusado en cuanto se limitó a seguir el contacto iniciado por el mismo, que incluyó el envío de las imágenes unidas a las actuaciones (ver el anexo 4º), luego se trataba de una actividad de investigación policial lícita. El propio acusado reconoce los hechos anteriores ante el Juez de Instrucción, en declaración prestada con todas las formalidades legales. En el plenario se retracta, sosteniendo que nunca envió «fotografías con pornografía infantil y que se limitó a reenviarle a Estibaliz las fotografías que ésta le había enviado previamente». Suscitada la contradicción, el Tribunal razona suficientemente sobre la credibilidad de la versión prestada ante el Instructor. Además, también ha valorado la prueba pericial practicada y el resultado del examen del ordenador del acusado. Por todo ello, ni existen las irregularidades denunciadas ni se ha vulnerado el derecho a la presunción de inocencia del recurrente. En relación con la vulneración del derecho al secreto de las comunicaciones, no aporta dato alguno fuera de identificarla con la captación de los mensajes y contactos realizados por el mismo a través de internet, olvidando que el acceso a la información así producida puede efectuarla cualquier usuario, no precisándose autorización judicial para conseguir lo que es público cuando el propio usuario de la red ha introducido dicha información en la misma (ver S.T.S. 739/2008 y las citadas en la misma)». [...].”

En nuestro país, el PDL actualmente en debate en el Congreso para la adopción del Convenio Budapest introduce en Chile al Agente Informático Digital, y en contra de esa posibilidad y destacando los riesgos de su instalación sin más, se muestra la ONG Derechos Digitales en <https://www.derechosdigitales.org/14890/el-regreso-de-los-delatores-en-el-proyecto-de-ley-de-delitos-informaticos/>

Aunque el Gobierno sostiene que en general una política de ciberseguridad integral supone preocuparse de personas e instituciones, como se lee en <https://www.latercera.com/piensa-digital/noticia/el-proyecto-que-busca-proteger-la-informacion-digital-de-los-chilenos/KVPEFOTXAVFLZJJ4IY3ES-2JH6Y/>



Propuesta: Art. 323 del CPP y Evidencia Digital

El Artículo 323 del CPP se dedica a los Medios de prueba no regulados expresamente, y dice que: “podrán admitirse como pruebas películas cinematográficas, fotografías, fonografías, videograbaciones y otros sistemas de reproducción de la imagen o del sonido, versiones taquigráficas y, en general, cualquier medio apto para producir fe”.

Si aceptamos que en esa última parte del precepto bien podrían caber las nuevas especies de Evidencia Digital que hemos descrito en este artículo, admisibles según su pertinencia, importancia y utilidad, hecho el test de legalidad para calibrar si han sido o no obtenidas con violación de garantías o son lo suficientemente bien fundadas con rigor técnico apreciable para considerarlas una Pericia u Opinión Experta, como lo plantea la doctrina más aceptada en el punto. Vid Nuñez Ojeda en https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S071800122017000100007.

Debiéramos decir que al menos son admisibles como “evidencia de apoyo” (en términos de Lubet: 2009, Modern Trial Advocacy).

Y al nivel de la prueba indirecta, siempre y cuando provengan de hechos probados y no otra vez del contexto, pues “la prueba de contexto no es prueba” como escribimos en <https://mbcia.cl/2020/07/27/la-prueba-de-contexto-no-es-prueba-marco-inferencial-prueba-indirecta-y-riesgo-de-prejuicio-indebido-por-juan-carlos-manriquez/> servirá para fundar juicios de inferencia sólidos (SCS 17. 385 – 2019) de que el hecho ha ocurrido y/o que en él han intervenido ciertas personas, ganando así capacidad, preferencia probatoria y fuerza persuasiva de acuerdo a la Constitución, la Ley y los Tratados, y los mejores estándares internacionales que hemos venido tratando.

En consecuencia, sólo cabe llamar la atención de los académicos, jueces y abogados para interesarse en estas materias que ya están siendo parte del debate diario en los estrados.



PROGRAMACIÓN ALGORÍTMICA Y SU IMPACTO EN INDUSTRIA DEL JUEGO

Los abogados Juan Carlos Manríquez y Roberto Contreras abordan las bases de la nueva política nacional sobre inteligencia artificial y cómo ésta puede afectar, por ejemplo, en la programación algorítmica de las tarjetas de juego.

A fines de octubre de 2021, el Ministerio de Ciencia, Conocimiento, Tecnología e Innovación publicó la primera Política Nacional de Inteligencia Artificial (IA) en Chile y su Plan de Acción, convirtiendo a Chile en el país pionero en crear y proteger los neuroderechos, así como regular las neurotecnologías y las plataformas digitales.

Dicha legislación contiene cuatro principios y está dividida en tres ejes con interdependencia. Cada eje aborda las oportunidades y brechas en su ámbito e introduce los objetivos y acciones prioritarias que Chile debe emprender en un horizonte de tiempo de 10 años para cumplir con el objetivo de esta política el 2031.

Estos tienen relación con IA con centro en el bienestar

de las personas, respeto a los derechos humanos y la seguridad; IA para el desarrollo sostenible; IA inclusiva; e IA globalizada y en evolución.

Pero específicamente, según coinciden los abogados expertos en la materia, Juan Carlos Manríquez, y Roberto Contreras, el punto que aborda específicamente el interés por impulsar la transparencia algorítmica, tiene un impacto directo en la industria del juego y en especial, en la programación algorítmica de las tarjetas de juego, siendo –también– muy relevante para evitar discriminación o excesos en la predictibilidad de la “justicia algorítmica predictiva”.

Según el decreto “se debe establecer estándares y recomendaciones de transparencia algorítmica para aplicaciones críticas, esto es, la entrega de información sobre cómo funcionan los algoritmos decisionales que utilizan los órganos de la Administración del Estado, así como los datos involucrados en la toma de decisiones, incluyendo los de su fase de aprendizaje, debe ser oportuna y clara en concordancia con el derecho de acceso establecido en la ley Número 19.628”.

Asimismo, agrega la ley, “se debe velar por la identificación de sesgos en algoritmos, bases de datos y demás componentes de los sistemas de IA, y por la mitigación de riesgos de afectación de derechos fundamentales, especialmente tratándose de los de privacidad, protección de datos personales y no discriminación arbitraria utilizados por los órganos de la administración del Estado”.

Y este sentido, detalla la legislación “en base al liderazgo internacional de Chile en transparencia, “elaboraremos recomendaciones para los sectores privado y público en relación con identificación de sesgos no deseados y transparencia algorítmica, que podrán ser piloteadas en áreas de riesgo”.

Al respecto, Manríquez explica que “dentro de las bases de la nueva política nacional sobre inteligencia artificial, se promueve el desarrollo, la educación constante en los colegios, recolección

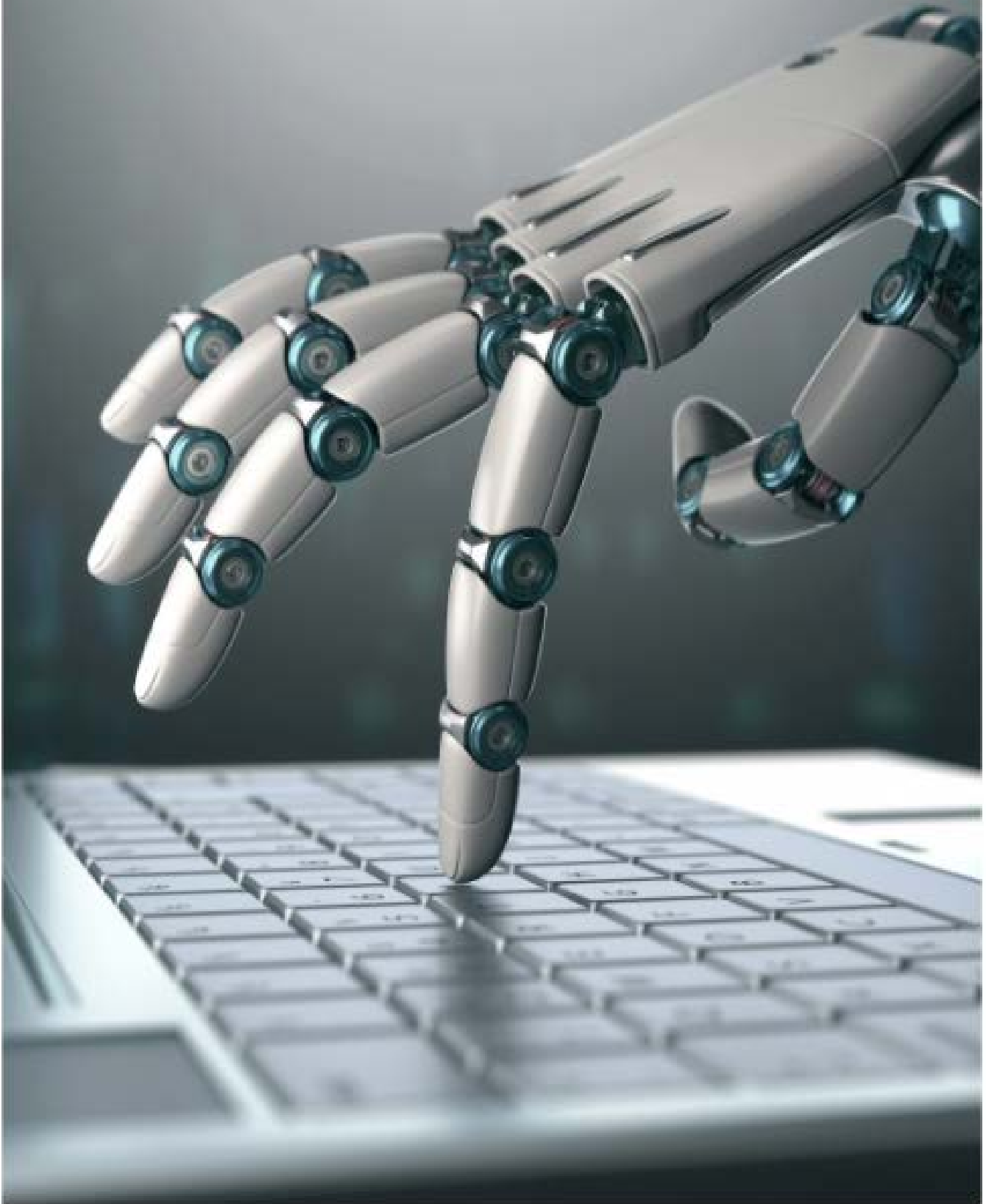
de talentos y establecimiento de laboratorios de trabajo, mencionando que “el tema de los algoritmos, impacta en múltiples actividades: las ventas, la economía, el retail, el juego, la salud, y todo aquello que se basa en decisiones en razón de bases y procesamientos de datos, muchas veces, invasivos; muchas veces, con traqueos absolutamente bombásticos que lo que hacen es molestar a las personas, en este caso, transparentar la programación algorítmicas, evitar la predictibilidad en materias judiciales, de familia, penales, etc., y también, en determinar las necesidades de los consumidores en materia comercial”.

“De ser así, se vería obligado el programador a entregar las bases de la programación algorítmica, sobre todo, en las tarjetas de juego, cuáles son los ciclos, cuáles son las probabilidades de ganar, etcétera, entonces, es interesante lo que viene como balance de derechos socioeconómicos de cuarta generación”.

Por su parte, Contreras – quien es académico de la Universidad Central y coautor del libro “Inteligencia artificial en el sistema de justicia” agrega que “es relevante señalar que la utilización de algoritmos basados en Inteligencia Artificial, podrían considerar una serie de datos parciales o bien, una metodología de diseño sesgada, que no recoja la totalidad de situaciones que representan una determinada realidad y en consecuencia, afectar la toma de decisiones, principalmente en temas tan sensibles como la impartición de justicia”.

“A esto se le denomina ‘los sesgos de los algoritmos’, consecuentemente, es muy relevante propender a que éstos se basen en datos que representen la totalidad disponible de antecedentes y, además, que sean constantemente analizados y recalibrados según la nueva información disponible, como también revisada la operatoria en el diseño. De esta manera, maximizamos los datos, para que los algoritmos permitan decisiones conforme a la realidad y en forma democrática, en concordancia con el párrafo final incorporado en el artículo 19 N° 1 de la Carta Constitucional”, concluye Contreras.





2021